

Authorised push  
payment (APP) scams:  
Requiring reimbursement

Non-confidential  
stakeholder submissions  
to September 2022  
consultation (CP22/4)

June 2023

# Contents

4 Keys International	4
Adam Kramer (Individual)	10
Age UK	12
Barclays	31
Bob Ford and John Bertrand (Individuals)	62
Building Societies Association	71
Call Sign	88
Citizens Advice Scotland	92
Clear Junction	95
ClearBank	102
Consumer Council	112
Counting Up	126
Coventry Building Society	139
Cyber Defence Alliance	149
CYBERA	154
Electronic Money Association	164
Experian	185
Featurespace	189
Financial Services Consumer Panel FINTRAIL & RUSI	205 215
Fire	223
Fraud Advisory Panel	225
Hargreaves Lansdown	236
Innovate Finance	247
Investec	276
ISPAY Limited	284
Larkfleet Group	294
Law Society of Scotland	300
Leeds Building Society	311
Lending Standards Board	319
Lloyds Banking Group	340
Lyddon Consulting	374
Modulr	380
Money Advice Trust	389
Money Saving Expert	404
National Trading Standards	409

Nationwide	419
Natwest	437
Open Finance Association	473
Ordo	481
Pay.UK	490
Payments Innovation Forum	514
Prepay Technologies (PPS)	523
Santander	535
Stafford Railway Building Society	548
Starling	550
Steven Murdoch (Individual)	567
Stop Scams	571
The Money Charity	581
The Payments Association	591
Tink	601
Token	604
Transpact	608
Truelayer	611
TSB	621
UK Finance	637
Unity Trust Bank	664
Victim Support	671
Virgin Money UK	677
Which?	684

Names of individuals and information that may indirectly identify individuals have been redacted.

# 4 Keys International



Submitted by [REDACTED], 4Keys International.

By email to: appscams@psr.org.uk

Dear PSR

Thank you for the opportunity of contributing to the development of a new standard of reimbursement for victims of Authorised Push Payment Scams / Fraud (APPFraud).

## **1. Scam or Fraud?**

Before setting out my response I would like to make a request that you review the use of the words “scam” and “fraud”. If they are used interchangeably, then using two terms is both confusing and unnecessary. If they have different meanings, then please clarify what they each mean.

To assist in your review, I offer the following:

***Scam***: a proposition, in the form of an advert, social contact, urgent email, or phone call; which is based on false information and encourages the potential victim to take an action on the basis that there will be a benefit to them as a result.

***Fraud***: a civil or criminal act, involving deception or omission, which results in financial or personal gain to the fraudster, and/or causes loss to another party, i.e. the victim.

In my view they are two sides of the same coin. The scam is what draws the victim in. The fraud is when they suffer loss.

I suggest that the primary responsibility for preventing scams falls to the media and telecoms companies.

If the primary responsibility for reimbursing people who become victims of fraud falls to the Payment Service Providers, then this proposal should be headed “APPFraud - Requiring Reimbursement”, and the word ‘scam’ should only be used in very limited and specific circumstances.

In addition to the use of words I invite the PSR to consider the standard of test that the banks should apply to deciding if it is fraud. I believe that the test for fraud in this context should be the civil test “on the balance of probability” not the criminal test of “beyond reasonable doubt”.

I am deeply concerned that if the banks are allowed to apply the criminal test then they will hide behind statements such as “there has not been a successful criminal prosecution” as the basis for claiming that it is not fraudulent and does not, therefore, have to be reimbursed. This is important because the Police do not have the resources to pursue more than a tiny handful of cases, so there will only be a limited number of criminal prosecutions.

## **2. The Executive Summary**

These are just a few notes on specific points in the Executive Summary

Para 1.13

There needs to be greater focus on the responsibilities of the receiving banks because they have been ‘getting-away-with-it’ for far too long.

APPFraud could not happen if banks did not provide account services to fraudsters and, in my view, there has been widespread failure on the part of receiving banks in that they have not:

- complied with AML when accounts are opened
- monitored whether account activity is in-line with the declarations made when the account was opened
- responded to clear warning signs (such as a letter from NFIB)
- held and validated exceptional inbound payments.

The new ‘regulations’ should make it mandatory for the beneficiary bank to disclose the recent transaction history of the account to the victim of an APPFraud. This will assist the victim of the fraud in making a complaint against that bank.

#### Para 1.22

I agree with 50:50. In many cases it could be argued that there is greater ‘fault’ on the part of the receiving bank as they have failed in the opening and management of the account used by the fraudster.

#### Para 1.23

I agree that Pay.UK should place more emphasis on “preventing fraud from entering the system” (see below).

### **3. The Introduction**

#### Para 2.9

Measure1 - publishing data is very important because greater transparency will help consumers make better choices about the PSPs they go to for financial services.

Para 3.9 includes the following words:

*Fundamentally, we want all PSPs to take steps to reduce fraud in the system.  
Having robust fraud controls should effectively be a condition of operating in UK payment systems.*

I propose that the phrase “*robust fraud controls*” should be replaced with “*robust fraud prevention measures*”.

As part of Pay.UK’s scheme rules all PSP’s should be required to include at least the following fraud prevention measures:

- a) A mandatory 24-hour delay on the first high value payment [£500?] from a consumer, small charity and SME to a new payee. This allows both the bank and, importantly, the customer, time to realise that the transaction is fraudulent.
- b) An opt-in function to allow consumers, small charities and SMEs to always delay all high value payments by 24 hours, based on a user set threshold.
- c) An opt-in function of Second Party Notification so that all consumers, small charities and SMEs can instruct the bank to copy security messages to a Second Party. This

creates an additional layer of protection for anyone who considers that they may be vulnerable to APPFraud.

- d) Bank Identification under which the bank must demonstrate to the customer that they are their bank when making or receiving phone calls. A system to prevent spoofing of calls, texts and emails must be developed in the longer term.
- e) Active Account Monitoring for inbound payments measured against an account profile. This will be designed to detect cases of accounts 'going rogue' through either fraudulent account creation or account takeovers.

#### **4. Q 3(a) - Payers in Scope**

The scheme should include SMEs as well as micro-enterprises, because the definition of a micro-enterprise is taken from Article 1 and Article 2(1) and (3) of the Annex to Recommendation 2003/361/EC of 6th May 2003, and is therefore completely out of date.

Many SMEs are so busy trying to develop a successful and sustainable business in today's challenging climate that they do not have a "greater capability to protect themselves".

SMEs should, however, be required to show that they had, and complied with, internal systems and process that were designed to protect them from APPFraud. This would include the correct response to CoP warnings and two-factor approval for all payments to new payees.

Including SMEs would also bring this scheme into line with the FOS rules.

#### **5. Q 3(b) - Payment Types in Scope**

It is vital that this scheme covers both 'on-us' and CHAPS.

To exclude 'on-us' would be simply unfair because the payer has no way realistic way of knowing that the payment is 'on-us'.

Fraudsters target high-value payments, such as property transactions, which are often paid by CHAPS. Excluding these from the scheme, when they are currently included in the CRM Code, would have very serious consequences for victims of high value fraud that the scheme should be protecting.

#### **6. Q 3(c) - APPFraud in Scope**

Para 1.2 of this consultation explains that:

*Authorised push payment (APP) scams [fraud] happen when fraudsters trick someone into sending a payment to a bank account **controlled** by the fraudster.*

This is subtly different from the wording in section DS1(2)(a)(ii) of the CRM which reads:

*The Customer transferred funds to **another person** for what they believed were legitimate purposes but which were in fact fraudulent.*

Para 4.11 of this consultation says:

*the payment order was executed subsequent to fraud or dishonesty*

These three approaches may all be applied in different ways by the banks.

I have recently written to both the LSB and FOS regarding the wording of the CRM Code because the phrase ‘another person’ is being interpreted to exclude an account that is, or appears to be, in the name of the victim. I am dealing with two very high value APPFrauds where the fraudster opened the account in the name of the victim, resulting in both they and the victim holding the security credentials, meaning that the fraudster was able remove the money from the account.

In one way the funds were transferred to an account held by the payer, meaning that it would classed as ‘me-to-me’, but from another perspective the account was ‘controlled’ by the fraudster because they had free access to take the money from it.

I suggest that this section be revised to define the scope along the lines of either:

- a) a payment to a beneficiary account where the fraudster holds the security credentials
- or
- b) as set out in paragraph 4.11

## **7. Q 4 - Consumer Caution Exception and Gross Negligence**

It appears to me that this consultation is confused in respect of exceptions to mandatory reimbursement.

The exception in respect of the complainant being involved in the fraud must reflect the provisions of paragraph 71 of PSDII (Directive (EU) 2015/2366) that requires a suspicion of fraud to be communicated to the relevant national authority.

The exception that “the consumer does not exercise adequate caution” is presented in various different ways through the consultation, creating a confused message.

I propose that the exception should be in cases of ‘gross negligence’.

The question of what constitutes ‘gross negligence’ was carefully considered by FOS in 2017/18 when I brought the matter to their attention in respect of the repayment of unauthorised transactions as set out in regulation 75 of PSR 2017, which links back to sections 71 and 72 of PSD2 Directive (EU) 2015/2366.

A possible definition of gross negligence is:

**Gross negligence is** when an individual makes a conscious and voluntary decision to do (or not do) something, with a clear understanding of a foreseeable risk of loss that is directly attributable to that action (or inaction).

This definition places a suitable measure of responsibility on the consumer, whilst taking into account the social engineering and sophisticated scam tactics that result in consumers making decisions that are not “conscious and voluntary”.

In addition, there should be an exception if the consumer failed to respond to a clear negative CoP warning, subject to any such warnings requiring a two-factor over-ride.

## **8. Q 10 - Time Limits**

“A time limit on claims of no less than 13 months from the date of the payment” is completely unacceptable because the banks will have no reason to set a higher limit.

Also, the comparison between unauthorised payments and APPFraud demonstrates a misunderstanding of the nature of certain types of APPFraud.


I am currently investigating an alleged APPFraud in the form of an investment scheme that was launched in 2018. There is strong evidence that the original Information Memorandum contained 'false representations', and the matter is now, 4 years after the scheme was launched, the subject of a Police Investigation.

There are at least four reasons why it has taken this long to reach this point:

1. The investment bonds were issued for three years so it was not until the early investors passed the redemption date that serious concerns were raised.
2. It is most likely that it was a Ponzi with 'profits' being paid out for the first 18 months for the sole purpose of drawing in more investments. A significant proportion of people added to their investment when they received 'profits', or simply asked for their 'profits' to be put back in.
3. The Covid pandemic gave the Director an excellent excuse for putting 'profit' payments on hold and telling investors that they would need to wait for four years (rather than three).
4. There is a catalogue of emails that suggest that the Director of the Investment company may have conspired with the Director of the Security Trustee to stop investors forcing the scheme into administration for up to a year after concerns were being raised.

I propose a time limit of at least five years, and question if there is any reason why it should not be six years.

I would be happy to engage in discussion with PSR, and others, in respect of any of the comments made above, or any other aspect of the consultation.

  
4Keys International  
30 Farley Copse  
Bracknell  
RG42 1PF





23 November 2022

# Adam Kramer (Individual)

My thoughts are as follows:

- I can well understand the desirability of incentivising the banks to act to prevent push payment frauds—effectively to increase education and improve computer systems to detect irregular payments etc.
- I am concerned however that the balance is struck poorly by setting the bar to recovery at fraud or gross negligence. This means that although (because the banks are strictly liable without fault, in contrast with the common law) the customer has within its power the ability to impose almost the entire cost of the fraud on the bank, the customer does not have the duty or incentive to take reasonable care. A careless customer will still recover. This is unfair, but also potentially sets back the improvements in the last few years in customer awareness and behaviour (as customers can now be advised ‘there is no real need to be careful any more when reading emails from your building contractors, creditors, etc- APP fraud is the bank’s problem’). A carelessness standard would be better, and would also provide a framework within which the regulator or other bodies (including the FOS) could build up a body of guidance e.g. if your creditor gives you a new set of bank details these are the steps you must take to verify them before paying to those details.
- The obligation to reimburse within 48 hours unless there is evidence or reasonable grounds for suspicion of fraud or gross negligence (in circumstances where the bank’s own systems plainly have not flagged the payment to be frozen otherwise there would be no need for reimbursement) is unworkable. It does not allow the bank to e.g. request certain information about the fraud and conduct its own investigation (which takes days or weeks from a standing start), and reach a view as to whether the customer acted grossly negligently and contrary to clear guidance, or even was fraudulent.
- On this last point, the automatic nature of the reimbursement can be expected to be a green light to fraudulent claims. It will create an industry of fraudsters who coopt account holders to act as victims, cooperate in the appearance of a phishing or similar attack, and then send money to the fraudster in exchange for a cut of the funds, the customer knowing it will be reimbursed. Indeed, such a fraud is cheaper than a real phishing attack since the fraudster does not need to work out over a period of monitoring what payee to pretend to be, but can just ask the customer who to pose as (what payments are due soon?). The banks will have no way of knowing whether this fraud took place without detailed investigation of the customer’s alleged mistake, computer system, correspondence etc, and with a 48 hour reimbursement period will not even be able to present the appearance of investigating so as to discourage account holders on the basis of fear that they may be found out. These proposals therefore risk creating a new fraud industry to replace APP frauds, albeit that the scale of the new fraud industry will be unknown.
- More thought needs to be given to the fact that most APP fraud payment chains will involve numerous banks, i.e. multiple receiving banks, as to what the at least presumptive rule of allocation of responsibility is.

# Age UK



# Consultation Response

## Authorised push payment (APP) scams: Requiring reimbursement consultation.

### Payment Systems Regulator (PSR)

November 2022

Contact: [REDACTED]

All rights reserved. Third parties may only reproduce this paper or parts of it for academic, educational or research purposes or where the prior consent of Age UK has been obtained for influencing or developing policy and practice.

Age UK  
7th Floor, One America Square  
17 Crosswall  
London  
EC3N 2LB  
T 0800 169 87 87 F 020 3033 1000  
E [policy@ageuk.org.uk](mailto:policy@ageuk.org.uk)  
[www.ageuk.org.uk](http://www.ageuk.org.uk)

Age UK is a charitable company limited by guarantee and registered in England (registered charity number 1128267 and registered company number 6825798). The registered address is Tavis House  
1-6 Tavistock Square, London WC1H 9NA.

## About this consultation

The Payment Systems Regulator (PSR) is aiming to reduce Authorised Push Payment (APP) scams significantly by introducing mandatory reimbursement for victims in all but exceptional cases. This consultation asks for views on proposed measures to: Require reimbursement in all but exceptional cases; improve and make consistent the levels of protection; incentivise banks and building societies to prevent APP scams. The PSR will consider responses in developing its policy decisions on pertinent regulatory requirements in the first quarter of next year. The Regulator will also publish a policy statement on mandatory reimbursement and draft regulatory requirements in line with statutory deadlines. In the second quarter, the PSR will publish the final regulatory requirements.

## Key points and recommendations

- Age UK welcomes the introduction of the reimbursement requirement after APP fraud has occurred.
- We encourage the regulator to work with firms, the Government, the third sector, and the police to develop a comprehensive preventative strategy to sit alongside these proposals.
- Age UK strongly agrees with the proposal to require reimbursement of vulnerable consumers and those with protected characteristics even if they acted with gross negligence.
- The broadest definition of vulnerability should be consistently applied by all Payment System Providers (PSPs) when assessing liability to APP scams,
- We are concerned firms may be less likely to continue providing services to those at higher risk of scams – the Government, Financial Conduct Authority and PSR must monitor this and ensure equal access to payment systems.
- PSPs must provide offline routes (e.g., in a bank branch or over the phone) for consumers to manage payments, demonstrate the legitimacy of transactions, report fraud, and access an APP refund.
- PSPs should comprehensively promote the reimbursement scheme via both online and offline routes – this must include print media, mail drops, and community and voluntary organisations.
- Firms and PSPs must ensure the mechanism for accessing the new reimbursement scheme is intuitive and accessible for digitally excluded older people and those with only low-level digital skills.

- The PSR should investigate extending mandatory reimbursement to include victims defrauded via wider payment systems (e.g., BACS transfers and cryptocurrency platforms).

## About Age UK

Age UK is a national charity that works with a network of partners, including Age Scotland, Age Cymru, Age NI and local Age UKs across England, to help everyone make the most of later life, whatever their circumstances. In the UK, the Charity helps more than seven million older people each year by providing advice and support. It also researches and campaigns on the issues that matter most to older people. Its work focuses on ensuring that older people: have enough money; enjoy life and feel well; receive high-quality health and care; are comfortable, safe, and secure at home; and feel valued and able to participate.

## Introduction

We welcome the opportunity to respond to this consultation<sup>1</sup> on improving redress for victims of Authorised Push Payment (APP) scams. APP fraud involves criminals tricking people into transferring money to them by posing as legitimate payees or socially engineering reasons for payment. This type of fraud has increased substantially in recent years and remains the most significant type of payment fraud in the UK. 2021 saw losses of £583.2m – an increase of 39% from the previous year.<sup>2</sup> In the first half of 2022, compared to the same period in 2021, APP fraud fell by 17 per cent,<sup>3</sup> but it is still higher than in the same period in 2020. Many cases go unreported, so actual figures are likely to be higher.

Fraudsters continue to devastate the lives of older people – annually, around one in twelve (940,000) will fall victim to a scam<sup>4</sup>. APP scams can be highly insidious as victims can lose their life savings in a matter of just seconds, suffering catastrophic, life-changing losses. This can destroy not just their finances but their physical, mental, and emotional well-being. As a result, Age UK warmly welcomes the PSR's mandatory reimbursement proposals.

Implementing the Contingent Reimbursement Model (CRM) Code in 2019 represented a significant leap forward in protecting consumers, but some victims were denied protection because the Code was not mandatory. In the first six months of 2022, 56% of APP scam victims had their funds returned.<sup>5</sup> Although this is an improvement, Financial Ombudsman

Service (FOS) complaints about banks' handling of authorised fraud – the majority of which are APP – increased in the 2021-22 financial year, from 7,700 to 9,370.<sup>6</sup>

We welcome the PSR's proposed scheme to make reimbursement mandatory, as this will ensure the vast majority of APP scam victims receive financial compensation regardless of who they bank with. While we have specific recommendations for maximising the success of the PSR's proposals, we want to make it clear that we strongly support the principle of mandatory reimbursement and are keen to see these proposals implemented as swiftly as possible.

Our extensive experience delivering support to vulnerable older people has given us unique insight into the devastating impact fraudsters have on the lives of older victims. Alongside the PSR's proposals, we want all banks, building societies and other payment providers to do more to prevent APP scams from occurring in the first place. UK Finance has warned that the level of fraud in the UK has reached a point where it must be considered a national security threat,<sup>7</sup> a sentiment we strongly share.

While enforcing the liability of Payment Systems Providers (PSPs) for fraudulent transactions is a welcome development, prevention of scams is also key. Even after the PSR implements its proposals, the benefits will only be felt by older people who have already been victimised, with all the stress and strain this entails. We believe that alongside these proposals, there needs to be a renewed focus on preventing fraud. This will require the Government, police, regulators, industry bodies, payment service providers and the community and voluntary sector to work collaboratively to shut down the scammers and reduce the wider risk of fraud.

## **1. Do you have views on the impact of our proposals on consumers?**

These proposals will be of tremendous benefit to older consumers. Fraud affects people of all ages and backgrounds, but older people can be particularly vulnerable to certain scams – often leading to severe emotional and financial harm. One in 12 older people (eight per cent) – around 940,000 – are victims of scams each year.<sup>8</sup> A recent survey by Which? found fraud victims aged 65 and over reported losing more money than any other age group (an average of £2,697 compared with £1,731 overall).<sup>9</sup> Women aged 65 and over lost twice as much as male victims of the same age. Older people may be specifically targeted for scams because of their age. Some may be particularly vulnerable due to ill health, dementia, social isolation, digital skill needs, and a perception of increased wealth.<sup>10</sup> With this in mind, Age UK warmly welcomes the regulator's proposal to impose mandatory reimbursement for all APP scams to benefit older consumers by substantially increasing the proportion of victims reimbursed by PSPs.

However, there is a risk that mandatory reimbursement proposals could incentivise some PSPs to apply stringent criteria when deciding whether to allow a customer to open an account. We are concerned that firms may be less likely to continue providing services to those at higher risk of falling victim to scams – including many older people. This would be a patently unacceptable outcome at odds with PSR and Government efforts to improve financial inclusion.

Although we want firms to refuse atypical transactions to deter fraudsters, we do not want aggressive warnings geared specifically towards demonstrating gross negligence on the consumer's part if they proceed. Our concern is that this may create an unwelcome environment for consumers, with PSPs trying to use disclaimers to get around the rules and make it increasingly difficult to access a legitimate reimbursement claim. This approach could also result in lengthy battles through the Ombudsman or the courts to resolve who is at fault in different scenarios. This should not be confused with a clear warning of a potential scam which is of course an essential preventative measure.

Older people also face increased rates of digital exclusion, with two-fifths of those aged 75+ not using the internet. Age UK is aware that some older people are increasingly reluctant to use online payment services because of greater awareness and fear of scams, with 39% saying they don't trust the internet.<sup>11</sup> Santander data shows that the number of those over 55s who continue to avoid using digital banking has remained roughly the same since the pandemic, with around one in six (16%) choosing not to use their bank's digital services to manage their money. Among those over 55s who don't bank online, 64% blame concerns over security.<sup>12</sup>

PSPs must be mindful of consumers facing barriers to getting online and those who are reluctant to undertake day-to-day transactions or manage their money over the internet. PSPs must provide offline routes (e.g., in a bank branch or over the phone) for consumers to manage payments, demonstrate the legitimacy of a transaction, report suspected fraud, access an APP refund, and speak with their provider about any concerns. PSPs should be mandated to comprehensively promote the reimbursement scheme via online and offline routes. The PSR should also arrange the promotion of the scheme through various sources, including print media, mail drops, and community and voluntary organisations.

## **2. Do you have views on the impact of our proposals on PSPs?**

The proposed measures will significantly impact the PSPs' reimbursement requirements and public image, incentivising firms to focus on their communication and education

strategies. Only 51% of APP scam losses were reimbursed to the victim under the Voluntary Code in 2021, creating a reimbursement lottery depending on who you bank with.<sup>13</sup> As mentioned, complaints to the FOS about banks' handling of authorised fraud cases – the majority of which are APP – have increased. And three-quarters (73%) of these were upheld in favour of the customer, so banks often get it wrong. These proposals will compel PSPs to do better.

### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

Age UK welcomes the introduction of the reimbursement requirement after APP fraud has occurred, but it is also important that more action is taken to prevent APP scams in the first place. We would encourage the regulator to work with firms, the Government, the third sector, and the police to develop a comprehensive preventative strategy. Reimbursement is a critical component of ensuring consumer redress after a scam, but by the time this occurs many of the negative consequences of being targeted have already taken their toll on the victim.

From experience, we know that for many older victims, this creates a sense of panic at the prospect that they may have been defrauded out of life-changing amounts of money. Needless to say, the impact on their mental and physical well-being can be truly devastating, often leaving them fearful and isolated. While the PSR's proposals will doubtlessly bring much-needed relief to many more victims, it is important comprehensive preventative measures are put in place alongside these proposals.

Technology and telecoms firms, which are part of the APP scams ecosystem, also need to do more to stop scams at source before they adversely impact consumers. UK Finance analysis has shown that seven in 10 (70%) of APP scam cases originate through search engines, social media, and fake websites.<sup>14</sup> We welcome the Government's intention to combat scam advertisements in the Online Safety Bill and hope to see this carried out.

### **4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

The regulator is proposing an exception to mandatory reimbursement if a consumer is grossly negligent, which aims to incentivise customers to take care. This is designed to limit any disproportionate costs to PSPs if customers were to exercise less caution following the implementation of mandatory reimbursement. However, there is no evidence to show that consumers will act with less caution following implementation. If the regulator goes ahead with this, they should require PSPs to provide consumers with clear guidance on what they expect of their customers. The regulator should be clear what constitutes gross negligence and take legal advice to ensure that it aligns with a consistent definition. Without a robust regime from the outset, we can expect years of legal challenges.

We note that TSB bank exemplifies gross negligence as repeatedly ignoring safety advice. This has resulted in a 98% reimbursement rate due to scams under their fraud refund guarantee. In contrast, at other banks, on average, only 47% of stolen money is refunded to victims.<sup>15</sup> We want a robust and consistent definition of gross negligence policies similar to TSB's determination of gross negligence applied by other PSPs to achieve similar reimbursement rates. The regulator should consider committing to TSB's fraud refund guarantee as additional guidance for gross negligence to cover consumers against honest mistakes.<sup>16</sup>

## **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

Age UK strongly agrees with the proposal to require reimbursement of vulnerable consumers and those with protected characteristics even if they acted with gross negligence. As the regulator rightly points out, there is evidence that older consumers are more likely to be victims of APP scams.<sup>17</sup> Some older people are especially at risk, either because scammers target them or because their circumstances make them vulnerable to scams, for example, if they are recently bereaved, lonely, or mentally or physically ill. Evidence also shows that there is a correlation between ageing and the likelihood of falling victim to a scam.<sup>18</sup> For older people experiencing mental health problems, it can mean they are less likely to get their money back and are more than twice as likely to fall into debt because of fraud.<sup>19</sup>

To advance equality of opportunity, the regulator should implement this requirement within its powers to require mandatory reimbursement in cases of APP scams. The regulator might consider utilising centralised records of vulnerability across the payment system to ensure consistency of approach for all PSPs' customers. The Lending Standards Board has highlighted that when disclosure of a vulnerability is not apparent or forthcoming from customers, firms tend to struggle to identify vulnerable cases.<sup>20</sup> This can happen at a firm



and employee level due to poor questioning of customers and the need for awareness training on vulnerability to scams.

Although we are supportive, an existing vulnerability or protected characteristic must not be used to discriminate against consumers when it comes to accessing payment services. PSPs should review their vulnerability training to ensure that customer circumstance is fully considered. This could lead to more specialised teams that comprehensively account for consumer vulnerability and determine a customer's circumstances so as to understand how this has impacted them when being scammed. We urge the regulator to ensure PSPs improve their vulnerability training, so that customer circumstance is fully considered.

## **6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

While it is important that older age is not automatically equated with vulnerability, Age UK is acutely aware that people in later life are more likely to be exposed to the circumstances (e.g. social isolation, digital exclusion, poor health) which make them more vulnerable to exploitation by fraudsters. We would therefore welcome a definition of vulnerability which comprehensively encompasses at-risk older people. This will better reflect the threat they face from fraudsters, particularly given that they generally suffer higher losses<sup>21</sup>, while mitigating the risk of them missing out on reimbursement due to issues such as digital exclusion.

The Financial Conduct Authority's (FCA) definition of a vulnerable customer as "someone who, due to their circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care" serves as an appropriate definition, particularly as some PSPs and the FOS have applied this concept previously.<sup>22</sup> We welcome the PSR using this definition, particularly as customers identified as vulnerable via this approach will be exempt from claims of gross negligence. However, we wish to reinforce that this definition must be interpreted in a consistent way with a focus on ensuring the broadest range of vulnerable customers are included within the scope.

The FCA views vulnerability as a spectrum of risk, which we agree with. All consumers are potentially vulnerable to APP scams, but this risk is increased by certain characteristics such as mental health problems, physical disability, and low income. Many other factors, such as 'time poverty', confidence in using the internet, and educational attainment, are likely to affect consumers' ability to engage in specific markets.<sup>23</sup>

Recently, a Pay.UK poll found that 54% of UK adults had at least one characteristic of financial vulnerability<sup>24</sup> – in line with the FCA's most recent survey (53%, as of October 2020).<sup>25</sup> Indeed, there are specific market contexts in which all of us can experience a degree of vulnerability – for example, when we need to purchase at a stressful time. Vulnerability is also known to arise when assessing the value of a product, where it involves complex estimations of risk or probability. UK Finance highlighted this year that more than half of the public (56%) said they are likely to look for opportunities to make



extra money in the coming months due to the rising cost of living. And one in six (16 per cent) Britons said the increasing cost of living meant they were more likely to respond to an unprompted approach from someone offering an investment opportunity or a loan.<sup>26</sup> This could leave many people more susceptible to fraud. Therefore, we would like to see the broadest definition of vulnerability applied by all PSPs when assessing liability to APP scams, which we believe the FCA's above definition should cover.

## **7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

We understand the rationale behind the proposal to allow sending PSPs to apply a fixed 'excess' of £35 to reimbursement as an incentive for smaller PSPs to use preventative measures and deal with administration costs. However, currently under the CRM Code, victims of APP fraud get all their money back if the customer has taken all the steps set out in the code.<sup>27</sup> When there is an increase in the cost of living, applying an excess to individuals who have reasonably done all they can to protect themselves is not practicable. PSPs should consider an individual's financial circumstances when assessing if they should implement the excess of £35. We therefore call for an exception for vulnerable customers from the £35 excess.

## **8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set.**

We know there will be a post-implementation review of the minimum claim threshold to see if it needs to be reduced or eliminated. Age UK's view is that within the context of a cost-of-living crisis it would be better to instead trial the mandatory reimbursement scheme without the £100 minimum and then consider if this needs to be added later.

While we understand the rationale for the proposal that the sending PSPs should be allowed to set a minimum claim threshold of no more than £100, we are concerned about the impact this might have on those struggling to balance their household budgets. While

APP scams under £1000 represent just 8% of losses by value<sup>28</sup> the PSR must be mindful that for many of those reliant on the State Pension as their sole source of income a hit of less than £100 to their bank balance can still prove a devastating blow to their finances. Our view is that it is often less about the volume of money taken and more about the impact this has based on the specific circumstances of the victim.

Furthermore, we can envisage scenarios where scammers target victims to make small payments over a period. As we know, victims often end up on lists passed around by criminal groups perpetrating scams. In these circumstances, we do not want the discretion to be up to PSPs to determine if these victims should be reimbursed – instead, we want these transactions to be counted cumulatively instead of being treated in isolation. It is crucial that if scammers target victims multiple times over separate transactions for less than £100 at a time, that any minimum claim threshold cumulatively accounts for this rather than treating them as separate incidents.

We would also warmly welcome a minimum claims threshold exemption for vulnerable consumers. We strongly encourage the PSR to go further than its proposals and make this vulnerability exemption mandatory across all PSPs.

## **9. Do you have comments on our proposal not to have a maximum threshold?**

We strongly agree with the proposal not to have a maximum threshold. Increasing numbers of older people risk losing truly staggering sums of money through APP scams. Given this, we agree that if a PSP allows a substantial fraudulent payment, it should be liable for victim reimbursement regardless of the value of the transaction. This will ensure protection for those who might otherwise lose their life savings through no fault of their own.

## **10. Do you have comments on our proposals that:**

- sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- any time limit should be set at no less than 13 months?**

We understand the reasoning for allowing sending PSPs to set a time-limit for mandatory reimbursement, as we acknowledge this is the same limit set for claims for refunds of unauthorised payments under the Payments Systems Regulations 2017.<sup>29</sup> However, there is an issue where some payment instructions will be large amounts from fictional investment and pensions schemes (or romance fraud), and it may not be apparent that these payments have been fraudulent for many years.

Indeed, as part of its latest quarterly data publication, the Financial Ombudsman has found that investment scams have seen the most considerable increase in the proportion of “authorised” scam complaints, despite the number of “authorised” scam complaints decreasing overall.<sup>30</sup> In such scenarios, a 13-month time limit is not realistic. Granted, the regulator has noted that consumers may appeal to the Financial Ombudsman Service (FOS) up to six years from a problem occurring, or longer, if still within three years of the consumer becoming aware (or when the consumer should have reasonably become aware) of the scam.

However, our concern is the extent to which the 13-month time limit would curtail the powers of the FOS and prohibit victims from accessing reimbursement. We encourage the PSR to implement a more flexible approach, avoiding setting a hard deadline regardless of circumstances. This would ensure that victims of particularly insidious scams, such as romance fraud, who may not have been aware that they were scammed until much later than 13 months, can still come forward and access reimbursement from PSPs.

## **11. Do you have comments on our proposals that:**

- the sending PSP is responsible for reimbursing the consumer**
- reimbursement should be as soon as possible and no later than 48 hours after a claim is made unless the PSP can evidence suspicions of first-party fraud or gross negligence.**

We agree with this approach. The Lending Standards Board (LSB) has reported that nearly all PSPs’ processes of assessing reimbursement claims focus their investigation on the repatriation of funds from the receiving bank. Conversations with customers tend to allude to the fact that reimbursement would only be successful if the receiving bank had managed to freeze and return the funds to the sending bank.<sup>31</sup>

By compelling the sending PSP to reimburse victims of APP fraud as soon as possible and no later than 48 hours, we hope this will deter firms from giving victims incorrect

information of placing reimbursement solely on recovery of funds from the receiving firms. Ultimately, we hope this will put less onus on the victim to prove themselves by jumping through standard-of-care tests, which require consumers to meet a disparate set of standards imposed by different PSPs before being reimbursed.

## **12. What standard of evidence for gross negligence or first-party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The provision of a warning should not be used as evidence for gross negligence or first-party fraud or as a strict measure of liability for declining reimbursement. Nor do we believe Confirmation of Payee (CoP) should be used by PSPs as a rigorous measure of liability in declining reimbursement. All considerations concerning the scam should be deliberated to assess the victim's reasonable basis for belief and inform the PSPs' cause for investigation.

As mentioned above, PSPs may try and gear their warnings toward proving gross negligence which consumers may not pay mind to as they believe the transaction to be legitimate (as such is the reality of being scammed). Therefore, using such warnings and CoP may allow situations where PSPs treat legitimate victims negatively.

## **13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

Ultimately, we would like to see a system where the reimbursement levels are split 50:50 at the outset. Current data shows that receiving PSPs are not doing enough to reimburse victims (contributing less than 5% on average to reimbursement costs) even though the fraudster banks with them.<sup>32</sup> Receiving PSPs must do better in vetting their clients and ensuring a stable financial ecosystem that avoids harm to UK consumers, especially those at risk or vulnerable to becoming victims.

While we are cognisant that this may disadvantage new market entrants<sup>33</sup> we don't want a situation where smaller PSPs are freely onboarding customers and not doing their due diligence in the name of competition. We believe smaller PSPs and new entrants should

respond by developing more effective fraud controls. Granted, such advanced controls would also come at a cost. Nevertheless, smaller PSPs and new entrants should now start considering how this proposed model might affect them and what improvements they can make to their system to disrupt scammers and create a more secure financial ecosystem.

A 50:50 default allocation of reimbursement costs between sending and receiving PSPs will enable cross-sector data-sharing to better prevent and detect APP scams. Data and information sharing will be crucial to dealing with APP fraud. By incentivising both the sending and receiving PSPs to share data through a default allocation of reimbursement costs, the regulator will ensure industry pursues preventative measures to tackle APP fraud. Moreover, since better information sharing is one of the Strategic Objectives of the UK Government's current Economic Crime Plan (and is likely to underpin the upcoming second iteration), we believe this proposal aligns with the Government's sentiment that prevention is better than cure.<sup>34</sup>

**14. Do you have views on our proposal that PSPs can choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We fear that departing from the 50:50 default allocation by negotiation, mediation, or dispute resolution based on a designated set of more tailored allocation criteria will lead to tension between PSPs. We can envisage situations where PSPs differ in opinion in developing and implementing such arrangements. For example, the Lending Standards Board indicates a need to draw out expectations more clearly for receiving firms. After all, a PSP has helped scammers collect their money. It is not right that receiving PSPs do not contribute enough to reimbursement costs. Receiving PSPs must do better to vet their customers and ensure a stable financial system. Therefore, we do not support the proposals to depart from the 50:50 default allocation. We prefer if they both automatically send 50% to the victim. Then they can depart from the 50:50 allocation if they have repatriated the funds. If banks are compelled to each send 50% of the stolen money, then all PSPs will do more to communicate quickly and effectively work with one another to detect and freeze fraudulent funds. This should allow for all PSPs to implement stringent preventative mechanisms that deter APP scams from happening in the first place.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

Multi-generational scams are where the end-to-end journey involves more than one payment. For example, fraudsters may 'socially engineer' a consumer to transfer money from their bank account to the account they hold at a different PSP (or perhaps persuade them to open a new account in their own name). The fraudster then persuades the consumer to transfer the money from that account into the account under the fraudster's control. Sometimes, that second payment may be a transfer using Faster Payments to an account held at a PSP. In other cases, the second payment may be to a different type of account, such as a crypto wallet, which does not happen over Faster Payments, but uses an alternative method (e.g., a card or crypto-based payment system). An increasing proportion of scams involve consumers being convinced to move payments from their bank accounts to accounts in their name with legitimate cryptocurrency platforms, with converted cryptocurrency then transferred to the scammer. The funds remain in the consumer's control after the initial transfers from the account with the PSP, and the scam takes place from the cryptocurrency wallet (and not by Faster Payment). It is not clear if such scenarios of multi-generational fraud are intended to be covered by the mandatory reimbursement proposal. Which? have warned that there is limited legal protection for such losses with their research finding that 20% of fraud victims tricked into sending money to criminals in the past two years used cryptocurrency, and 17% used digital wallets such as Apple Pay.<sup>35</sup> It remains unclear how the proposed 50:50 default allocation can be applied in these instances. This represents a potential gap in the PSR's proposals as cryptocurrency exchanges cannot, as it stands, be required to refund their customers.

The regulator must analyse these situations further to determine the liability of mandatory reimbursement. Age UK would encourage an approach which extends reimbursement to include victims defrauded via cryptocurrency platforms.

## **16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

Repatriation of APP scam losses occurs when the receiving PSP can detect, freeze, and return funds stolen as part of an APP scam. Fast and effective communication from the sending PSP may aid receiving PSPs in detecting and freezing fraudulent funds. Data from UK Finance show that there are currently very low repatriation rates. In 2021, £12.4 million was returned to victims through repatriation, accounting for just 5% of the total reimbursed to victims by CRM Code signatories.<sup>36</sup>

Scammers often quickly transfer stolen money to other accounts and jurisdictions, making it hard for PSPs to trace and return. However, there is also a lack of incentive for receiving PSPs to try increasing repatriation rates. Age UK believes that a 50:50 default allocation of

repatriated funds between sending and receiving PSPs is the right way to incentivise all PSPs to prevent APP scams from happening in the first place. Nevertheless, this will only work if the mandatory reimbursement is split 50:50 between the sending and receiving banks as a default – if banks are compelled to each send 50% of the stolen money, then all PSPs will do more to communicate quickly and effectively with one another in order to detect and freeze fraudulent funds.

## **17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We welcome the proposal that the rules on allocating reimbursement costs apply to all directly connected PSP participants sending and receiving payments over Faster Payments and PSPs indirectly sending and receiving payments. Trends show scammers are migrating to receiving PSPs who are not participating in existing safeguards such as the CRM Code and CoP. For example, PSPs that were not given Specific Direction 10 (SD 10)<sup>37</sup>, requiring the UK's six largest banking groups and building societies to provide CoP checks for Faster Payments, accounted for 20% of Faster Payment transactions in 2021 but received 50% of APP scam payments sent from SD 10 PSPs. Applying the allocation of costs of reimbursement to all directly connected PSPs and indirect PSPs sending and receiving payments would allow for a consistent model and incentivise all PSPs to detect and prevent APP scams.

## **18. Do you have views on our long-term vision and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

We cautiously welcome the call for the Payment Systems Operator (Pay.UK) to introduce new rules to provide better governance of the payment systems under its control. We are cautious in supporting this expanded role for Pay.UK because it has so far failed to implement fraud mitigation measures in its ruleset without intervention from the PSR.

Currently, Pay.UK's existing constraints do not allow for implementing the proposals set out. However, in the long term, after developing the resources and arrangements it requires, Pay.UK may be the appropriate body to undertake the role of maintaining, refining, monitoring, and enforcing compliance that addresses fraud risk in the system. We would welcome ongoing consultation on what arrangements for the monitoring and assurance of implementing the regulator's requirements are needed for Pay.UK to carry out this role adequately.



## **21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

We cannot foresee a scenario where dispute resolution arrangements for allocating reimbursement liabilities are developed and implemented in the short term. The regulator posited a system where this arrangement could be implemented after asking the industry to develop and implement the agreements. However, this scenario would most likely return a varied response from PSPs and push such arrangements back into the long term.

If the regulator does choose to impose a dispute resolution arrangement, it would be better if a body such as the LSB maintained such arrangements. The LSB already oversees, monitors, and enforces the CRM Code and has made significant progress in identifying a set of standards for preventing and detecting APP scams and linking these to the allocation of reimbursement liabilities. Such future arrangements would therefore be better built on the achievements of the LSB by designating them to oversee the allocation of reimbursement liabilities.

## **22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

One of the key challenges of the mandatory reimbursement proposal is ensuring PSPs follow the rules. The PSR will need comprehensive and timely information on compliance to pursue any necessary enforcement action or provide regulatory updates if required. A clear and rigorous compliance assessment framework is essential to achieving this goal. This monitoring regime must be implemented from the outset of the mandatory reimbursement scheme. PSPs should be required to report regularly to Pay.UK on their performance. This will ensure that regulators, consumer groups, and the Government can assess the Scheme and, if necessary, recommend changes.

## **23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system, and when could it be introduced?**

As outlined in response to question 22, the PSR must ensure that a monitoring regime is implemented from the outset of the mandatory reimbursement scheme. This should include a real-time compliance monitoring system as early as possible.



## 24. Do you have views on the best option for short-term enforcement arrangements?

The best option for short-term enforcement would be for the regulator to apply fines and penalties on any PSP that fails to comply with scheme rules on reimbursement within the set timescale. If these measures fail to ensure the rules are followed in the short term, the regulator should escalate action against non-compliant PSPs. Any proceeds from fines or penalties should also be redirected towards scam victims.

This would give Pay.UK time to develop and improve its enforcement regime. Longer term, we would like to see Pay.UK apply its enforcement regime as the Payment Systems Operator, but with escalation to the PSR as one of the steps in that regime.

## 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?

The Faster Payment System allows all participants to connect safely and securely, directly or indirectly, to the Faster Payment System central infrastructure to facilitate real-time payments. However, presently, Faster Payment rules only apply directly to direct participants. The regulator has posited that if it were to initially implement reimbursement requirements on PSPs through a direction, with Pay.UK operationalising those requirements, the regulator's direction would apply to direct and indirect participants.

Although this is not the PSR's preferred option, this option would enforce reimbursement rules for all Faster Payments. We suggest such rules apply initially so that older consumers are protected before, longer term, the New Payments Architecture (NPA) rules on reimbursement apply to all NPA participants (direct and indirect participants of Faster Payments).

---

<sup>1</sup> : [CP22/4: Authorised push payment \(APP\) scams: Requiring reimbursement | Payment Systems Regulator \(psr.org.uk\)](#)

<sup>2</sup> [Fraud The Facts 2021- FINAL.pdf \(ukfinance.org.uk\)](#)

<sup>3</sup> [APP fraud - less talking, more acting | Insights | UK Finance](#)

<sup>4</sup> Age UK analysis of data from the Crime Survey for England and Wales 2018-19, scaled up to the England and Wales aged 65+ population using ONS midyear population estimates for 2020.

<sup>5</sup> [Half year fraud update 2022.pdf \(ukfinance.org.uk\)](#)

<sup>6</sup> [Annual complaints data and insight 2021/22 \(financial-ombudsman.org.uk\)](#)

<sup>7</sup> [UK Finance: Scale of fraud a 'national security threat' | This is Money](#)

<sup>8</sup> [OLDER PERSON BECOMES FRAUD VICTIM EVERY 40 SECONDS| PRESS RELEASE | AGE UK](#)

<sup>9</sup> [One in five fraud victims send money to criminals via cryptocurrency - Which? News](#)

<sup>10</sup> [age uk briefing fraud and scams sept 2016.pdf \(ageuk.org.uk\)](#)

<sup>11</sup> Age UK, 2021. *Briefing Paper: Digital inclusion and older people – how have things changed in a Covid-19 world?*. Age UK. [Online]. Available at: <https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/active-communities/digital-inclusion-in-the-pandemic-final-march-2021.pdf>. [Accessed 05/08/21].

<sup>12</sup> [Over 55s Flock Online during Coronavirus Pandemic but Miss Out on Digital Banking Opportunity | Santander UK](#)

- 
- 13 [Annual Fraud Report 2022 FINAL .pdf \(ukfinance.org.uk\)](#)
  - 14 [70% of APP scam cases start online, UK Finance study reveals - Money Age](#)
  - 15 [Annual Fraud Report 2022 FINAL .pdf \(ukfinance.org.uk\)](#)
  - 16 [Fraud Refund Guarantee | TSB Bank](#)
  - 17 [Most vulnerable in society are more at risk of falling victim to fraudsters | Action Fraud](#)
  - 18 [Correlates of Susceptibility to Scams in Older Adults Without Dementia - PMC \(nih.gov\)](#)
  - 19 [Fraud victims experiencing mental health problems are twice as likely to fall into debt - Which? News](#)
  - 20 [CRM-Review-R21c-Follow-Up-Summary-Report.pdf \(lendingstandardsboard.org.uk\)](#)
  - 21 [One in five fraud victims send money to criminals via cryptocurrency - Which? News](#)
  - 22 [Guidance for firms on the fair treatment of vulnerable customers | FCA](#)
  - 23 [Consumer vulnerability: challenges and potential solutions - GOV.UK \(www.gov.uk\)](#)
  - 24 [Internal Longform \(wearepay.uk\)](#)
  - 25 [Financial Lives 2020 survey: the impact of coronavirus \(fca.org.uk\)](#)
  - 26 [Public are warned to stay alert to fraud as a result of the rise in the cost of living | Insights | UK Finance](#)
  - 27 [Information-for-customers-CRM.pdf \(lendingstandardsboard.org.uk\)](#)
  - 28 [Annual Fraud Report 2022 | Policy and Guidance | UK Finance](#)
  - 29 [The Payment Services Regulations 2017 \(legislation.gov.uk\)](#)
  - 30 [Consumers warned about rise in investment scams \(financial-ombudsman.org.uk\)](#)
  - 31 [CRM-Review-R21c-Follow-Up-Summary-Report.pdf \(lendingstandardsboard.org.uk\)](#)
  - 32 [CP21/10 Authorised push payment \(APP\) scams consultation paper | Payment Systems Regulator \(psr.org.uk\)](#)
  - 33 New market entrants may argue that this approach could reduce competition because of the potentially significant cost implications for them as a new firm.
  - 34 [\[Title\] \(publishing.service.gov.uk\)](#)
  - 35 [One in five fraud victims send money to criminals via cryptocurrency - Which? News](#)
  - 36 [Annual Fraud Report 2022 FINAL .pdf \(ukfinance.org.uk\)](#)
  - 37 [PS19/4 - Specific Direction 10 \(Confirmation of Payee\) | Payment Systems Regulator \(psr.org.uk\)](#)

Barclays

Payment Systems Regulator

Consultation on Authorised Push Payment (APP) Scams: Requiring  
Reimbursement

CP22/4

Response on behalf of Barclays Bank UK plc and Barclays Bank plc

8 December 2022

## Submission by Barclays

Barclays is a universal consumer and wholesale bank with global reach, offering products and services across personal, corporate and investment banking, credit cards and wealth management. With over 330 years of history and expertise in banking, Barclays operates in over 40 countries and employs approximately 85,000 people. Barclays moves, lends, invests and protects money for customers and clients worldwide.

We welcome the opportunity to respond to the Payment Systems Regulator's (PSR) consultation CP22/4 on Authorised Push Payment (APP) Scams: Requiring Reimbursement.

## Executive Summary

Barclays welcomes the Payment Systems Regulator's (PSR) continued efforts to help the victims of scams. We support a mandatory reimbursement rule, and the intent to require all Payment Service Providers (PSPs) to be accountable and liable for reimbursement – driving consistency in consumer outcomes across the payments sector.

### **Prevention needs to be as important as reimbursement**

While a necessary step, underwriting victims' financial losses will not slow the UK's growing epidemic of scams, nor prevent the non-financial impacts on customers and industry. Therefore, we strongly encourage the PSR – and wider policymakers and regulators – to take further action to prevent scams from occurring in the first place, and to not take steps that will disincentivise current scam-preventing activity.

As an example, the proposed mandatory reimbursement rule will effectively replace the current Contingent Reimbursement Model (CRM) Code for Faster Payment System (FPS) payments. Whilst this will enhance the reimbursement provisions, it will also have the impact of removing non-reimbursement related provisions. For example, the CRM Code requires actions from PSPs such as customer education and effective warnings. Our previous recommendation to mandate the CRM Code was to ensure that these preventative actions were also mandated across the sector, in addition to reimbursement.

### **Upstream polluters must do more**

Even more critical is the need to have an end-to-end strategy for tackling scams at source, that involves all the relevant actors in the 'scam journey', with the payment from victim to criminal being only the last step in a complex range of interactions and actors. As has been evidenced by Barclays and various organisations, and spotlighted in the recent House of Lords report 'Fighting Fraud: Breaking the Chain'<sup>1</sup>, the majority of scams are perpetrated through criminals' exploitation of vulnerabilities 'upstream' in other sectors, such as online platforms (e.g., social media, online

---

<sup>1</sup> Fighting Fraud: Breaking the Chain', House of Lords: Fraud Act 2006 and Digital Fraud Committee Report, Nov 2022 – pg. 5 "Fraudsters use a variety of channels to reach their victims, and they follow a series of steps before they are able to 'cash out' their stolen funds. Within this fraud chain, there are multiple stakeholders across several sectors that enable fraud to take place and often fail to put adequate systems in place to prevent it. For too long, these businesses have been allowed to enable and facilitate fraud."

marketplaces, dating websites etc.) and the telecommunications ('telco') sectors, to target, socially engineer and scam victims.

For this reason, it is critical that all upstream polluters in the 'scams ecosystem' are suitably regulated and incentivised to take the necessary action to prevent criminals leveraging their infrastructure. And where they fail to do so – as is largely the case today – they must be liable for the consequences.

It is therefore our concern with the PSR's proposals that they serve to only solidify PSPs' responsibilities, while doing nothing with respect to the wider scams ecosystem, which will have the impact of increasing liability for PSPs for the failures of others. It is clearly right that banks should be liable where their actions have been insufficient, but this must be accompanied by similar requirements for others. We therefore welcome the recommendation in the House of Lords report, that "To incentivise companies to act on fraud and more accurately reflect the balance of responsibility for fraud, the Government must establish a mechanism by which fraud-enabling sectors—in addition to the outgoing and recipient PSP—are required to contribute to the costs of reimbursement in cases where their platforms and services helped to facilitate the fraud."<sup>2</sup> We would therefore encourage the PSR to work with Government to consider how this could be realised, or at the very least not prevented by the PSR's proposals.

In this vein, a further concern we hold with the PSR's proposals is that they do not include any mechanism for moving to a model that includes a role for other sectors, even where this is within the PSR's remit. For example, as we have previously argued, a small but important first step would be through the PSR mandating that PSPs publish their 'scams enabler' data, i.e., data on the extent to which successful scams have been enabled through the action or inaction of others in the 'fraud chain'. This could potentially be mandated as part of the PSR's Measure 1 Data Publication proposal, which would serve to evidence who the worst polluters are, and encourage policymakers to require them to take preventative action. We would therefore strongly encourage the PSR to reconsider on this matter, as without a commonly accepted evidence base on the nature of the threat, it will be highly challenging to agree on the right solutions.

### **Government needs to lead a cross-sectoral approach to tackling scams**

The links between fraud, organised crime and terrorism pose a significant and growing threat to the UK's national security which requires a holistic policy and operational response.

While we recognise that the PSR's remit only applies to PSPs, we would strongly encourage them to urgently come together with their counterparts in His Majesty's Treasury (HMT), the Home Office, the Department for Digital, Culture, Media and Sport (DCMS), the Financial Conduct Authority (FCA), Ofcom and others, to devise and implement a comprehensive strategy for tackling scams that includes requirements for all relevant actors, and apportions liability fairly.

We therefore need government to lead a coordinated effort in developing a comprehensive approach to addressing this societal issue. System leadership and coordination on the public sector side must be informed by an understanding of how criminals exploit firms whose platforms are used to target and socially engineer victims. We note some positive progress in this respect, with the proposed Online Safety Bill, containing positive steps towards placing requirements on sectors outside of financial services to take responsibility for preventing harm, including fraud – but more

---

<sup>2</sup> Fighting Fraud: Breaking the Chain', House of Lords: Fraud Act 2006 and Digital Fraud Committee Report, Nov 2022 – pg. 162, para 59.

must be done to ensure that a wider proportion of the scams ecosystem is held accountable, and liable, for the part they play.

An important next step would be the Government's appointment of a 'Fraud and Scams Lead', responsible for designing and delivering a comprehensive framework across Government, regulators, and industry, aligning existing activities across sectors, identifying gaps that require further action, and setting clear responsibilities on designated entities to enforce that action. We would therefore encourage the PSR to work with industry on communicating to Government the importance of mandating requirements and placing accountability on the wider scams ecosystem, and offer our industry's support in how best this can be achieved to reach our collective aims of reducing fraud and scams.

### **PSR to consider unintended consequences of their proposals**

Turning to the specifics of the PSR's proposed mandatory reimbursement rule, we would encourage the PSR to consider the following unintended consequences, and how they might each be mitigated, when finalising the rule and its implementation:

- **Increase in 1<sup>st</sup> party fraud** – Criminals are likely to capitalise on the mandatory reimbursement rule, exploiting the system. This may also create a new money laundering technique. Furthermore, we may see some consumers make scam claims, rather than raising purchase disputes with legitimate merchants.
- **Increase in volumes of scams** – Some consumers will take less care over certain payments, particularly regarding purchase scams and investment scams, due to the reimbursement fallback (aka 'moral hazard').
- **More money funding the criminal economy** – Focusing only on reimbursement, not prevention, will have an effect of more money being channelled to criminals. Fraudsters may also further target UK victims for these scam types, recognising that there is likely to be less consumer caution due to the reimbursement fallback, versus other markets.
- **Financial inclusion impacts** – Firms could place tighter controls at account opening, including possible assessment of a customer's scam claim risk, based on previous claim history. It could also lead to other consequences such as the creation of differing levels of customer access to (and speed of) payment options, and potentially refusal to make payments to certain jurisdictions, or to and from certain consumers or businesses.
- **Impact on legitimate payments** – Firms will likely introduce increased friction into FPS payments, which would reduce the utility of this payment method and the current consumer experience. Firms will inevitably also start delaying and blocking FPS payments (both sending and receiving) more frequently, in order to manage their risk. This will have an impact on a number of legitimate payments due to 'false positives', which could cause disruption to consumers and businesses, including for significant time-critical purchases such as making investments, and transferring housing deposits to solicitors.
- **Impact on provision of indirect access services** – The implementation of mandatory reimbursement through scheme rules, as proposed, would place significant burden and increased risk on Indirect Access Providers (IAPs), effectively resulting in them taking on the role of a pseudo-regulator for their indirect access clients, as well as a potentially open-ended credit risk.

### **Our recommendations for implementation, to drive consistent and good outcomes**

Smooth and consistent implementation of the new rule will enable it to be positively received by consumers, consumer groups, and the media. It will help reduce any short-term confusion or

customer detriment that could be caused through inconsistent application across the industry, which otherwise could result in bad outcomes leading to more cases being taken to the Financial Ombudsman Service (FOS) and/or through the Courts. We would therefore encourage the PSR to consider the following recommendations for implementation:

- **Reconsider the use of ‘gross negligence’ as the consumer caution exemption, instead requiring a greater degree of consumer responsibility (see responses to Q1 and Q4)** – The PSR should reconsider its proposal to use ‘gross negligence’ as the benchmark for consumer activity, below which they will not be reimbursed. Consumers must be required to exercise care in relation to the payments that they instruct. Use of ‘gross negligence’ would effectively absolve the consumer from their responsibility to apply sufficient caution when making a payment, and would remove the important role that the customer can play in preventing the scam. The consumer caution exemption must imbue the role of the consumer with responsibility and self-care, in particular for certain payment types such as purchases and investments. Absence of this sufficient standard of care heightens the risk of ‘moral hazard’, which is unacceptable in these circumstances. If, however, the PSR does proceed with the use of gross negligence, then to avoid inconsistency, confusion, and customer detriment at the outset, the PSR should properly and with sufficient granularity define gross negligence, including providing example scenarios of when a customer was or wasn’t grossly negligent. This would enable PSPs, consumers, and the FOS to better understand the responsibilities of all parties, and would deliver more consistent outcomes across the industry.
- **Provide greater consistency (raised throughout, including responses to Q1, Q3, Q4, Q7, Q8, Q10, Q11, Q18)** – e.g., when setting the time limit for making a claim, and potentially an excess, we would encourage the PSR to require all firms apply these consistently across the sector. We would recommend the PSR removes the minimum threshold proposal altogether. We believe that consistency for consumers will be extremely important in ensuring that they understand the new rule, and to ensure that they receive consistent outcomes. Allowing for relatively minor changes/nuances in approach by PSPs (such as slightly lower excesses or thresholds, and slightly different time limits), could cause confusion on the part of the consumer. This aligns to our recommendation for the PSR to place Directions on all PSPs (below), so that there is a single, clear set of defined rules that *all* PSPs must adhere to.
- **Effectively communicate the new rule, and likely impact on payments, to consumers (see response to Q1)** – We would encourage the PSR to effectively communicate the new reimbursement rule to consumers, including outlining what continues to be expected of them when taking caution over making payments. This awareness campaign should also educate and inform consumers to expect that legitimate payments will be impacted, and that there will be increased friction and delays to a number of payments (both outbound and inbound) – as a necessary step to prevent scams and protect consumers. This will help to avoid consumers being surprised and frustrated by payment delays, which would otherwise lead to increased complaints and potential negative sentiment towards the introduction of this new rule.
- **Provide greater clarity and definition regarding the rule and the scope (see response to Q3)**– including outlining specifically which payment is a scam payment in scope of the reimbursement rule (e.g., the payment that leaves a legitimate customer account and goes to an account controlled by a fraudster). The PSR should also clarify how complex/different types of scam claim must be treated under the rule, to provide consistent outcomes for victims. This should include clarity regarding how the rule applies for multi-generation scams, hybrid scam claims, Ponzi schemes, Open Banking payments, cases with multiple receiving banks, crypto scams, and cases where there is a repeat victim. We offer several examples, considerations and recommendations within our consultation response.



- **Set a ‘start date’ (see response to Q3)** – The PSR should set a ‘start date’ from which point if a consumer is scammed, they can make a claim under this rule. This start date should be clearly publicised when the final requirements are issued – so that consumers, PSPs, and the FOS have absolute clarity regarding whether a scam claim is to fall within this new rule. This will avoid any uncertainty over retrospective claims.
- **Extend the 48-hour reimbursement requirement (see response to Q11)**– We support the PSR’s view that there should effectively be a two-tier approach that encourages PSPs to reimburse the majority of scam claims in a timely manner, but that also enables PSPs to work to an extended reimbursement timeline in certain, more complex cases. However, we would encourage the PSR to consider a longer initial investigation period than 48 hours, which we believe is not an achievable timeline to assess whether a scam claim is valid, and whether the scam claim warrants further investigation into 1<sup>st</sup> party fraud or gross negligence. We would recommend setting a 5 working day reimbursement requirement for the ‘simpler’ scam cases (for example those that have one sending and one receiving bank, and a simple Modus Operandi (MO)). However, for more complex cases, PSPs should be able to work to an extended investigation timeframe, for example high value cases, cases with multiple payments across multiple receiving PSPs, cases where law enforcement are involved and cases where there is limited consumer cooperation in the investigation.
- **Place Directions on all PSPs, rather than Pay.UK changing scheme rules (see response to Q18)** – The PSR highlights a number of implementation challenges with its proposed approach of requiring Pay.UK to amend scheme rules, including current governance of Pay.UK needing to seek consensus of members to change rules; inability to apply FPS rules to indirect access PSPs; limited ability to enforce FPS rules. These challenges would be overcome if the PSR places Directions on all PSPs (including indirect access PSPs), in a similar manner to the approach taken for Confirmation of Payee. Pay.UK could continue to play a role in operationalising the reimbursement requirement, but the PSR’s Directions would mandate the consistent requirement across all PSPs and would reduce the significant burden and risk that would otherwise be placed on Indirect Access Providers. This would also serve to future-proof the rule for new entrants, and the transition to the New Payment Architecture (NPA).

We would encourage the PSR to consider the above unintended consequences, as well as our recommendations for how some of these risks could be mitigated, through issuing clear, detailed, and consistent Directions to all PSPs in the market.

## Consultation Questions

### 1. Do you have views on the impact of our proposals on consumers?

#### Overall, positive for scam victims and vulnerable customers

Overall, we recognise that this proposal could provide a number of positive outcomes for the victims of scams. Firstly, it will inevitably increase the number of victims who recoup their financial losses when falling victim to a scammer, irrespective of who the customer banks with. That being said, scam victims do not only suffer financial loss. They also suffer significant emotional detriment, and potentially develop a lack of trust in the digital economy. These impacts will continue long after the scam has taken place, regardless of whether they are reimbursed. The emphasis therefore must continue to be on how we can prevent scams from taking place in the first place, not only on

reimbursement. Measures must be taken to effectively prevent social engineering that scammers undertake by exploiting known vulnerabilities across a range of sectors, to trick consumers into making seemingly legitimate payments that can often evade bank detection – including phishing and smishing, number spoofing, fake websites, fake social media profiles, fraudulent adverts etc. As outlined above, we do not believe reimbursement alone will move the dial on scam prevention, and therefore a continued focus on prevention by financial services providers, as well as wider cross-sectoral efforts, are needed.

The PSR’s proposal also serves to support vulnerable customers, who can be more susceptible to falling victim to a scam, and therefore need additional considerations put in place to ensure they are supported, and in this context are effectively guaranteed reimbursement if they suffer financial loss from being scammed.

### **Potential for more consistent outcomes – if implemented with greater consistency and clarity**

The mandatory reimbursement rule also has the *potential* to drive more consistent outcomes for consumers when making FPS payments, but only if certain implementation issues are ironed out upfront. The primary item is the need for the PSR to define (and provide a number of examples of) gross negligence, which is imperative to achieve a broadly consistent industrywide approach from the outset. By leaving the definition unclear, and allowing it to be defined over time through case law and FOS decisions, this will inevitably create a period of inconsistency, where PSPs interpret the rule differently and consumers do not receive good outcomes – a repetition of the first couple of years of the CRM Code, where disparity in implementation greatly impacted the credibility of the Code, and made it harder for consumers to understand. A clearer definition of ‘gross negligence’ would be far more positive for consumers, who do not want to have to go to the FOS or through a lengthy court process in order to have PSP decisions overturned. It would also enable consumers to better understand what is expected of them when making a payment, and would drive greater standards of warnings and preventative action from Sending PSPs, as PSPs would have more clarity regarding what is required of them and their customer, and more assurance that the investment they make in preventative action will result in a reduction of reimbursement losses.

The PSR should also consider what happens when a customer and their PSP reach an impasse over a payment, with the PSP believing it is a scam (and therefore intervening e.g., through stopping the payment, speaking with the customer, invoking banking protocol etc), and the customer being adamant that the payment needs to be made. This may ultimately have to result in account closure, if the PSP cannot get comfortable that the payment isn’t a scam, and if the customer remains insistent on making the payment. Account closure doesn’t prevent the scam, however, it simply passes the risk across to another PSP. The PSR could consider, for example, allowing PSPs to use waivers<sup>3</sup>, which could help PSPs encourage customers in these relatively unique situations to take pause and really consider the payment they are about to make. This could provide the very last

---

<sup>3</sup> Waivers could be used in cases where the PSP is extremely concerned that the customer is trying to make a scam payment, but the customer is convinced that the payment must be made. The PSP has intervened accordingly to try to demonstrate to the customer why they believe the customer is being scammed, and may have even got law enforcement involved to assist in explaining this to the customer. However, if all efforts on the part of the PSP are ignored by the customer, and the customer still wants to proceed with the payment, then the PSP could issue the customer a waiver for them to sign, which effectively removes their right to reimbursement if it is a scam. The intention is to provide one final opportunity for the PSP to break the spell of the scammer, but also allows for the impasse to be overcome, as the customer can proceed with the payment – rather than the alternative which may require the customer to open another account through which to make this payment, if the PSP is not willing to take the risk of putting the payment through.

opportunity to break the scammer's spell, and prevent the scam payment from occurring. If the customer agrees to the waiver and is scammed, then this should be taken into consideration when determining (and defining) gross negligence. However, this doesn't fully resolve the issue, as the scam will still have taken place, and the money will have been sent to the criminal. Ultimately, there will need to be further consideration regarding how industry should approach these challenging impasse scenarios, to try to avoid poor customer outcomes (for example repeated account closures by multiple firms), whilst allowing firms to manage their liability risk.

The PSR should also consider what other simple implementation measures could help drive consistency and clarity for consumers, including defining a specific 'start date' so consumers know that if they are scammed on or after that date, they can make a claim under this rule.

The degree of consistency would, at this stage, only apply across FPS payments, and potentially 'on us' payments where the PSR has indicated that they would like PSPs to apply the reimbursement rule (albeit they are not mandated to). However, the scam reimbursement rule wouldn't extend to CHAPS or Bacs payments<sup>4</sup>, or card payments. Therefore, the PSR should aim to make the rule as clear and explicit as possible, so that consumers are best able to understand it, and take it into consideration when selecting their method of payment. The PSR should also consider whether, in the medium term, this new rule (and any corresponding increase in friction/intervention in FPS payments that firms implement to limit fraud risk) could drive a shift in fraudsters targeting payment types that are not covered by this rule (e.g., card payments). This could see a return of consumer detriment caused by scams, as consumers wouldn't receive reimbursement for scam payments made outside of FPS. Hence, our firm view that there needs to be much more coordinated effort across the wider scams ecosystem to prevent fraud and scams from taking place, rather than only focusing on reimbursement.

**However, there could be negative impacts for consumers that don't fall victim to a scam, which need to be clearly communicated**

There will also be a broader range of impacts on consumers as a whole (noting that the majority of consumers will not become a victim of a scam, and therefore won't benefit from this rule) – which should equally be taken into consideration. Firstly, firms will inevitably start delaying and blocking FPS payments (both sending and receiving) more frequently, in order to manage their risk. This will have an impact on a large number of legitimate payments due to 'false positives', which could cause disruption to consumers including for significant time-critical purchases such as making investments or transferring housing deposits to solicitors in advance of purchasing a home. Furthermore, in the medium term, we may see firms taking an insurance-style approach to risk of onboarding a customer, e.g., through asking for information about previous claims history, which may result in some victims finding it harder to open an account or maintain use of certain services within an account. We would therefore encourage the PSR to undertake further consideration as to the impact of these proposals on consumers in the wider sense (not just the benefits for consumers who have fallen victim to a scam). We would also encourage the PSR to effectively communicate the new reimbursement rule to consumers, including outlining what continues to be expected of them when taking caution over making payments, and informing them of the likely impact on legitimate payments, including through increased friction and delays to a number of payments (both outbound and inbound). Publicly informing consumers about this significant step that the PSR is taking, with the aim of preventing scams and protecting consumers, will help to avoid consumers being surprised

---

<sup>4</sup> In 2021, £22.5m scam payments made via CHAPS and £20.4m by BACS.



and frustrated by payment delays, which would otherwise lead to increased complaints and potential negative sentiment towards the introduction of this new rule.

### **Lack of clarity over consumer responsibility will lead to moral hazard, and more scams**

The PSR's proposal to use 'gross negligence' as the consumer caution exemption effectively removes customer responsibility for taking care when making a payment. Customers will receive a full reimbursement (less £35 excess, if applied), removing the concept of 'partial reimbursement' as per the CRM Code, where both the Customer and the PSP(s) take a degree of responsibility. This near complete removal of consumer responsibility over their payment is an unprecedented move which could have significant implications, including 'moral hazard'. It is unclear (due to the lack of definition of gross negligence) what the expectations will be on consumers to protect themselves from being scammed – but a number of preventative measures put in place (including effective and timely warnings) are in the CRM Code to try to 'break the spell' of the scammer, which inevitably require a role to be played by the customer, in taking some caution over the payments they make. We would not want to see the PSR's proposals leading to an increase in customers being scammed, as they for example make riskier purchases from unknown websites without checking reviews, because they know that they will receive reimbursement if it is a scam; likewise with too-good-to-be true investment 'opportunities'. Effectively eliminating the role of the customer in taking caution could lead to significantly more harm, leading to more victims being scammed, and more funds reaching criminals. As noted in the recent House of Lords report on 'Fighting Fraud: Breaking the Chain': "While we recognise the case for mandatory reimbursement of victims of APP fraud, we are concerned that a blanket reimbursement policy may lead to increased levels of moral hazard and fraud, and the perception that it is a 'victimless crime'. In some cases, it may even lead directly to new avenues for APP-reimbursement frauds."<sup>5</sup> The House of Lords Committee recommends "further exploration on the long and short term risks of this approach is required"<sup>6</sup>, before this unprecedented step is taken.

Whilst the PSR note that there is little evidence regarding moral hazard in this context, we would reflect that this is due to the unprecedented nature of this rule. However, there is some evidence regarding consumer sentiment and perspectives on scam reimbursement, that could be further explored through consumer research. There has been significant media attention surrounding scam pay-outs, with a number of journalists stepping in to assist customers in seeking reimbursement or overturning PSP reimbursement decisions. Reader commentary has often indicated an aversion to placing full responsibility on banks to reimburse, recognising that consumers should take some responsibility over their payments, including taking caution to protect themselves from being scammed. In light of this trend in consumer sentiment, Barclays undertook qualitative customer research<sup>7</sup> to better understand consumers' perspectives regarding their responsibilities when it comes to making payments, and the risk of being scammed. The research findings included:

- Consumers felt they had a responsibility over their payment, including if they were scammed. Removing consumer responsibility was seen as a negative, as they perceive that responsibility aligns with control – something which people wanted to maintain.
- Banks should be custodians, looking after a customer's money, but not how they spend it.

---

<sup>5</sup> 'Fighting Fraud: Breaking the Chain', House of Lords: Fraud Act 2006 and Digital Fraud Committee, Nov 2022 – page 162, para 57.

<sup>6</sup> Ibid, page 162, para 58.

<sup>7</sup> The research was undertaken for Barclays internal insight, and therefore has not been publicly published – however the research has been shared confidentially with the PSR.

- Banks' fraud and scam prevention efforts are welcome – however there is no expectation on banks to redress after 'self-inflicted' loss through a scam. Goodwill reimbursements were welcome in certain instances, especially for vulnerable customers.
- In regard to the 'moral hazard' concept – when asked what would happen if there were no customer responsibility (i.e., the banks would reimburse all scam cases):
  - o Some customers suggested that they would end up taking their eye off the ball
  - o Several more customers like to believe that they would still take as much care as they currently do – but they were convinced that other people wouldn't take care
  - o Either way – both groups were uneasy about the macro position that this could create, of unleashing widespread scamming.

We recognise that qualitative consumer research findings are based on a small number of interviews with real customers in order to obtain deeper insight into their thoughts on a specific topic, but it is limited in how far it can represent overall consumer sentiment. We would therefore encourage the PSR to undertake more comprehensive consumer research to consider whether consumers support the mandatory reimbursement rule as proposed.

### **Consider impact of Claims Management Companies on consumer outcomes**

Finally, we would encourage the PSR to consider what impact Claims Management Companies (CMCs) – as well as Solicitors/Law Firms acting as CMCs (collectively termed 'Third Parties')<sup>8</sup> - may have on consumers, and work with the FCA to consider how to limit this risk upfront. In their Dear CEO letter to CMCs (Oct 2020)<sup>9</sup>, the FCA identified multiple drivers of consumer harm from CMCs, including misleading, unclear and unfair advertising practices resulting in customers being misled about their claims; poor disclosure of pre-contractual information about fees and/or the availability of free alternatives to make a claim (e.g. the customer making the claim directly to their bank); unclear fee structure; poor service standards and a knock on impact of spurious claims resulting in slower processing and poorer outcomes for consumers. The PSR should ensure that the mandatory reimbursement rule is clear and simple for customers to understand, is applied consistently across all PSPs, and is well publicised – as this could help to ensure that consumers are aware of and understand the rule, including what is expected of them, and that they do not need to go through a Third Party, but instead can go directly to their bank to make the claim (for free). The PSR should also enable PSPs to insist that they deal with their customer directly (rather than solely via a Third Party) given the need for PSPs to gather customer testimony and evidence about the specifics of their unique scam claim, both to allow the PSP to determine whether the claim is applicable for reimbursement, but also so that the PSP can learn from the case and better understand evolving scammer MO, to help prevent similar scams on other customers.

---

<sup>8</sup> CMCs are regulated by the FCA. However, we are seeing increased Solicitors/Law Firms acting as CMCs (marketing, signing up customers, representing claims and complaints etc), who are regulated by the Solicitors Regulation Authority (SRA). SRA regulated firms are not yet restricted by a fee cap, which has resulted in a shift in CMCs either transitioning to become a law firm, or working together with one. Hence, the need to ensure that both CMCs, and Solicitors/Law Firms – collectively Third Parties – are considered in this context.

<sup>9</sup> Dear CEO letter - Portfolio Strategy: Claims Management Companies (CMCs), FCA, Oct 2020 - <https://www.fca.org.uk/publication/correspondence/claims-management-companies-portfolio-letter.pdf>

## **2. Do you have views on the impact of our proposals on PSPs?**

### **Increased financial liability for reimbursement**

The implementation of the rule will have considerable impact on PSPs. As the PSR outlines, PSPs will inevitably see an overall increase in their financial liability for scam victim reimbursement. However, for many PSPs who already have significant fraud and scam detection and prevention measures in place, this increased financial liability will not incentivise significantly increased investment in further detection capabilities (as the PSR intend) – because many PSPs are already implementing a wide range of controls to detect and prevent scams. In many cases, the customer has been socially engineered and is under a fraudster’s spell, resulting in them being convinced that they are making a legitimate payment. It is often not possible for a PSP to identify a scam payment from a legitimate payment, and even the most effective and timely warnings may not break the spell of the scammer. It is for that reason that it is imperative that policymakers mandate greater controls and preventative measures are applied across the wider scams ecosystem, to reduce the prevalence and effectiveness of social engineering tools. In the CRM Code, there has been the concept of ‘no blame’, whereby both the PSPs and the consumer did all they could, but the scam still took place. Often for these cases, blame lies elsewhere in the ecosystem, and therefore these other players must be held more accountable and liable for the role they play, and for contributing to reimbursement.

### **Impact on PSP risk appetite when onboarding consumers and providing indirect access services**

The mandatory reimbursement rule could effect change in PSPs’ risk appetite, with the possibility of a shift towards an insurance-style approach to risk when onboarding a customer, e.g., through asking for information about previous claims history. This may result in some victims finding it harder to open an account or use certain services within an account. It also could result in sponsor banks (Indirect Access Providers (IAPs)) changing their risk appetite for onboarding indirect access clients, depending on whether the PSR require IAPs to effectively underwrite and become pseudo-regulators of their clients (see response to Q18).

We would encourage the PSR to place Directions on all PSPs, rather than requiring Pay.UK make changes in scheme rules. This will allow for a much smoother and more consistent implementation, as all PSPs (direct and indirect) would be required to adhere to the same rule, with the same oversight and enforcement. We would also encourage the PSR to define gross negligence, set a ‘start date’ so that there is clarity on whether a scam claim would fall in scope, and extend the 48-hour reimbursement requirement. These measures will allow for a smoother implementation process for PSPs, leading to more positive consumer outcomes from the outset. It would also provide more clarity to the FOS regarding how to interpret and apply the rule.

There will also need to be improved interbank communications, to enable prevention and detection without even needing to speak to the customer. CIFAS Digital Fraud Checks, for example, would support this, where firms are mandated to respond within a short window, to confirm whether the payment is destined for the correct account.

### **More clarity required regarding Open Banking Payments**

We would request the PSR clarifies how they envisage the rule applying to Open Banking payments, including clarifying which party (/parties) is the Sending PSP, and which is the Receiving PSP(s), holding liability for reimbursement. In an Open Banking payment, there are more PSPs in the single payment chain (including the Payment Initiation Service Provider (PISP), the Account Servicing



Payment Service Provider (ASPSP) and the Receiving PSP). It is unclear how the 50:50 liability split would be applied in these cases, to ensure that all of these PSPs are accountable for fraud prevention, and are liable for their share when a scam takes place. This should be considered in the context that we are already seeing proportionately higher rates of fraud in Open Banking payments, than with payments made through our direct channels. Furthermore, an important part of scam detection and prevention is based on the Sending PSP knowing information about the payment (including the payment purpose), so that they can provide effective and timely scam warnings to the customer, to try to 'break the spell' of the scammer, and also to use this information in their fraud detection and prevention engines. In the case of Open Banking payments, the PISP is not mandated to share this data with the ASPSP, and therefore in many cases, the ASPSP does not have the information it needs to effectively detect fraud. Furthermore, the Customer Experience Guidelines (which are mandatory for the CMA9 to follow) place restrictions on an ASPSP's ability to have control over the payment journey, including placing effective and timely scam warnings. These issues therefore need addressing, to ensure that Open Banking payments do not further become a target for fraudsters, who seek to avoid the controls and warnings that are otherwise in place in FPS payments made through ASPSPs' direct channels. This would include mandating PISPs to share the necessary data with ASPSPs so they can effectively detect and prevent a scam, updating the Customer Experience Guidelines to allow ASPSPs to put in place effective and timely scam warnings into the customer payment journey, and incentivising PISPs to put in place necessary fraud prevention, by sharing the 'Sending PSP' liability for reimbursement – as in effect both the PISP and the ASPSP share the role of 'Sending PSP'. All participants in the Open Banking payment chain need to be appropriately incentivised and accountable to detect and prevent fraud and scams, and therefore the model needs to be set up appropriately to ensure this is the case.

#### **Potential for increased Breach of Mandate claims**

Sending PSPs will need to balance their liability risk, when they suspect a payment could be a scam. If a Sending PSP delays a 'suspicious' payment which turns out to be genuine this may cause the Sending PSP to be liable for any loss incurred due to the payment not having been made. This is of particular concern where payments are time-critical and consequential losses may flow from the breach e.g., a house purchase deposit, or an investment. In order to limit the impact on all legitimate payments (e.g. PSPs putting in place standard delays across all payments and including this in their T&Cs), the PSR could consider introducing a process akin to the reporting obligations under the Proceeds of Crime Act (POCA), whereby firms would be able to lodge a report (similar to a DAML SAR under POCA), allowing them to ringfence the funds until/unless the PSP is satisfied that the payment is not a scam, or until they are able to make further attempts to 'break the spell' of the fraudster, if the PSP continues to suspect it is a scam. If the PSP's concerted efforts to break the spell do not work, and the customer continues to push for the scam payment to be made, then this could be grounds for the PSP to determine consumer gross negligence, removing liability for the scam payment from the PSP, as well as providing a defence to any breach of mandate, or loss of opportunity claim against the PSP.

#### **Consider impact of Claims Management Companies on effective implementation**

Finally, we would encourage the PSR to consider upfront how Claims Management Companies and Third Parties may impact the effective implementation of this mandatory reimbursement rule, and how to support PSPs in enabling them to deal with CMC claims effectively, so as not to detriment the wider set of consumers making claims. As evidenced through PPI claims, the FCA addressed a

number of concerns about CMCs in their Dear CEO letter (Oct 2020)<sup>10</sup>, which highlighted that some CMCs were failing to undertake sufficient checks and/or collect relevant information about a claim, resulting in spurious claims slowing down the processing for all consumers, leading to poor customer outcomes. The PSR should therefore consider whether there could be certain exceptions applied for CMC and Third Party cases, such as extended timeframes, and a minimum bar of evidence unique to each customer case (noting that, in the majority of cases, each scam case is unique and specific to the action undertaken by the customer – therefore should not result in CMCs making significant volumes of identical claims across many customers). Additionally, as above, enabling PSPs to insist that they deal with customers directly (rather than solely via a Third Party) would help reduce these risks.

### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

The PSR are clear on the overarching scope being just consumer FPS payments (including microenterprises and small charities), and we agree that whilst the PSR isn't at this stage able to mandate this rule for on-us payments, that firms should be encouraged to apply the rule for these payments. However, there are a number of areas relating to 'scope' that would require benefit from further clarification, to provide consistency and clarity for consumers and the industry.

#### **Need more clarity regarding which is the scam payment in scope of the rule**

Firstly, we would encourage the PSR to clarify which payment (specifically) is the scam payment that can be claimed for reimbursement under this rule. In many cases, a scammer may convince a customer to first move money to a 'safe account' or an e-money account (in the customer's own name), and then the scammer encourages the customer to move the money from that account into an account controlled by the fraudster (likely a mule account). The money will then likely be moved out of that mule account at the direction of the fraudster, and so on. To provide clarity to industry (both Sending and Receiving PSPs), as well as to customers (regarding who to make their claim to), the PSR must be clear on which of these payments is the 'scam payment' that can be claimed under this rule. This will limit the risk of duplicate claims (where the customer could make a claim for both the 1<sup>st</sup> and 2<sup>nd</sup> payment in the above scenario, as they were manipulated into making both of these payments by the fraudster, but were only actually scammed out of the money once – through the 2<sup>nd</sup> payment when the money was sent to an account controlled by the fraudster). This clarity would also reduce some of the increased risk of 1<sup>st</sup> party fraud, that is likely going to be increased through the introduction of this rule. It will also significantly limit disputes between PSPs regarding who is liable as the Sending and Receiving PSP in this case. We would encourage the PSR to confirm that the 'scam payment' in scope of reimbursement is the specific payment that is made from an account held by a legitimate victim, to an account held or controlled by a fraudster. We will address this further in response to Q15.

#### **Need clarity regarding FPS payments outside of PSR's geographical jurisdiction**

The PSR should clarify that an FPS Payment Originated Overseas (where the inbound payment is from a different jurisdiction) is out of scope of this rule, given the significant operational complexities associated with applying this outside of the PSR's jurisdiction. Confirmation of this

---

<sup>10</sup> Dear CEO letter - Portfolio Strategy: Claims Management Companies (CMCs), FCA, Oct 2020 - <https://www.fca.org.uk/publication/correspondence/claims-management-companies-portfolio-letter.pdf>



scope would help drive consistency across the market, and would align to our understanding of the PSR's intention that this would cover only domestic-to-domestic payments. The PSR should also clarify the approach to Jersey, Guernsey, Gibraltar, and Isle of Man, in terms of how the liability for reimbursement of a scam payment sent via FPS from a UK Sending PSP to a Receiving PSP in one of these locations, should be allocated and implemented. We would recommend simply confirming that the reimbursement rule does not apply to any payments sent to or received from overseas.

### **Recommend setting a 'start date' for scam payments**

One area of scope that remains ambiguous is where the PSR states that the rule would apply to APP scams 'where the most recent payment was authorised after our regulatory requirements came into force'. This is ambiguous, and could leave PSPs with open-ended liability for long-running scams, made up of numerous payments, potentially dating back to several years before the rules came in. We would therefore encourage the PSR to set a 'start date', from which point if a customer makes a scam payment on or after that date, then it would be covered by the rule. This would provide certainty and clarity for all relevant parties (Sending PSP, Receiving PSP, customers, and the FOS). We would encourage the PSR to communicate this 'start date' clearly in any publication about the new rule, so that customers are appropriately informed. The simplest and clearest option would be to set the 'start date' as the day on which the rule comes into force. This would help drive consistency across the market, and would limit any questions on the part of the consumer/consumer groups/FOS if any other arbitrary date is chosen<sup>11</sup>.

### **Need to consider how to prevent systemic abuse of the new rule**

We support the PSR's decision that this rule should not apply to civil disputes, where the customer has paid a legitimate supplier for goods or services but has not yet received them, or they are defective in some way. It should be noted therefore that, in addition to gross negligence and 1<sup>st</sup> party fraud, a Sending PSP will also have to consider and determine whether the claim is in fact a legitimate scam claim, or a civil dispute which would not be in scope of the rule. This qualifying of the validity of a claim would take place up front, and would result in certain scam claims not being progressed (therefore resulting in no reimbursement – although the customer should, in the case of purchase disputes, take the matter forward with the legitimate merchant to seek a refund). We envisage that the introduction of the mandatory reimbursement rule would see the volume of buyer-seller disputes incorrectly being submitted by consumers as scam claims would increase, as consumers may perceive this to be the best route to get their money back if they are dissatisfied with a merchant's service.

Furthermore, the PSR should consider how industry can limit the risk of systemic abuse and increased 1<sup>st</sup> party fraud, for example through multiple scam claims. Industry may, for example, seek to share data (in a similar manner to CIFAS data and insurance claims data sharing), regarding claim history. This would enable firms to share intel regarding likely fraudsters abusing the system. However, there should also be a recognition that this could cause detriment for certain consumers who may legitimately have been scammed multiple times and therefore have made multiple claims,

---

<sup>11</sup> For example, if the PSR were to choose the date that falls 13-months prior to the rule coming into force, to align with their proposal regarding the 13-month time-limit for a claim, then this could be ambiguous for customers of any PSPs who choose to apply a different time limit for claims. If the PSR were to not set a 'start date' at all, and instead leave it to PSPs themselves to interpret the rule, then this would likely lead to inconsistent approaches being taken across the sector, causing customer confusion and detriment, and likely resulting in an increase of cases being taken to the FOS. A simple and consistent approach should therefore be applied.

but may find it difficult to open a new account with a PSP due to their scam claim history (in a similar manner to how some consumers may find it difficult to access certain insurance products due to claims history). This is one driver behind a potential financial inclusion risk, as outlined previously.

#### **Recommend clarifying how the rule may be applied differently based on customer and scam types**

The PSR should also consider whether the definition of the scope for ‘microenterprise’ is appropriate and proportionate in this context of APP scam reimbursement. It should be expected that firms of a certain size (for example with 5 or more employees) should be better equipped to take caution over making payments, and to protect themselves from being scammed, than individual consumers. The PSR could therefore consider amending the definition of ‘microenterprise’ for this context, or could offer more clarity in how a consumer caution exception may be applied differently to microenterprises than to individual consumers.

Finally, the PSR should consider and clarify how the reimbursement rule would apply for certain specific types of scams, for example Ponzi schemes. The PSR should also clarify how the reimbursement rule would apply for hybrid cases, for example claims where both a fraud and a scam has taken place (due to some payments within a claim being APP scams, and some being unauthorised frauds). It is unclear at this stage whether only the scam payments within this hybrid claim would fall in scope of the reimbursement rule and therefore liability is shared 50:50 between Sending and Receiving PSP for these payments, but the unauthorised frauds would be liable for reimbursement only by the Sending PSP, under the PSRs2017. It should also be noted that hybrid claims are often complex, and it can be challenging to determine which payments were unauthorised fraud, and which were authorised push payment scams – with the customer not always having the clarity on what has actually occurred.

#### **4. Do you have comments on our proposals:**

- a. that there should be a consumer caution exception to mandatory reimbursement**
- b. to use gross negligence as the consumer caution exception**
- c. not to provide additional guidance on gross negligence?**

The consumer plays a vital role in preventing a scam from taking place – reading the timely and effective warnings that are presented to them, considering the outcome of a Confirmation of Payee (CoP) check, and pausing to think whether they are being scammed. By effectively absolving customers from any responsibility over their payments, the industry runs the risk of significant increases in scams taking place, as consumers lower their guard due to a guaranteed fallback if a situation (e.g., a too-good-to-be-true investment or purchase) is actually a scam. Therefore, we support the concept that there must be a consumer caution exception to mandatory reimbursement.

However, we do not support the use of gross negligence for this purpose. The standard of care expected of customer in how they manage their own financial affairs and well-being cannot be set so low such that consumers can – in effect – abdicate personal responsibility in this way. If gross negligence is used as the customer caution exemption, it will have little to no impact in practice, especially for certain scam types (see Sidebar for further context). This is because it will be difficult for a financial institution to prove that a customer has been grossly negligent based on the information that the customer opts to provide with their claim, and therefore it will effectively absolve consumers of the important role that they play in preventing the scam. The removal of the

role to be played by customers and the agency customers have to prevent themselves becoming a victim of a scam will, in all likelihood, result in customers lowering their guard further in the knowledge that, even if they could be viewed as negligent, their bank will still be required to reimburse them.

We would therefore encourage the PSR to undertake detailed consumer research to understand where consumers feel an appropriate level of consumer caution should be set. A number of principles should be clarified to consumers, for example that consumers should pay attention to the warnings provided by their bank, and any CoP output presented to them, and the consequences of them not doing so.

If gross negligence is used as the consumer caution exception, we consider that the PSR should provide guidance around what constitutes gross negligence. The PSR should establish a working group with industry, the FOS and consumer organisations to help develop this.

---

#### SIDEBAR CONTEXT: FRAUD AND SCAMS

As the PSR notes, gross negligence is the consumer caution exception to PSP liability for unauthorised fraud under Section 77(3) of the PSRs 2017. However, there is a clear difference between unauthorised fraud, and authorised scams, that requires consideration when determining the extent to which a consumer must take care, and therefore the necessary consumer caution exception that needs to be in place to ensure that.

**Unauthorised Fraud:** In these cases, the customer was not involved in making the payment transaction – it was undertaken by a fraudster. The customer therefore cannot be expected to be able to play much of a role in preventing the fraudulent payment from taking place (as they are not present or aware of the transaction until after the event), other than the very high bar of ‘gross negligence’. To provide examples of how this exception has been applied in practice, the FOS has determined that customers have acted with gross negligence by: leaving all of their banking security information in their mother’s house<sup>12</sup>; sharing their PIN code with someone else<sup>13</sup>; and carrying a card together with its PIN code<sup>14</sup>.

**Authorised Push Payment Scam:** In these cases, the customer has instructed and authorised the payment themselves, and has directly issued the bank with a mandate to make the payment. The customer therefore has a much larger role in the context of a scam, and therefore there should be a greater expectation of consumer responsibility to take care over the payments that they instruct. In this way, we can see the use of ‘gross negligence’ as a test – adapted from the unauthorised fraud example – is inappropriate. The extent to which the consumer should take care should be directly related to the context of the payment, and the ‘scam type’. There should be varying degrees of expectation on the part of the consumer, for example:

- **Purchase Scams:** In these cases, the customer plays a considerable role in selecting the good or service that they want to purchase, and they make the payment. In some instances with purchase scams, the customer may be choosing the cheapest available option, from an unknown website, and hasn’t checked any reviews or made any attempt to determine

---

<sup>12</sup> <https://www.financial-ombudsman.org.uk/decision/DRN0113912.pdf>

<sup>13</sup> <https://www.financial-ombudsman.org.uk/decision/DRN-3418228.pdf>

<sup>14</sup> <https://www.financial-ombudsman.org.uk/decision/DRN4565989.pdf>

whether the purchase is legitimate. They may also have ignored the direct instructions of the platform / website when making the payment, for example a number of car trading websites provide customers with a simple checklist to follow, for example that they should view and test drive a car prior to purchasing, and that they should not make an advance deposit payment via bank transfer (only credit card, if a deposit is needed). If the customer ignores these warnings and is scammed, then they are not liable for a refund through the car trading site. The customer's actions (or inaction) in this context should be considered when determining whether the customer should be reimbursed, or whether they didn't take sufficient caution to ensure that the purchase was legitimate, and not a scam.

- **Investment Scams:** Similar to purchase scams, the customer plays a considerable role in making a decision to invest in an opportunity. These may often be 'too-good-to-be-true', but the customer has actively taken the decision to make the investment regardless. There is often considerable opportunity for a customer to take care in these cases, by undertaking some due diligence ahead of making an investment. Again, the customer's actions (or inaction) should be appropriately considered in the context of determining whether the customer should be reimbursed.
- **Impersonation Scams:** These scam types are very different to purchase and investment scams. The customer is often actively being tricked by a fraudster into believing that something has occurred that requires them to make a payment (whether that is a friend or family member in need, the threat of legal action by HMRC, or the risk of losing all of their money out of their bank account). The customer has not actively sought to make a purchase or investment that may be too-good-to-be-true— they have been tricked into making the payment, often under considerable pressure. In these instances, it is much more difficult for a consumer to take caution, due to the pressure and web of lies they are being convinced to believe. There aren't review websites to check, and fraudsters often use sophisticated technical tools and techniques to encourage the customer to believe the situation. Therefore, in this context, the consumer caution exemption could be set at a high bar, as there is much less a customer could be expected to do to prevent themselves from being scammed.

---

Each scam type, and each scam, is a unique situation with a unique set of circumstances that require consideration, and therefore it can be extremely complex and challenging to determine whether the consumer took sufficient caution when making a payment. The PSR's proposal to use (but not define) 'gross negligence' as an extremely high bar presents a number of challenges, that needs further consideration:

- The lack of any definition or examples will lead to inconsistent application, causing confusion and distress to consumers. Recognising that any definition will still require a degree of interpretation, the PSR should consider how to provide greater clarity over their expectations for when a PSP should and shouldn't determine gross negligence, and therefore reimburse the victim. This could be done through the use of examples or scenarios, which will help bring much needed clarity for consumers, industry, and the FOS (in a similar way to how the FCA has issued guidance with examples of good and bad practice, alongside the Consumer Duty, for similar reasons). The FOS could be asked to provide (anonymised) examples of cases where it has ruled against the customer (e.g., has deemed the customer did not take sufficient caution), to help develop this set of examples. Barclays would also be happy to contribute, as part of the aforementioned working group, anonymised examples of scam cases for consideration as to whether a gross negligence ruling would have been appropriate in those cases – for example where the bank has been extremely explicit to the customer not to make a certain payment due to our strong

expectation that it is a scam, and other cases where the bank has requested law enforcement steps in to speak to the customer, in an attempt to break the spell of a scammer.

- The degree of consumer caution, or 'gross negligence' definition, should vary by scam type and complexity (as outlined in the Sidebar). What is expected of a consumer when they are tricked into believing the scammer to be a loved one or person of authority, in a high-pressure situation, should be very different to what should be expected of them when they are choosing to make a £100,000 investment. The level of due diligence and care expected of a consumer when making each of these payments should be different, including in response to any interventions from their bank. In effect, the bar for 'gross negligence' should be lower for the high value investment claims, as customers should be expected to do some due diligence before investing/transferring such high value payments.
- Gross negligence should also vary by customer type e.g., we would expect a greater level of care to be taken by a business (microenterprise and charity) or a 'sophisticated and/or high net worth investor' such as a Private Banking or Wealth client, than by a retail consumer. Other contexts should also be considered when determining gross-negligence on a case by case basis, for example microenterprises and small charities should be out of scope for making romance scam claims (as this would not be a valid use of business funds), and where a microenterprise is operating in an investment or financial capacity, they should be out of scope for investment scam claims (as these firms should be expected to have the capability and governance processes in place to protect themselves from this type of scam).
- Finally, we have a number of concerns with the PSR's suggestion to ultimately leave the interpretation of 'gross negligence' down to the FOS. The role of the FOS should remain that of an arbiter of single-issue disputes between firms and customers, applying decisions based on extant law and regulation – it should not extend to that of a quasi-regulator, defining rules, or taking decisions that could potentially have market-wide implications, for example because firms are required to apply FOS rulings in individual cases to all other cases of a similar nature. The PSR should encourage the FOS to liaise with them regarding any cases which may have wider impact, to ensure that the market and regulatory impacts of the FOS's decisions are properly assessed by the PSR, as the relevant regulator. This will help to ensure that the regulator's intents are applied clearly, without misinterpretation or overreach, thus providing a stable policy environment for firms and customers. We have experienced numerous examples of the FOS ruling inconsistently on very similar scam claims, and not applying decisions consistently with rules in place at the time (e.g., retrospective application of the standards within the CRM Code, for scams that took place prior to the Code launching). In order for the mandatory reimbursement rule to be applied consistently – and therefore most effectively to achieve good customer outcomes – we need clarity of the parameters for 'gross negligence', and the FOS needs to align their decisions to these. To further assist in achieving this, we would also encourage an independent appeals process for FOS decisions be established which allows for the scrutiny of the decisions made in respect of wider implication cases. This would move away from the adversarial judicial review process and allow the substantive merits of the decision to be addressed rather than the narrow grounds for judicial review currently.

##### **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We support the PSR's proposal to require reimbursement of vulnerable customers, even if they acted with gross negligence. At whatever point in an investigation PSPs identify a vulnerability, they should still have the opportunity to complete that investigation in full as this provides the PSP the

opportunity to support and educate their vulnerable customer, to try to prevent them from becoming a repeat victim.

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

Overall, we support the PSR's proposal of using the FCA's definition of a vulnerable customer, although this should be tailored/applied in the context of the vulnerability having an impact on the susceptibility of the customer to falling victim to a scam, and not other types of vulnerability that may mean their susceptibility is not hindered. This is because evidence of a vulnerable situation may not necessarily increase the likelihood of the customer falling victim to an APP scam, and equally a consumer may in normal circumstances not be deemed as vulnerable, but the timing and nature of the scam makes them vulnerable at that time.

**7. Do you have comments on our proposals that:**

- a. sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- b. any 'excess' should be set at no more than £35**
- c. PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

Barclays understands that the PSR's intention behind the excess is to encourage consumers to take caution over their lower value payments, and to prevent systemic abuse (e.g., civil disputes with merchants being put through as purchase scam claims).

Although we do not believe that the excess will impact consumer behaviour in the vast majority of cases, if the PSR continue with their proposal as outlined (e.g., with 'gross negligence' as the extremely high bar, and including purchase scams), then we support the inclusion of an excess. This will enable the PSR's theory to be tested, and the level and experience of the use of the excess should be considered in the post-implementation review, to consider whether it has adequately prevented customers taking less care over their lower value payments, and in preventing systemic abuse.

However, we would encourage the PSR to reconsider whether an excess correlating to a defined percentage of the total claim would better meet the intended outcome, of continuing to encourage customers to take caution over their payments. A 5% excess, for example, could still be a considerable amount in the context of large investment scams, and could therefore act as an incentive to ensure the customer takes caution over their investment payment. Noting the PSR's comparison to insurance excesses, this approach would be more akin to that taken in the insurance market, where excesses can act as a deterrent to systemic abuse and false claims – with excess amounts in the insurance market often in the region of hundreds of pounds, and tied to the likely potential size of a claim, in order to sufficiently act as a deterrent. A scam claim could vary significantly from tens of pounds, to millions of pounds, therefore a fixed amount does not work as appropriately – whereas a percentage amount would be more applicable.

Any excess outlined as part of this rule should be applied consistently across all firms, consumers, and cases, to provide much needed additional clarity regarding the reimbursement rule, particularly for consumers.

**8. Do you have comments on our proposals that:**



- a. **sending PSPs should be allowed to set a minimum claim threshold**
- b. **any threshold should be set at no more than £100**
- c. **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

Whilst we recognise that a minimum threshold of £100 could help PSPs limit the volume of lower value claims that they are investigating, we are concerned that the threshold could lead to negative outcomes. First and foremost, it is likely that this would prevent smaller scams from being reported, resulting in PSPs missing opportunities to identify scams that are taking place, and in particular identifying and closing the mule accounts that are receiving the scam payments – therefore limiting the opportunity to prevent money getting in the hands of criminals. Secondly, varying thresholds being applied across industry could create inconsistency, leading to customer confusion regarding the reimbursement rule. We therefore are of the view that the PSR should remove the proposal to allow minimum claim thresholds.

If the PSR does go ahead with the proposal, we believe that the PSR should set a specific threshold, rather than allowing PSPs discretion to determine the level (below £100) at which this is set, to ensure consistent application, and to prevent the latter negative outcome.

#### **9. Do you have comments on our proposal not to have a maximum threshold?**

We support the PSR's proposal not to have a maximum threshold, as applying a consistent approach across all PSPs will help to provide a degree of consistency and clarity in the rule for consumers, PSPs, and the FOS.

We would, however, encourage the PSR to consider how scam value is factored into consideration in the context of gross negligence determination. As per our response to Q4, we should expect consumers to undertake some due diligence / caution before making a high value payment. If the customer ignores bank warnings for these high value payments, then there should be more of a case for gross negligence.

#### **10. Do you have comments on our proposals that:**

- a. **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- b. **any time-limit should be set at no less than 13 months?**

We support the need to have a time-limit for claims, to ensure that there isn't an open-ended liability for PSPs. 13 months is a reasonable time limit, and aligns to other similar time limits in the industry (e.g., SEPA Direct Debit).

However, we would encourage the PSR to clarify their wording and approach, to ensure consistent outcomes are applied across the industry, for the benefit of clarity for consumers. For example, would encourage the PSR to set a 'start date' from which point if a consumer is scammed, they can make a claim under this rule. For example, if the consumer made a payment to a scammer on or after 20 September 2023 (an example 'start date') then that payment would fall under the reimbursement rule. Any scam payments made before the defined 'start date' should not fall under the reimbursement rule (although, as the PSR note, many consumers would still be able to make a

claim to their PSP e.g., under the CRM Code). A well-publicised 'start date' will provide clarity and consistency to consumers, PSPs, and the FOS, when it comes to the scope of the rule, which will help drive positive outcomes regarding this new rule.

**11. Do you have comments on our proposals that:**

- a. the sending PSP is responsible for reimbursing the consumer**
- b. reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We support the proposal (a) that the Sending PSP reimburses the customer, and then claims 50% back from the Receiving PSP, as this would likely create more clarity for the consumer (who would receive all the funds back in one go), and a lower operational burden than mandating that Receiving PSPs reimburse their 50% (likely via the Sending PSP) at the same time that the Sending PSP reimburses their 50% of the claim.

However, this does require some implementation and liability considerations that will need further clarification. For example, the PSR should consider a time limit on how promptly the Receiving PSP must settle-up with the Sending PSP. We should not see instances where Receiving PSPs owe significant amounts to Sending PSPs for long periods of time. This would introduce a range of risks, including the risk of the Receiving PSP going insolvent having not settled the claims with the Sending PSPs.

For part (b) – we support the PSR's view that there should effectively be a two-tier approach that encourages PSPs to reimburse the majority of scam claims in a timely manner, but that also enables PSPs to work to an extended reimbursement timeline in certain, more complex cases. However, we would encourage the PSR to consider a longer initial investigation period than 48 hours. From an operational perspective, it would not be possible for a Sending PSP in that short time period to form an initial view on whether the scam claim: 1) was a qualifying scam claim (and not a purchase dispute with a legitimate merchant) 2) was not 1<sup>st</sup> party fraud, and 3) that the customer was not grossly negligent. This initial investigation would still require (often multiple) discussions with the customer, information sharing from Receiving PSP to Sending PSP, and internal review of data and evidence, which takes time to complete. We would therefore encourage that the PSR proposes a longer time limit for this initial investigation, for example 5 working days.

We have considerable concerns that a 48-hour requirement would detrimentally impact the implementation of this reimbursement rule. It would mean that firms' investigations are not suitably effective, it would not provide sufficient time to gather and review relevant information from the Receiving PSP, and it could ultimately drive *even* higher rates of 1<sup>st</sup> party fraud as fraudsters capitalise on the limited checks on claims and effectively the automation of certain scam claims (noting that we anticipate 1<sup>st</sup> party fraud to increase due to the introduction of the mandatory reimbursement rule anyway, but this time limit could make this even worse).

We also believe that the lack of ability to properly investigate scam claims, due to this prohibiting time limit, could lead to detriment for consumers, in terms of a PSP's ability to support and educate their customer regarding scams, and to identify vulnerability. The liaison with customers regarding their scam claim (including the customer providing evidence/information to the Sending PSP to assess the case), provides a vital opportunity for PSPs to educate their customers about scams,



including how to spot and prevent future scams from taking place (as once a scam claim has been reimbursed, the customer is less incentivised to actually engage with their PSP on this topic, because they have received their money back). Furthermore, the customer information provided through the scam claim investigation process can mean that the PSP is made aware of a customer vulnerability, that they weren't informed of previously. This information can help the PSP in tailoring future support for their vulnerable customer. By putting too much onus on a short-time limit, the PSR will limit the opportunity that the Sending PSP has to properly engage with the customer regarding the scam that took place.

Furthermore, the PSR haven't clarified how this would work over weekends, as operationally PSPs may not have full investigation teams working over weekends on assessing scam claims. This would therefore create a significant operational burden on PSPs to support, and/or could mean that fraudsters target weekends to commit 1<sup>st</sup> party fraud, knowing that certain PSPs are likely to have reduced investigations teams working and therefore the investigations may not be as detailed. We would therefore encourage that, for whatever time-limit is agreed upon, the PSR ties this to a typical workweek (i.e., only Monday-Friday count within the time limit).

The PSR should also apply a time limit requirement on Receiving PSPs to provide Sending PSPs with information regarding the scam claim, as the Sending PSP will need this information in order to be able to take an initial view as to the validity of the claim and whether it will need further investigation. For example, in the case of purchase scams, the Receiving PSP may be able to provide evidence that the beneficiary is a known and legitimate merchant, and therefore the claim is likely to be a civil dispute rather than a scam. Likewise, the Receiving PSP may have information that other scam claims are being made against that beneficiary, which could be an indicator that it is a mule / fraudster account. We would therefore encourage the PSR considers requiring the Receiving PSP to meet a certain time limit (for example 3 working days – subject to the PSR extending the reimbursement requirement to 5 working days) to return information to the Sending PSP. If the Receiving PSP fails to meet this time limit, then the Sending PSP should be able to delay the standard reimbursement timeframe. Receiving PSPs should also be able to confirm to the Sending PSP that they require more time to provide the Sending PSP with information relating to the claim, due to the complexity of the case, and in these instances, it is likely that the Sending PSP would treat this claim as one which requires additional investigation and therefore an extended timeframe. However, Sending PSPs should have the ability to highlight to the PSR any Receiving PSPs who consistently miss the time limit to provide this information, as ultimately this does result in customer detriment, due to a delay in their victim reimbursement.

The PSR should also consider what blanket extensions should be applied to this 48-hour time limit (or whatever the final time limit is that is placed on Sending PSPs to reimburse victims). For example, if the customer has not provided sufficient evidence/information about their scam claim, then the Sending PSP should not be expected to reimburse the customer until sufficient information has been provided. The PSR should also consider whether firms are able to consistently extend the time limit for all high value cases and cases where there are a large number of transactions involved (potentially with multiple Receiving PSPs), as these claims are likely to be more complex and need more detailed consideration, and submission of evidence by the customer and the Receiving PSP(s). Similarly, this should be the case for claims where law enforcement is involved in the case, as these claims are usually more complex and take longer to reach an outcome into the investigation.

The PSR should also contemplate the impact of this time-limit on specific scenarios, such as with vulnerable customers at significant risk of being re-scammed. If the bank believes that the customer remains under the spell of a scammer or is highly likely to fall for another scam immediately, then

the bank should not be required to reimburse the money to the customer until they have had the opportunity to speak with the customer to try to educate them about the scam that took place, and to limit this risk of further customer detriment.

With regards to the implementation of the 'extension' to the Sending PSP reimbursement time limit, the operational burden on both the PSPs and Pay.UK would be significant if all PSPs have to notify Pay.UK if they are delaying reimbursement past 48 hours (or whatever the final reimbursement time limit is set as) to investigate each single claim. We would encourage the PSR and Pay.UK to consider a more proportionate operational requirement, for example that each PSP must report these cases to their own nominated officer, as is the case where a PSP does not refund a customer for an unauthorised payment within the required timescales (under Reg. 76(3) of the Payment Services Regulations 2017).

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Noting our earlier argument (see response to Q4) that 'gross negligence' should not be adopted in these circumstances, should the PSR nonetheless proceed with its use, it is our position that this must be sufficiently and granularly defined. In the absence of this definition, it is extremely challenging to respond fully to this question – however we do support the need to outline some industry standards (to mesh with the fuller definition of gross negligence we call for).

Even so, Sending PSPs will need sufficient information (from both the customer and the Receiving PSP) in order to be able to effectively determine even an initial assessment of whether a scam claim is valid (or a civil dispute), as well as whether they suspect 1<sup>st</sup> party fraud or gross negligence (or any other bar for consumer caution, once finalised). It can therefore be the absence of evidence submitted by the consumer that could mean a claim needs more investigation before a decision can be determined. PSPs will need to strike a balance between supporting their customer, who is likely very distressed, with the need to investigate the claim. If the customer has not submitted sufficient evidence to support their claim, then the PSP will need to request further information, but equally needs to be careful not to put too much additional pressure on the customer at that time. Hence, we would not encourage the PSR be too strict in the time limit for this, in case this could have a detrimental impact on consumers, and result in PSPs having to apply undue pressure on their customers in order to meet a deadline. PSPs are incentivised to undertake a claim in an efficient and timely manner, to support their customer and avoid complaints, and therefore there is no need to be overly strict in setting a time limit.

As above, the Sending PSP will also require information from the Receiving PSPs to be able to determine whether a scam claim may need further investigation. For example, in the case of purchase scams, the Receiving PSP may be able to provide evidence that the beneficiary is a known and legitimate merchant, and therefore the claim is likely to be a civil dispute rather than a scam. Another example of this is with regards to building work disputes, whereby a customer makes a scam claim against a builder who has stopped work onsite (which can occur for various reasons), when this should in many instances be a civil dispute between the customer and the builder, rather than a scam claim. Alternatively, the Receiving PSP may have information that other scam claims are being made against that beneficiary, which could be an indicator that it is a mule / fraudster account. We would therefore encourage the PSR considers requiring the Receiving PSP to meet a

certain SLA to return information to the Sending PSP, for them to be able to make an initial assessment of the claim within the standard timeframes (which should be longer than 48 hours as addressed in response to Q11). If the Receiving PSP fails to meet this SLA, then the Sending PSP should be able to delay the standard reimbursement timeframe. As noted in response to Q11, Sending PSPs should have the ability to highlight to the PSR any Receiving PSPs who consistently miss the SLAs to provide this information.

If a PSP suspects fraud or gross negligence, then they also need a reasonable timeframe to be able to investigate these claims in an accurate and efficient manner. Thorough and accurate investigations will be of paramount importance to the effective implementation of this reimbursement rule, as PSPs will need to try to spot and prevent the needle-in-the-haystack cases of 1<sup>st</sup> party fraud, to prevent fraudsters undermining the entire system and infiltrating it with 1<sup>st</sup> party claims.

Aligned to the above, the consumer should be expected to cooperate with the PSP in their investigations. A lack of cooperation, withholding evidence and/or acting dishonestly should all be red flags when considering reimbursement, and should lead to an extended timeframe for further investigation.

Furthermore, the scam type and value, as well as the customer type (e.g., retail consumer, or microenterprise) will impact what 'standard of evidence' would be appropriate. For example, for a complex and high value investment claim, it is likely that a significant amount more evidence would need to be provided than for a £200 purchase scam. For these larger and more complex cases, a lack of evidence could be an indicator of gross negligence. Evidence regarding interventions that the PSP took (such as effective warnings, interrupting and delaying payments, and direct communications with the customer prior to the payment being made), should all be taken into consideration, alongside the customer action that followed these interventions from the PSP. It should also be noted that gross negligence should be assessed on the balance of probabilities, rather than the criminal 'beyond reasonable doubt'. Hence, there is a need for more clarified indicators for PSPs to consider and compare against.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

We support the principle behind a default allocation of 50:50 for Sending and Receiving PSPs, to share the liability for the reimbursement claim (although noting that there should be limited and defined exceptions clarified by the PSR, for example for Open Banking payments, where there are more than 2 PSPs in the payment chain). As per our other responses, we would encourage this to be as operationally simple as possible, with clear guidelines and requirements, to avoid unnecessary additional operational burden on PSPs – particularly given this aspect bears no impact on the consumer (as they get reimbursed regardless), and so is an area where operational efficiencies can be made without any consumer detriment.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We have concerns that the proposed approach could be impractical, and could lead to a significant operational burden, lack of clarity for PSPs, and lengthy disputes between PSPs. As per the response

to Q13, this makes no difference to the outcome for the consumer, and therefore needs to be as operationally efficient as possible. Having a swift, consistent, certain, and fair arbitration process that is mandated across all PSPs (rather than voluntarily signed up to), and enshrined in law/regulation/Directions (rather than through scheme rules) could be one option, or otherwise, the 50:50 split is just simply applied without exception. If the PSR does determine that a dispute process should be put in place, then they should ensure there is an arbiter, who can take a binding decision on all PSPs, to ensure any decision is actually abided by.

The PSR should also consider how disputes could arise not only regarding the 50:50 default allocation, but also regarding the Sending PSP's decision to reimburse – as the Receiving PSP may dispute whether the reimbursement should have happened at all. The Sending PSP is the firm ultimately deciding whether a scam claim should in fact be treated as a scam, or whether it would instead be a civil/purchase dispute (e.g., if the customer ordered goods and they arrived not as expected, this is not a scam but a purchase dispute, but a customer may incorrectly raise this as a scam claim). The Receiving PSP may dispute that the Sending PSP should ever have reimbursed the claimant in the first place, and refuse to settle their share of the claim. How should this be treated – will the Receiving PSP have a legal right to not pay their 50% of the liability back to the Sending PSP, leaving the Sending PSP on the hook to have paid for the full claim? This would also be the case for cases of 1<sup>st</sup> party fraud, and gross negligence, where it would ultimately be down to the Sending PSPs to determine whether either of these were the case – and the Receiving PSP may dispute the Sending PSP's decision. We would encourage the PSR to consider applying the model that currently works for Bacs Direct Debit, whereby the Sending PSP makes the decision, and there is a specific set of criteria through which a Service User (in this context, the Receiving PSP) would be able to challenge this decision.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

As outlined in response to Q3, we would encourage the PSR to clarify which payment (specifically) is the scam payment that can be claimed for reimbursement under this rule, to provide clarity to industry (both Sending and Receiving PSPs), as well as to customers (regarding where to make their claim). We would encourage the PSR to confirm that the 'scam payment' in scope of reimbursement is the specific payment that is made from an account held by a legitimate victim, to an account held or controlled by a fraudster. This will help to bring clarity regarding liability, for a large number of multi-generation scam cases, including the following example:

- A scammer convinces a customer that their money isn't safe, and encourages them to transfer their money to a family member's account. The scammer then convinces them that the money needs to be transferred again to another account to be kept safe – and this account is being controlled by the scammer.
  - o In this example, the first transfer would not be in scope for reimbursement, as the victim has transferred money to a family member's account, but the money has not yet been transferred to an account controlled by the fraudster. The second transfer would be the scam payment in scope of reimbursement, as this is the payment that left a legitimate customer's account and moved to an account controlled by the fraudster.
  - o By clarifying the specific payment that is in scope of the reimbursement rule, the PSR would provide clarity to the customer and their family member regarding which



payment can be claimed (therefore also avoiding the risk of duplicate claims), as well as providing clarity to the Sending and Receiving PSPs in this multi-generation scam claim regarding which parties are liable.

However, there would still be a number of multi-generation scam cases that would not be clear as to how the rule would be applied, including the following example:

- A victim is encouraged by the scammer to open a crypto wallet in their own name. The victim transfers money from their bank account to their crypto wallet and purchases cryptocurrency (therefore at this point, the customer is still in possession of their money, albeit in cryptocurrency form). The scammer then convinces the customer to transfer the cryptocurrency to a crypto wallet held by the scammer (which would not be via faster payments). This is the point at which the scam payment takes place – however it is unclear whether the PSR is able to place the mandatory reimbursement rule on the crypto wallet firms that enabled this scam payment to take place, or whether this scam claim would be out of scope under this reimbursement rule, due to the actual scam payment not being made through FPS.

In all circumstances, multi-generation scams should be considered complex scam cases, and therefore should be allowed to fall outside of the Sending PSPs time limit for reimbursement to the victim – as these cases often require dialogue between multiple PSPs and victims, which takes time to investigate properly.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

We support the PSR's proposal that the allocation of repatriated funds should align to the proportion of reimbursement that each PSP made to the consumer (which would be 50:50 as default, however if the PSR does implement a process where the PSPs can dispute and change the allocation, then any repatriated funds being repaid would need to align to whatever the eventual allocation was for that case).

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We support the PSR's proposal that the cost of reimbursement should be allocated to all directly connected PSP participants as well as PSPs indirectly sending and receiving payments.

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

We would encourage the PSR to reconsider its approach to implementation of the mandatory reimbursement rule via the PSO. The PSR should instead place Directions on all PSPs to adhere to the mandatory reimbursement rule (with a potential opportunity in the longer term to amend legislation

to reflect the mandatory reimbursement requirements, for example through an amendment to the Payment Services Regulations 2017). This would allow for a consistent and clear rule to be applied across the industry, to all participants (direct and indirect) and would reduce the significant burden and risk that would otherwise be placed on Indirect Access Providers. It would overcome the many challenges that the PSR has highlighted with regards to requiring Pay.UK to implement the rule (as Pay.UK would no longer need to play a role in setting and enforcing this reimbursement rule), and would eliminate the need for a short and long term approach, which is operationally inefficient and could lead to significant wasted expenditure, through infrastructure and processes being implemented and then changed. This would also enable Pay.UK to focus on delivering the NPA programme, which industry is mindful will require significant focused resource to implement and deliver effectively.

The PSR will be provided the powers to implement this rule through the Financial Services and Markets Bill (FSM Bill). As currently drafted, the FSM Bill states that “the Payment Systems Regulator must prepare and publish a draft of a relevant requirement for reimbursement in such qualifying cases of payment order as the Regulator considers should be eligible for reimbursement. The Payment Systems Regulator must impose a relevant requirement, in whatever way and to whatever extent it considers appropriate, for reimbursement to be made in qualifying cases of payment orders.” A ‘relevant requirement’ means a requirement imposed by or under section 54 or 55 of the Financial Services (Banking Reform) Act 2013 (or by or under a combination of those sections). Section 54 relates to Directions, and Section 55 relates to System Rules. The PSR’s proposal currently chooses implementation via System Rules, which presents a number of problems:

- As the PSR notes, it is not clear how the rules could be enforced by Pay.UK, or what sanctions they would be able to impose should firms fail to comply (other than being removed from the FPS altogether, which would be a significant penalty).
- Also, as the PSR notes, not all market participants are direct participants in the FPS. Therefore, indirect participants would not be bound by the FPS rules; they would only apply to direct participants. This would require a workaround that would carry significant complexity across industry. It is, for example, unclear how indirect participants would be bound to comply with the rule, and how the 50:50 split could be enforced against them – as how could the Sending PSP enforce that an indirect participant Receiving PSP must reimburse them 50% of the scam claim, without there being any direct contractual relationship between them. Contractually, the only way to seemingly do this would be for Indirect Access Providers (IAPs) to undertake to ‘procure’ compliance by their indirect participant clients. However, this would likely mean:
  - o If the indirect participant did not meet the requirements of the FPS Rules, it is the direct participant (the IAP) which would be in breach, not the indirect participant. That is despite the lack of fault by the direct participant.
  - o Potentially the direct participant (the IAP) could have to cover the 50:50 split and recover this from the indirect participant, which would create significant credit risk in the process.
- The consequence of this would be significant for a direct participant IAP. It would create barriers to direct participants providing services to indirect participants and may lead to existing indirect access providers withdrawing from the market or further limiting their risk appetite in a market which does not have a surfeit of indirect access providers.

It is unclear to us why the PSR has chosen the route of implementing the rule via System Rules, rather than via Directions, which would overcome a significant number of the issues that are highlighted by the PSR in this consultation. The PSR is set to be empowered under the FSM Bill to



implement the rule via Directions, and there is precedent for the PSR to issue Directions to a significant volume of PSPs (e.g., most recently, the decision to require 400+ PSPs implement CoP). We would therefore encourage the PSR to outline why it is not willing to issue Directions to implement this rule, which would resolve these contractual issues, and would remove the reliance that is due to be placed on Pay.UK who are not currently set up to be able to implement, monitor and enforce this rule.

One alternative to the PSR issuing Directions would be to create a contractual nexus; a separate multi-lateral agreement for reimbursement, to which all direct and indirect participants are a party, with an obligation in the FPS rules for direct participants to ensure that indirect participants are parties to this multi-lateral agreement. This Reimbursement Framework could still be developed/owned by Pay.UK, but would create a direct contractual nexus between all impacted participants. It would exist separate to the FPS Rules which would continue to bind only the Direct participants.

Finally, we would also dispute the terminology re: Pay.UK becoming the 'rule-setter for mitigating fraud'. As we have outlined, fraud and scams are perpetrated across a wide ecosystem of firms, many falling outside of the financial services sector. Pay.UK are one body overseeing the payment systems that fall at the end a fraud taking place, when the payment is eventually made (noting that a lot of fraud will also fall outside of Pay.UK's coverage as well). That being said, we do strongly support the principle that Pay.UK should seek to ensure that the payment systems that it operates are effective at supporting PSPs in preventing fraud, including ensuring that this is an integral part of the design of the NPA.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

As outlined in response to Q18, we would strongly encourage the PSR to reconsider its approach, and to instead issue Directions to all direct and indirect participants.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

As outlined in response to Q18, we would strongly encourage the PSR to reconsider its approach, and to instead issue Directions to all direct and indirect participants. We do not believe that Pay.UK would need to play a role in the setting and enforcement of this rule, which could be solely achieved through PSR Directions on all PSPs. Pay.UK could play a role in helping to operationalise the rule, so that it can be implemented effectively.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

As per our response to Q14, we have concerns that the proposed approach could be impractical, and could lead to a significant operational burden, lack of clarity for PSPs, and lengthy disputes between

PSPs. The allocation and dispute resolution between PSPs makes no difference to the outcome for the consumer, and therefore needs to be as operationally efficient as possible. Having a swift, consistent and fair arbitration process could be one option, or otherwise, the 50:50 split is just simply applied without exception.

If the PSR does go down the route of establishing an allocation criteria and dispute resolution arrangement, then this could be based on the CRM Code, although it would need to apply to all PSPs in order to be effective in practice, therefore could no longer be a voluntary code.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

As outlined above, we do not believe there is a need for a short-term approach, which adds complexity and could increase implementation costs for firms if changes are required to switch over to any longer-term implementation. Instead, the PSR should issue Directions on all PSPs, removing the need for this workaround. PSPs under Direction of the PSR should be expected to self-certify compliance, with an SME responsible for this self-certification, as part of the Senior Managers Regime (which is due to apply to payment institutions and e-money institutions shortly, as well as banks who are already covered).

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We do not believe that real-time monitoring would be practical or proportionate, and would carry significant cost and operational burden on all PSPs in the market, as well as on the entity undertaking the monitoring. It is also unclear what benefit Realtime monitoring would provide, particularly given scam claims and cases can go on for long periods of time due to detailed investigations. We would therefore encourage a more proportionate approach is taken, e.g., periodic reporting, or the aforementioned self-certification approach. The PSR will, as part of Measure 1 Directions, receive data regarding reimbursement rates and scams figures from the largest PSPs in the market – this could be extended to apply to all PSPs.

**24. Do you have views on the best option for short-term enforcement arrangements?**

As outlined above, we would encourage the PSR to place Directions on all PSPs, with one of the many benefits of this option being that enforcement arrangements are already pre-defined. The PSR is permitted (under Section 72 of FSBRA) to publicise compliance failures, and (under section 73 of FSBRA) to impose penalties.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**



Please see response to Q18.

In summary, we would welcome the rules to be applied directly to Indirect Participants, as this would best provide a consistent approach across all PSPs. This should be implemented in a way that does not create a disproportionate burden on Indirect Access Providers (IAPs), e.g., through significantly increased credit risk exposures, liability, and cost. Our preference is therefore for the PSR to issue Directions on all PSPs, including Indirect PSPs.

Our least favoured approach would be 7.31c, which would apply the reimbursement rule to all transactions, and would make the IAP responsible for the transactions of its indirect access clients. This approach would lead to lack of consistency in application across the market, and would create significant credit risk and liability for IAPs. Implementing new contract terms for all indirect clients could lead to different negotiated terms, with different outcomes for consumers and PSPs, as the IAP is forced to act as the arbitrator of the rule for each of their clients. Furthermore, termination of supply would be the only sanction available to IAPs to enforce the rule upon their clients. Operationally, the routing of claims and counter claims via the IAPs for all of their indirect clients would create significant operational burden, and increase the cost of providing IAP services. Finally, if an indirect PSP were to cease trading, would the relevant IAP be responsible for 13 months of claims as beneficiary (and sending) bank? If this this were the case, the provision of domestic FPS payments would become a credit risk product, with various mitigations having to be in put in place.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

We would encourage the PSR to place Directions on all PSPs (see responses to Q18 and Q25). If the PSR does go down the scheme rules route as proposed, then we would encourage the PSR places Directions on indirect PSPs (rather than on IAPs), for the reasons outlined in Q18.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

No comments

**28. Do you have any other comments on the proposals in this consultation?**

No comments

# Bob Ford and John Bertrand (Individuals)

APP Scams Team  
Payment Systems Regulator  
12 Endeavour Square  
London  
E20 1JN

November 22<sup>nd</sup> 2022

Dear Team,

We are pleased to have read and feedback on the 28 questions asked in your well researched and written Consultation paper: Authorised push payment (APP) scams: Requiring reimbursement.

The new measures fighting payment scams, based on bank/PSP being mandated to reimburse consumers is outstanding. This will help stop the erosion of trust in banking created by the bank/PSP blaming their customers for the majority of frauds.

Giving consumers peace of mind that if they are scammed, financially, that loss will be back in their bank account in 48 hours minus a small fee. Emotional the consumers will still be traumatised but financially OK.

Pay.UK is a great choice to be the compliance monitor over the Bank/PSP interactions and resolving, away from the consumer, who owes whom. The 50/50 initial split of the reimbursement is fine and gets the confidence back into the financial system immediately.

The banks themselves will bilaterally sort out which bank/PSPs are most responsible for the individual frauds taking place between each other. Those bank/PSPs not using Confirmation of Payee (CoP) are often the most culpable as shown in your report by the migration by scammers to non-using CoP banks for their unlawful activities.

Unfortunately scammers need a bank account for Faster Payments. Many new bank/PSPs need to add customers fast to drive market valuations. As a result KYC becomes a key element needing to be robustly regulated to keep standards high.

One aspect we should look at is incentivising bank/PSPs to not give scammers and their mule networks access to their bank accounts. By fining the bank/PSP £3,500 per scammer's bank account, the average consumer fraud, £660 million in 2021 could have combatted fraud.

We also note the mandatory reimbursement does not address the amount of fraud that was not reimbursed over the period 2018 to 2021 by the bank/PSP. A total of £1.1 billion is now in limbo having enriched the bank/PSPs unfairly. The Financial

Ombudsman and Standards Lending Board have rightly questioned the bank/PSPs over this behaviour. The bank/PSP industry should make a contribution to the House of Lords 'Fighting Fraud: Breaking the Chain' activity.

Whilst we agree there should be exceptions to mandatory reimbursements, the bank/PSP must collaborate on the activity of the New Payee bank account before the consumer makes the payment. The use of the Government's Take Five, while well intended, is too generic and easy to ignore. Only a minority of people read Terms and Conditions in the internet/digital space. Even with CoP, Lloyds Bank research showed 41% of people do not really "get it".

Bank/PSPs need to work more actively with consumers about to make a new payment to a New Payee. This includes requesting further due diligence by the consumer on the New Payee. If nothing changes notify the consumer; if there is a scam the liability belongs to them. The messaging has to be made very clear about the responsibilities taken on by overriding the warnings and Pay.UK has to ensure vulnerable people, designated by FCA are treated with extra care by bank/PSPs.

Well done for proposing a way forward in the tricky world of APP scams. Mandatory reimbursement is an important part in preventing frauds. The other components in the fraud chain – social media platforms, telecom and ISP – also need incentives to stop the fraudsters' scams. Here the EU new proposals for 2023 include fines of up to 10% of the global revenue for these components. We anticipate Pay.UK will be working closely with both Ofcom and the Police across the fraud chain.

Getting fraud prevention right can enable the UK to lead the world in integrating real time payment with traditional banking.

Kind regards

John Bertrand and Bob Ford

## Questions

### 1. Impact on Consumers (Page 20)

Significant and far more empathetic as the first point of contact being scammed is with their bank. Their bank (the Payer) now has the mandatory obligation to reimburse the APP scam within 48 hours. By making the consumer financial wholly, relieves the fiscal pressure and helps smooth the emotional issues of being scammed.

Consumers will see the transparency of resolving the scam within 13 months. Similar to Insurance Claims there is a charge (excess) for the claim (£35) itself along with and minimum amount claim (£100).

Having a single point of contact, Pay.UK, simplifies the reimbursement path considerably. Today the consumer is blamed for the scam and receives little empathy in discussing the circumstances with bank/PSP.

Consumers need to be clear of where their liability lies and their role in the transaction. Lloyds Bank research showed 41% consumers were unfamiliar with CoP and 24% would recognise that a 'No match' message means they could be getting scammed.

The European Commission (EU) proposal on Instant Payments in euro recommends ([https://eur-lex.europa.eu/procedure/EN/2021\\_341](https://eur-lex.europa.eu/procedure/EN/2021_341)) once CoP becomes obligator that the Payer can continue to make the payment after being informed of discrepancies but “in such cases bank/PSPs should not be held liable for the execution of the transaction to an unintended payee”. “The bank/PSPs should inform the client about the loss of reimbursement rights given the choice taken to ignore the notified discrepancy”. (Clause 11) The EU addresses the need to verify the payee name by making it mandatory for IP. (Clause 11)

<https://www.finextra.com/newsarticle/39985/millions-of-brits-risking-fraud-by-ignoring-confirmation-of-payee-warnings>

It is not only the vulnerable that are susceptible to scams, we all are. The vulnerable consumers must be protected, like the non-vulnerable, and not by denying APP capabilities.

### 2. Impact on PSPs (21)

The cost of reimbursements of reimbursements will probably double. Over the past four years bank/PSPs have refused to reimburse 500,000 customers £1.1billion resulting from APP Fraud. While the Financial Service Ombudsman, over turns the majority of the bank/PSPs decisions.

By mandating Confirmation of Payee for all bank/PSPs extensive technical work is needed at each location to ensure the Payer knows the right Payee is receiving the money. This did not happen with Cheques as the signatures and bank details were checked before payment was made. Volume, digitalisation and the need to pay faster created instant payments that did not verify the owner of the bank account worldwide. The NPA will be addressing this.

Culturally the bank/PSPs will have to collaborate more around scammers/mules bank accounts as APP only works with a bank account. The initial 50:50 split of reimbursement solves the customer’s immediate problem. UK.Pay will need to arbitrate amongst the Bank/PSPs as to who pays who and what that Payee Bank Account Owner is going to do to meet the new fraud prevention standards of the industry.

These standards will evolve out as scammers use the weakest fraud prevention bank/PSP. The quarterly results and settlement between Payer and Payee conducted by a third party (Pay.UK) will result in a league rating. The rating will determine what acts are required to improve scam protection.

The FCA will be interest the banks with the most scammer accounts as Principle 6 states:

A firm must pay due regard to the interests of its customers and treat them fairly. (FCA Handbook COBS 4.4.3R)

**Having scammers with bank accounts is not treating anyone fairly.**

**Incentives should be applied to banks providing scammers with Bank Accounts.**

***Recommend an incentive of £3,500 fine***, the average consumer loss, for each fraud case.

***This would have generated £661 million in 2021 and cumulative £2 billion since 2017 to pay for combatting fraud.***

<b>Incentives</b>	<b>2017</b>	<b>2018</b>	<b>2019</b>	<b>2020</b>	<b>2021</b>
Per case (£'000)	£3.5	£3.5	£3.5	£3.5	£3.5
Cases (£'000)	£135,086	£273,753	£401,559	£508,225	£661,374
Cumu (£'000)	£135,086	£408,839	£810,397	£1,318,622	£1,979,996

In addition, from 2018 to 2021 banks have withheld £1,120 million from their defrauded clients. This money under the PSR proposal is left in limbo as reimbursement is only mandatory going forward. The bank/PSP industry should offer this money for infrastructure to combat crime.

Banks, as they retain bank account details, often up to 7 years know the names of who opened the bank accounts, transactions made and where the money went. Faster Payments has a built in tracking mechanism for each payment. Therefore by looking at the past the scammers' details can be discovered today and forwarded onto law enforcement.

### **3. Scope of reimbursements**

Coverage is clearly defined as in regulation 2(1) and agrees with the last consultation wanting more or all PSPs included in reimbursements.

Having the reimbursement rules applied only to APP Scams after the regulations come into force in 2023 ignores the £1.1 billion kept by bank/PSPs in the four years ending 2020.

### **4. Comments on proposals (29)**

#### **a. Consumer caution exception**

Not really as a clear set of rules around payment, explanation of their role in making the payment and where the liability lies when ignoring bank/PSP warnings should suffice.

#### **b. Use gross negligence**

Yes when customers can be proved to show 'gross negligence' by paying the money away after the Payer Bank warnings showing high scam probability. The Payer bank/PSPs collaborating with Payee Bank/PSPs on 'is the scammer working this account' needs to be documented and technology or people used to warn the Payer before the payment..

#### **c. Guidance on gross caution**

No, as gross caution, like the Take Five campaign, become generic and ineffective very quickly. Few people read the Terms and Conditions.

### **5. Vulnerable customers acting with gross negligence (29)**

Only the first few scams should be reimbursed for vulnerable people and then a protection for that person should be installed, for example, having a Trusted Third Party approve the payments.

### **6. Using FCA's definition of vulnerable customers (29)**

Perfect

### **7. Comments on proposals that (30)**

- a. Applying a modest fixed excess  
Agree
- b. £35 max excess  
Agree with future levels agreed by PAY.UK
- c. **Exempt vulnerable consumers from excess**  
Probably on a case by case basis

#### **8. Comments on Proposals that (32)**

- a. Sending PSP setting minimum claim threshold  
Provided it does not exceed Pay.UK limits
- b. Thresholds should be no more than £100  
Yes with raising the limits agreed collectively with Pay.UK
- c. Exempt vulnerable consumers from thresholds  
Only on the first few scams then follow 5 above

#### **9. Maximum threshold (32)**

There should not be a maximum threshold as this is very important for the consumer to have confidence reimbursement applies to all. Scams above £50,000 are investigated by the bank/PSPs. The greater single losses are in the Large Corporate arena that are excluded from these regulations.

#### **10. Comments on proposals that (32)**

- a. **Sending PSP setting time limits**  
Not covered by the Pay.UK
- b. **Any time limits greater than 13 months**  
13 months should be enough time, any changes covered by Pay.UK

#### **11. Comments on proposals that (34)**

- a. **Sending PSP responsible for reimbursing consumer**  
Agree
- b. **Reimbursement should be as soon as possible**  
Agree – 48 hours seems fair

#### **12. How long investigating gross negligence (34)**

The 13month rule should be standard with exceptions approved by Pay.UK

#### **13. Default 50:50 allocation (35)**



The 50:50 proposal is great because it resolves the immediate need to replace the money bank into the account it was sent from and making the account owner happy and relieved.

Suggest on a quarterly basis that there is reconciliation between the bank/PSPs on who owes who what. The scammer bank account owner should be responsible for any losses as it is their responsibility to Know Your Customer. Reconciliation is overseen and adjudicated by Pay.UK.

Should fines be mandated for Bank/PSPs (Section 2) providing scammers with Bank Accounts again Pay.UK adjudicates.

**14. PSP's departing from 50:50 allocation (35)**

No, all must follow the rules with an annual health check by Pay.UK to address any issues or developments.

**15. 50:50 allocation on multi-generational scams (35)**

The sources of the scams need to be tracked and presented back to the originators and their regulators or associations to help prevent scams starting. For example, social media platforms and telecomm companies need to be part of the solution in reducing APP fraud.

**16. 50:50 on repatriation of funds (36)**

Excellent as it starts with everyone being equal

**17. Allocating the costs of mandatory reimbursement (37)**

50:50 is a great starting point and as the trends start showing where the scammer and mule accounts are centred those Bank/PSPs need to contribute more towards the amounts being reimbursed. This can be done on a bilateral basis under the supervision of Pay.UK.

**18. PSO being the rule setter (40)**

Very good call and as frauds change so should the rulebook to counter scams. Here speed is key in making the necessary changes

**19. Minimum set of Faster Payments Scheme Rules (43)**

Looks a good balance between minimum set of changes and NPA arrival

**20. Powers under FSBRA (43)**

Yes exercise the powers under section 55

**21. Dispute resolution agreements (45)**

Good place to start as Pay.UK is known and respected by all parties

**22. Pay.UK being an compliance monitor (46)**

Good way to go as it can be started immediately

**23. Cost/benefits for Pay.UK (46)**

Initially the monitoring system need not be in real time and once the functions are working well then the need for real time can be reviewed.

**24. Short -term reimbursement arrangements (47)**

As APP Fraud is a major threat then bank/PSPs need to take it much more seriously than they do at present. To this end we need to start as we need to go on which is firm but fair using all incentives at our disposal.

**25. Short -term reimbursement arrangements - non direct participants (48)**

There should be no difference between direct and non direct participants. The Direct Participants that are the agents for the non direct should be held responsible for their non direct activities.

**26. Direct indirect PSPs or IAPs (49)**

Both need to be on the same roadmap

**27. Cost benefits in Annex 2 (50)**

Clear picture presented in Annex 2 - well done

**28. Any other comments**

Excellent proposal for a difficult, hard to solve problem that APP fraud presents. Provides the Bank/PSPs and their clients a clear, transparent and mandated course of action that reflects well on the payment industry.

The EU proposal contains suggestions to keep the KYC up to date by mandating daily checking of clients against EU Sanctions and PEP lists for IP. Once the money is gone, it's gone as there is no time to pull the payment back.

# Building Societies Association

# Authorised push payment (APP) scams: Requiring reimbursement

Payment Systems Regulator CP22-4

Response from the Building Societies Association

24 November 2022



## Introduction

The response from the Building Societies Association to CP22/4 is set out below.

The Building Societies Association (BSA) represents all 43 UK building societies, as well as 7 credit unions. Building societies have total assets of over £480 billion and, together with their subsidiaries, hold residential mortgages over £357 billion, 23% of the total outstanding in the UK. They hold over £333 billion of retail deposits, accounting for 18% of all such deposits in the UK. Building societies account for 40% of all cash ISA balances. They employ approximately 43,000 full and part-time staff and operate through approximately 1,345 branches.

With the exception of two members who also offer a current account, BSA members are savings account payment services providers (PSPs) and many societies restrict the availability of Faster Payments transfers to the customer's nominated current account only. As a result, they have not seen the same scale of APP fraud cases and losses as current account providers – and therefore have significantly lower volume / value of customer reimbursement - or a significant increase in APP fraud following the implementation of Confirmation of Payee phase 1. However, they recognise the need to remain vigilant in case their account holders become more heavily targeted.

## Summary of our response

### The key issues for our members

- BSA members would like clarification on the impact of these proposals on savings provider PSPs whose principle role in the APP scam payment journey involves the customer making a Faster Payments transfer from their savings account to a current account which then funds or part funds a subsequent payment from that current account to a fraudster.
- Members have also raised concerns about the disproportionate impact of the 48 hour reimbursement requirement on smaller savings provider PSPs with lower APP fraud risk which do not operate 27/7, 7 days a week. We would welcome discussions with the PSR on a differentiated approach for savings account providing PSPs with lower APP fraud risk.

### Impact on consumers and PSPs

- We agree that this consultation's proposals will mean more customers receiving more reimbursement for losses from APP fraud. However, we do not agree that mandatory reimbursement will lead to lower numbers of APP fraud scams even with implementation of additional measures around intelligence sharing etc.
- It is likely that the introduction of the safety-net of mandatory reimbursement may have the unintended consequence of encouraging some consumers to be more reckless to fraud risk when making payments.
- It is unlikely that the building society / credit union sector would withdraw services from certain types of consumer because they may be perceived as more likely to fall victim to APP scams – in particular older customers who are our main demographic for savings products. More likely are restrictions on payments to particular types of recipient that are known to be particular favourites for fraudsters – as has already been the case with some PSPs refusing to allow payments to crypto-currency exchanges.

- However, one additional impact will be that individuals or firms who are discovered allowing their accounts to be used for laundering the proceeds of fraud as money mules are more likely to have services withdrawn and will find it more difficult to open accounts elsewhere.
- Where firms refuse more payments on the grounds of suspicions of fraud, it would be helpful if the FCA's Consumer Duty requirements confirmed that refusing a payment on these grounds is "a good customer outcome". It would also be helpful to brief the Financial Ombudsman Service to this effect.

#### Reimbursement requirements

- We broadly agree with the consultation proposals on payments and payment service providers in scope - subject to clarification on the scope of "sending PSP" - and on the definition of an APP scam.
- We welcome the exclusion of private civil disputes from the scope of APP fraud reimbursement but some of the practicalities of distinguishing these cases from APP frauds need to be worked through.
- To avoid the inconsistency issues associated with the CRM Code and FOS' current complaint assessment criteria, guidance on the requirements of defining "gross negligence" should be included within the Faster Payment scheme rules from the start.
- We are pleased to see that PSR has acknowledged the concern that introducing the safety-net of mandatory reimbursement is likely to lead to the unintended consequence of some consumers becoming reckless to fraud risk when making payments because they know that they will not lose out. It is sensible to keep the option of a customer caution exemption under review and we suggest that this is retained as an option beyond the proposed post-implementation review as it may take longer for changes in behaviour to show through in data from PSPs.
- Our view is that the gross negligence provision would be inappropriate as a framework to counter such behaviour as typically the evidence for reckless behaviour will be a series of lower level incidents rather than a major event that would trigger the "gross negligence" threshold
- In principle, using broad brush assumptions in the context of supporting vulnerabilities is contrary to the FCA's objectives in their guidance to firms on supporting vulnerable consumers and we would prefer that claims for reimbursement for APP fraud losses based on vulnerability contain a clear causal link between consumer's individual circumstances and the decision to pay to the fraudster. In practice, it is likely that the causal link between characteristics of vulnerability and unwise decisions leading to becoming a victim of APP fraud with serious losses will be clear and obvious for most cases.
- We support the use of the FCA's definition of a vulnerable customer.
- We support the excess / minimum claim threshold / no maximum threshold proposals in principle but members currently have no sense of whether these are too much or too little. We suggest that all proposals are adjustable under review to see if they are sufficient to deliver the objectives behind them. Giving PSPs the capability to exempt vulnerable consumers from any excess / minimum claim threshold that they do apply is sensible and fits well with the FCA's guidance on supporting vulnerabilities.
- It would also be sensible to keep the option of a maximum threshold available, particularly for reimbursement claims associated with fraudulent purchase scams

where losses are less likely to be life-altering and the consumer's own responsibility under "caveat emptor" is higher than for other types of APP fraud.

### Liability for reimbursement

- While in agreement with the rest of the proposal on the sending PSP's responsibilities, BSA members have raised concerns around applying the 48 hour requirement to PSPs that offer savings products and so to not operate 24/7, 7 days a week as the fraud risk associated with their products does not warrant this. Requiring introduction of the infrastructure to support the 48 hour requirement for lower risk PSPs would be a disproportionate cost to savings providers and their members / customers which will not be offset by reduced APP fraud losses. We would welcome discussions with the PSR on a differentiated approach for savings account providing PSPs with lower APP fraud risk.
- It is impossible to develop any workable standard for investigation of gross negligence without a definition of what "gross negligence" means. For first party fraud, the individual under investigation has potentially committed a criminal offence and so the standards of evidence that might lead to a decision as to whether or not to peruse a criminal prosecution seems the most appropriate. It is difficult to generalise as to how long an investigation might take – this may include police involvement - but it will certainly be more than 48 hours. Time limiting criminal investigations would not be appropriate.
- We support the proposal on 50:50 default allocation of reimbursement costs. BSA members have suggested that it would be a more effective incentive for organisations with serial fraud control failure to improve if the PSR or a PSO has the ability to vary the 50:50 allocation to allocate more reimbursement cost to the failing PSP rather than penalising consumers by refusing their payment requests.
- We also support development of more tailored criteria for allocation, and associated dispute resolution arrangements designated into scheme rules must include checks and balances so that there are no unintended consequences which undermine the PSR's objectives of maintaining fair competition in the payments sector and would welcome the opportunity for the BSA and other trade bodies representing smaller, non-current account providers to be included in discussions on how a more tailored framework might look.

### Implementation

- We see the sense in the PSR's long term objective of there being a one-stop PSO for payment systems with fraud prevention and consumer protection as part of its remit. However, from the perspective of a sector where the majority of building societies are indirect PSPs and therefore at arms' length from Pay.UK's governance and operations, Pay.Uk is not ready to step into this role. Preparing Pay.UK for the PSO role will require significant changes to its constitution and management culture to make the arrangement work for indirect PSPs.
- We support the proposed minimum initial set of Faster Payments scheme rules subject to clarification of a number of points discussed above. In particular, the initial Faster Payments rules set should include clear definition of gross negligence.
- We agree that a reporting requirement on PSPs is the best short term option for monitoring compliance with the proposed reimbursement requirements rather than

waiting for delivery of a real time monitoring system. Bearing in mind, that Pay.UK currently has no jurisdiction over indirect PSPs we suggest that the reporting requirement is voluntary for indirect PSPs on the basis that pressure from consumers and consumer groups will make it difficult for any PSP to opt out.

- As Pay.UK would have no enforcement jurisdiction over them, any imposition of formal short term enforcement arrangements on indirect PSPs would require a suitable direction from the Payment Systems Regulator.
- In practice, the role of formal enforcement will be reduced by pressure from the media and consumer groups on PSPs to follow the Faster Payments rules on reimbursement being more of an incentive for PSPs to comply than any formal direction or enforcement arrangements.

### Cost / benefit analysis

- APP fraud has cost the industry an average of £500m annually since 2020, these losses may increase as a result of mandatory reimbursement and the anticipated increase in recklessness towards fraud of some individuals. This will impact portfolio pricing and result in reduced consumer value in product offering across the industry to allow PSPs to cover costs.
- The outlined proposals will take significant investment to implement which WILL NOT be offset by a reduction in losses for PSPs with lower APP fraud-risk product portfolios as it will be with the tier 1's.
- The consultation's cost benefit analysis has ignored the opportunity cost of funding APP fraud reimbursement - which will include the potential to offer lower lending and higher savings rates (both much needed in the context of the cost of living crisis) as well as the opportunity for PSPs to invest money spent on reimbursement in improved efficiency / controls / customer outcomes.

### **APP fraud reimbursement & the building society context**

With the exception of two members which also offer a current account, the BSA's membership are providers of savings not current account providers.

BSA members have asked for clarification on the impact of these proposals on savings provider PSPs whose principle role in the APP scam payment journey involves the customer making a Faster Payments transfer from their savings account to a current account which then funds or part funds a subsequent payment from that current account to a fraudster.

Based on conversations with PSR colleagues, our assumption is that the customer should only be reimbursed once and the savings account PSP making a Faster Payments transfer to a current account is not defined as an additional "sending PSP" as they were not the PSP that made the payment to the fraudster on the customer's instruction. We would be grateful if the PSR could confirm this.

Within the above, our members still have other responsibilities in respect of APP fraud:

- To reimburse APP fraud losses following the implementation of this consultation's proposals where, if allowed under the account terms & conditions, the customer authorises a payment directly to a fraudster from their savings account and incurs loss.



- To follow up on suspicions that a customer is being targeted for fraud when suspicions arise and to warn the customer appropriately.
- To support / participate in fraud education for all consumers.
- To identify / support customers whose circumstances might make them particularly vulnerable to fraud or financial abuse.

## **Our views on the PSR's consultation questions**

### *1. Do you have views on the impact of our proposals on consumers?*

We agree that this consultation's proposals will mean more customers receiving more reimbursement for losses from APP fraud.

However, we do not agree that mandatory reimbursement will lead to lower numbers of APP fraud scams even with the additional measures around intelligence sharing etc. that are planned to be implemented alongside reimbursement. Unfortunately, the introduction of mandatory reimbursement is likely to be seen by organised crime as a signal that they can continue targeting UK consumers for fraud scams at low risk so the impact on consumers will be that they are targeted for more fraud not less.

It is likely that the introduction of the safety-net of mandatory reimbursement may have the unintended consequence of encouraging some consumers to be more reckless to fraud risk when making payments – see 4. below.

On the comments around PSPs being expected to refuse more payment orders and block accounts that they consider suspicious, it is reassuring that the regulator recognises that refusing a payment in suspicious circumstances is a legitimate course of action to take. We would like this recognition to be explicitly referenced in the FCA's Consumer Duty requirements to confirm that refusing a payment on suspicion of fraud is "a good customer outcome" (we understand that PSR and FCA are already working together on the Consumer Duty). It would also be helpful to brief the Financial Ombudsman Service to this effect.

It is unlikely that the building society / credit union sector would withdraw services from certain types of consumer because they may be perceived as more likely to fall victim to APP scams – in particular older customers who are our main demographic for savings products. More likely are restrictions on payments to particular types of recipient that are known to be particular favourites for fraudsters – as has already been the case with some PSPs refusing to allow payments to crypto-currency exchanges.

However, one additional impact will be that individuals or firms who are discovered allowing their accounts to be used for laundering the proceeds of fraud as money mules are more likely to have services withdrawn and will find it more difficult to open accounts elsewhere because of spreading of the cost of reimbursement to all receiving PSPs.

### *2. Do you have views on the impact of our proposals on PSPs?*

BSA members have asked for clarification on the impact of these proposals on savings provider PSPs– see "The building society context" above. We would be grateful if the PSR could confirm this.

Members have also raised concerns about the disproportionate impact of the 48 hour reimbursement role on smaller savings provider PSPs with lower APP fraud risk – see 11 below.

We broadly agree on the consultation's wider assumptions around the impact on PSPs.

*3. Do you have views on the scope we propose for our requirements on reimbursement?*

We broadly agree with the consultation proposals on payments and payment service providers in scope - subject to clarification on the scope of "sending PSP" – see "The building society context" above – and on the definition of an APP scam.

We welcome the exclusion of private civil disputes from the scope of APP fraud reimbursement as it is completely inappropriate for a PSP to reimburse in circumstances where they have had no part in the sale negotiation other than releasing a payment to have liability for reimbursement – and even more inappropriate for a receiving PSP holding the account of a legitimate seller to do so. But, there is a need for further consideration on how this would work in practice so that both consumers and PSPs are clear on where they stand. For example:

- How will the proposed requirement for the sending PSP to reimburse within 48 hours work alongside the time needed for a PSP to determine whether a reimbursement claim is related to actual fraud or to a private civil dispute?
- Would a PSP be allowed to refuse reimbursement where it looks like a claim of fraud is actually a private civil dispute?
- Who would bear the burden of proof – sending PSP or customer?
- How would the receiving account be protected from being identified as being used to receive the proceeds of fraud?

Again, it would also be helpful if this exclusion was reconciled with the Consumer Duty requirement on good customer outcomes.

*4. Do you have comments on our proposals: • that there should be a consumer caution exception to mandatory reimbursement • to use gross negligence as the consumer caution exception • not to provide additional guidance on gross negligence?*

Asking stakeholders to consider whether a gross negligence test should be included as part of mandatory reimbursement without specifying how it is defined and how it should be applied is not helpful. If these proposals are to learn the lessons from implementation of the CRM Code and from FOS' inconsistent application of their own test there should be clear guidance up front on what constitutes "gross negligence" in this context. Otherwise there is a risk that the same inconsistency of interpretation that PSR has highlighted as a major problem for the CRM Code will occur again.

We are pleased to see that PSR has acknowledged the concern that introducing the safety-net of mandatory reimbursement is likely to lead to the unintended consequence of some consumers becoming reckless to fraud risk when making payments because they know that they will not lose out. It is sensible to keep the option of a customer caution exemption under review and we suggest that this is retained as an option beyond the proposed post-implementation review as it may take longer for changes in behaviour to show through in data from PSPs.

We appreciate the PSR's point about lack of evidence of such changes to consumer behaviour following the implementation of the CRM Code and TSB's reimbursement scheme but mandatory reimbursement as proposed in this consultation is a completely different proposition and therefore an unknown quantity in terms of impact on consumers' behaviour - we also note that TSB's scheme does not offer reimbursement to repeat scam victims so

cannot be directly compared. This makes the proposal to retain the option to introduce a consumer caution exemption even more appropriate -we suggest that Pay.UK, as the organisation charged with monitoring implementation of mandatory reimbursement, collects and publishes data from PSPs on volumes of reimbursement of reckless payments – for example where individuals repeatedly claim reimbursement for payments made to fraudsters that repeat the same fraud MOs.

This is likely to be a minority of consumers only – those with no related vulnerability issues who repeatedly ignore warnings / advice that payments may be fraudulent - but could still be a significant, unwarranted cost to PSPs. It is also important to retain a customer caution element to support the deployment of Confirmation of Payee and other measures designed to make the consumer aware of fraud risk – if there are no consequences for ignoring warnings received the considerable investment in CoP etc. will not generate the reduction in frauds that is expected. There also has to be recognition of the principle of the Consumer Duty and the “caveat emptor” principle of UK contract law, both of which stress that that consumers should take responsibility for their own decisions.

While we have no detail to verify this assumption (see above) , our view is that the gross negligence provision would be inappropriate as a framework to counter such behaviour as typically the evidence for reckless behaviour will be a series of lower level incidents rather than a major event that would trigger the “gross negligence” threshold – for example, a repeated pattern of ignoring warnings may be too low level to be defined as gross negligence but is clearly reckless behaviour in the context of fraud risk.

The consultation proposal to keep the option of a customer caution exemption additional to gross negligence under review is sensible and appropriate and we suggest that this is retained as an option beyond the proposed post-implementation review as it may take longer for changes in behaviour to show through in data from PSPs.

*5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?*

In principle, using broad brush assumptions in the context of supporting vulnerabilities is contrary to the FCA’s objectives in their guidance to firms on supporting vulnerable consumers and – the onus being on identifying characteristics of vulnerability individually and putting appropriate support in place for each individual – and so we do not support this proposal. We would also be concerned that establishing a requirement for consumers identifying as vulnerable to be reimbursed for or bad decisions resulting in APP fraud creates too much of a precedent for other reimbursement of losses from poor decisions in other, non-APP fraud contexts. Also, where a declaration of vulnerability appears to be retrospective. A BSA members summarised this concern as follows:

*“As there are different categories of a vulnerable customer, we do not agree that every vulnerable customer should be exempt from gross negligence. A vulnerable consumer could be someone who has broken their arm – how would this make them exempt? We feel that guidance should be provided, and financial institutions should provide their own judgment, especially as they are already required to identify vulnerabilities. Consumers are also partly required to inform financial institutions of their vulnerabilities. If a consumer’s vulnerability is known before a transaction, and is a contributing factor, then we agree for reimbursement. However, if a vulnerability is only declared after the event, then it shouldn’t be an automatic refund decision”.*

Members also highlighted that sending and receiving PSPs may have different relationships with the individual due to the nature of the products held and therefore different perceptions of their vulnerability: *“Could this risk increased liability disputes should one PSP deem a consumer vulnerable and reimburse but another does not deem them vulnerable and there has been gross negligence (i.e. controls deliberately evaded)”*.

We would prefer that claims for reimbursement for APP fraud losses based on vulnerability contain a clear causal link between consumer’s individual circumstances and the decision to pay to the fraudster and that PSPs have the right to challenge claims that appear to use vulnerability to attempt to game the reimbursement rules and conceal failures of judgement.

In practice, it is likely that the causal link between characteristics of vulnerability and unwise decisions leading to becoming a victim of APP fraud with serious losses will be clear and obvious for most cases (and therefore not gross negligence) and that challenges will be few and far between:

- Some consumers have vulnerabilities that impair their decision making capability and therefore make them particularly vulnerable to APP fraud – decisions that these consumers make would not be likely to qualify as gross negligence.
- Consumers who have made payments to fraudsters having been the subject of grooming or consistent deception may have acted unwisely when looked at objectively but were making decisions framed by the fraudsters’ manipulation of them – also not likely to qualify as gross negligence.

*6. Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?*

This is a sensible proposal as it will provide a welcome consistency of approach between regulators on an area where consistency is so important to both customers and to firms. The FCA’s definition also gives firms the scope to treat vulnerable individuals individually with bespoke support appropriate to their circumstances.

*7. Do you have comments on our proposals that: • sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement • any ‘excess’ should be set at no more than £35 • PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?*

*8. Do you have comments on our proposals that: • sending PSPs should be allowed to set a minimum claim threshold • any threshold should be set at no more than £100 • PSPs should be able to exempt vulnerable consumers from any threshold they set?*

*9. Do you have comments on our proposal not to have a maximum threshold?*

We support these proposals in principle but we have not seen any data to judge whether an excess of £35 and minimum claim threshold of £100 and no maximum threshold as proposed are too much or too little. We suggest that all proposals are adjustable under review to see if they are sufficient to deliver the objectives behind them.

Giving PSPs the capability to exempt vulnerable consumers from any excess / minimum claim threshold that they do apply is sensible and fits well with the FCA’s guidance on supporting vulnerabilities.

It would also be sensible to keep the option of a maximum threshold available, particularly for reimbursement claims associated with fraudulent purchase scams where losses are less likely

to be life-altering and the consumer's own responsibility under "caveat emptor" is higher than for other types of APP fraud.

*10. Do you have comments on our proposals that: • sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement • any time-limit should be set at no less than 13 months?*

As above, we support this in principle and suggest that the no less than 13 months proposal be trialled to check its effectiveness against the PSR's objectives – though clarification will be needed as to what point the clock starts ticking on any time period. The start point could be either the date that the Faster Payments transfer to the fraudster took place or the date that the customer realised that they had become a fraud victim but clarification is important as there could be a significant time difference between the two dates.

Members are particularly concerned about cases involving a series of payments to a fraudster. If the 13 months is from the final payment in the APP scam, then with some types of scams, especially for example romance scams, PSPs could be liable for payments much further back than 13 months. The proposal does not seem to confirm whether the 13 months would be retrospectively applied when the regulation is introduced.

*11. Do you have comments on our proposals that: • the sending PSP is responsible for reimbursing the consumer • reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?*

While in agreement with the rest of this proposal, BSA members have raised concerns around applying the 48 hour requirement to PSPs that offer savings products and so to not operate 24/7, 7 days a week as the fraud risk associated with their products does not warrant this. While it is sensible for current account providers and others with higher APP fraud risk (where it should be already in place), requiring introduction of the infrastructure to support the 48 hour requirement for lower risk PSPs would be a disproportionate cost to savings providers and their members / customers which will not be offset by reduced APP fraud losses.

*"There should be recognition that smaller firms do not operate 7 days a week / 365 days a year. In addition to the time it takes to conduct enquiries / investigation, not all BS are members of CIFAS which is often used a verification method before supporting another firm with an investigation. It would be beneficial for there to be encouragement for firms to support each other in investigations within the 48 hr window without presence of CIFAS membership for example".*

*"48 hours even if working days is recognized, industry wide, to be inadequate time to complete robust fraud investigations".*

*"Some smaller organisations such as ourselves (a small building society providing savings products only) may struggle with a 48 hour timescale. We think a longer timescale should be considered".*

We would welcome discussions with the PSR on a differentiated approach for savings account providing PSPs with lower APP fraud risk.

Members also asked for clarification on:

- Whether 48 hours was calendar or working day
- Will there be any conditions / expectations set as an industry standard regarding victim co-operation? i.e. to support reimbursement timescales, victims must

cooperate with investigation and provide reasonable response to requests for evidence.

It will also create some communications challenges in terms of managing consumers' and consumer groups' expectations. In particular, what messages should PSPs relay to reimbursement claimants when they do have suspicions of first party fraud or gross negligence and how should they balance the need to keep the claimant informed, the need to progress their investigation unhindered and the risk of inadvertently labelling the claimant as "criminal" or negligent" until investigations are complete.

Again, reviewing actual experience with implementation of the 48 hour proposal will be important in ascertaining whether the proposal is meeting the PSR's objectives.

*12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?*

It is impossible to develop any workable standard for investigation of gross negligence without a definition of what "gross negligence" means. But, subject to clarity on what this means, members have suggested the following as potential evidence of gross negligence:

- Breach of T&C's e.g. attaching a nominated account not in the consumer name
- Suspected fraudulent documents
- Evidence of COP fail being ignored
- Evidence of other warnings – e.g. via the Banking Protocol – being ignored
- Little to no care/due diligence carried out by the victim in scenarios of increased complexity and/or are considered atypical.
- Refusal to co-operate with investigations.

For first party fraud, the individual under investigation has potentially committed a criminal offence and so the standards of evidence that might lead to a decision as to whether or not to peruse a criminal prosecution seems the most appropriate. It is difficult to generalise as to how long an investigation might take – this may include police involvement - but it will certainly be more than 48 hours. Time limiting investigation in this context would hand an advantage to the criminal and would potentially encourage more collusion scams.

Presumably, PSPs will also be allowed time to determine whether a reimbursement claim is in fact a private civil dispute rather than fraud – see 3. Above.

As with the other proposals above, it would be sensible to collect some examples of actual investigations before finalising the requirement. Guidance also needs to be given as to how PSPs balance informing the customer of a delay in reimbursement against the need avoid tipping off the customer that they are under investigation – see 11. Above.

*13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?*

We support this proposal.

But, the statement within the consultation that that "Receiving PSPs are providing the accounts that fraudsters control and that they use to implement APP scams" is concerning as it ignores the reality that in many cases the account holding customer is providing the account that the fraudster is using to receive the proceeds of fraud – sometimes innocently but sometimes deliberately.



It is important that any package of measures against fraudsters allows receiving PSPs to robustly discourage account holders from becoming money mules even if that means that some consumers who do not follow warnings not to let their accounts host proceeds of crime find obtaining financial services more difficult as a result.

Feedback from BSA members also raised the issue of treatment of receiving PSPs which consistently demonstrate lack of proper AML or money mule controls. This was alluded to earlier in the consultation in a scenario where sending PSPs could legitimately refuse to send Faster Payments to these PSPs. BSA members have suggested that it would be a more effective incentive for these organisations to improve if the PSR or a PSO has the ability to vary the 50:50 allocation to allocate more reimbursement cost to the failing PSP rather than penalising consumers by refusing their payment requests.

*14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?*

We agree with this in principle.

But, development of more tailored criteria for allocation, and associated dispute resolution arrangements designated into scheme rules must include checks and balances so that there are no unintended consequences which undermine the PSR's objectives of maintaining fair competition in the payments sector.

- Firstly, any designated set of more tailored allocation criteria can only be applied fairly as long as all types of PSP have equal access to the intelligence sharing mechanisms between sending and receiving PSPs currently under development and referred to earlier in this consultation. This would include pricing the service so that it doesn't cost smaller PSPs disproportionately more as well ensuring that the technical delivery allows equal access for agency banking users and other non-current account business models.
- Recent experience shows that fraud prevention initiatives – for example CoP and the CRM Code – are initially designed for current account providing PSPs with development to support non-current account business models lagging behind. As with the other two examples, there could well be a significant period of two tier fraud protection while development for other business models catches up when it would be discriminatory to apply inappropriate allocation criteria against PSPs unable to take the service.
- Secondly, the criteria must align with regulatory requirements. For example, the PSR has recognised differentiated fraud risk in allowing PSPs who offer restricted Faster Payments transfers to the account holder's current account only to opt not to implement "send" Confirmation of Payee. Tailored allocation criteria should not then disadvantage PSPs who have taken this option.
- Finally, any allocation criteria will need to be cost effective and address unequal negotiating power to ensure that a choice to depart from the 50:50 allocation is genuinely supported by both parties – a larger organisation can deploy far greater legal leverage in negotiation, mediation or dispute resolution than a smaller PSP can. Again it would be discriminatory were the cost and complexity of proceeding to hit smaller PSPs disproportionately.

We understand that PSR is currently in discussion with UK Finance on the possible structure of a set of tailored acquisition criteria and would welcome the opportunity for the BSA and other trade bodies representing smaller, non-current account providers to be included.

*15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?*

Our assumption is that the multi-generational scams outlined in the consultation start with the sending PSP i.e. the PSP which the customer authorised to make a payment to the fraudster.

*16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?*

We agree. Any repatriated funds should mirror the original repayment split.

*17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?*

We agree – though the trend of fraudsters targeting PSPs who did not (or, in the case of building societies, until recently could not) adopt CoP has not been apparent for BSA members.

*18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?*

We see the sense in there being a one-stop PSO for payment systems with fraud prevention and consumer protection as part of its remit.

However, from the perspective of a sector where the majority of building societies are indirect PSPs and therefore at arms' length from Pay.UK's governance and operations, Pay.Uk is not ready to step into this role.

- Pay.UK is a membership organisation and is accountable to the group of large banks that make up its membership. How does the PSR envisage Pay.UK being a rule setter for these PSPs and might not there to a potential competition issue of a group of PSPs being able to influence the creation of scheme rules etc. when other PSPs to whom the rules will also apply do not have the same influence?
- As noted in this consultation, Pay.UK cannot currently apply Faster Payments scheme rules directly to indirect PSP participants in the payment system. Does PSR envisage a long term change to Pay.UK's constitution in order to address that?
- Pay.Uk currently doesn't have the experience and understanding of non-current account business models needed to develop scheme rules, monitoring and enforcement arrangements suitable for PSPs using other business models.
- If it is to be an effective cross-sector PSO it will need to significantly improve its communication to / interaction with indirect PSPs, which is currently not at an appropriate level to be able to take on its proposed role.

Preparing Pay.UK for the PSO role will require significant changes to its constitution and management culture. The BSA would be happy to support the process of re-aligning Pay.UK into an organisation fit to take on a PSO role in the longer term.

*19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?*



We support the proposal subject to clarification of a number of points discussed above. In particular, the initial Faster Payments rules set should include clear definition of gross negligence.

*20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?*

We have no comments on this issue.

*21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?*

We support the principles set out in the consultation. See 14 above for additional comments.

*22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?*

*23. Do you have views on the costs and benefits of Pay.UK implementing a real time compliance monitoring system and when it could be introduced?*

We agree that a reporting requirement on PSPs is the best short term option for monitoring compliance with the proposed reimbursement requirements rather than waiting for delivery of a real time monitoring system. As with any system of its kind, this should be aligned with existing reporting for internal MI and for trade bodies so that the additional admin burden on PSPs is kept as low as possible. We assume that the reporting requirement will include nil returns where appropriate.

Bearing in mind, that Pay.UK currently has no jurisdiction over indirect PSPs we suggest that the reporting requirement is voluntary for indirect PSPs on the basis that pressure from consumers and consumer groups will make it difficult for any PSP to opt out.

We are unable to comment on the feasibility / cost of building a real time compliance monitoring system.

*24. Do you have views on the best option for short-term enforcement arrangements?*

*25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?*

*26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?*

All but one BSA member are indirect PSPs in the Faster Payments context so, as the consultation notes, Pay.UK would have no enforcement jurisdiction over them. Any imposition of formal short term enforcement arrangements on indirect PSPs would require a suitable direction from the Payment Systems Regulator.

In practice, the role of formal enforcement will be offset by consumer expectations. Pressure from the media and consumer groups on PSPs to follow the Faster Payments rules on reimbursement is likely to be as much of if not more of an incentive for PSPs to comply than any formal direction or enforcement arrangements. Our assumption is that media / consumer groups will be actively scrutinising how they are implemented and that PSPs – direct or indirect - would risk severe reputational damage if they were exposed as not following rules.

*27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?*

BSA members have made the following points on the costs of this proposal:

- APP fraud has cost the industry an average of £500m annually since 2020, these losses may increase as a result of mandatory reimbursement and the anticipated increase in recklessness towards fraud of some individuals. This will impact portfolio pricing and result in reduced consumer value in product offering across the industry to allow PSPs to cover costs. Given the current economic climate firms need to be encouraged to pass value back to consumers. Increasing operating costs (especially where firms cannot reasonably be expected to prevent all fraud/scams) will have detrimental impact on all consumers.
- Shifting the burden of funding APP fraud losses almost entirely to PSPs will result in burden that some smaller firms are unable to bear, and may result in reduced enterprise across the industry – ultimately stifling innovation and competition
- The outlined proposals will take significant investment to implement which WILL NOT be offset by a reduction in losses for PSPs with lower APP fraud-risk product portfolios as it will be with the tier 1's.
- The consultation's cost benefit analysis has ignored the opportunity cost of funding APP fraud reimbursement - which will include the potential to offer lower lending and higher savings rates (both much needed in the context of the cost of living crisis) as well as the opportunity for PSPs to invest money spent on reimbursement in efficiency / controls / good customer outcomes.

*28. Do you have any other comments on the proposals in this consultation?*

No further comments

THE BUILDING SOCIETIES ASSOCIATION

24 November 2022

By [REDACTED]  
Policy Manager – Financial Crime

York House  
23 Kingsway  
London WC2B 6UJ

020 7520 5900  
@BSABuildingSocs  
www.bsa.org.uk

BSA EU Transparency Register No: 924933110421-64

[www.bsa.org.uk](http://www.bsa.org.uk)

The Building Societies Association (BSA) is the voice of the UK's building societies and also represents a number of credit unions.

We fulfil two key roles. We provide our members with information to help them run their businesses. We also represent their interests to audiences including the Financial Conduct Authority, Prudential Regulation Authority and other regulators, the Government and Parliament, the Bank of England, the media and other opinion formers, and the general public.

Our members have total assets of over £400 billion, and account for 23% of the UK mortgage market and 19% of the UK savings market.

# Call Sign

## Payments Systems Regulator Consultation Paper CP22/4 Authorised push payment (APP) scams: Requiring reimbursement

---

### Callsign response

November 2022

#### Introduction

Founded in 2012, Callsign is a British technology company and a global pioneer in digital identity and fraud prevention. We have developed the first identification platform in the world that uses artificial intelligence to build digital DNA to authenticate users with unparalleled accuracy – right down to the way users type and swipe. Our technology is built on the foundation of privacy, confidentiality, and the protection of user data, with the very highest levels of encryption.

We work with 60% of the UK consumer banking market, helping our clients to authenticate users, meet Strong Customer Authentication (SCA) requirements under PSD2, and tackle social engineering and APP scams.

In 2020, Callsign participated in the Financial Conduct Authority (FCA) and City of London's Digital Sandbox Pilot alongside one of our banking partners to develop our 'dynamic fraud intervention' solution, which aims to tackle APP fraud.

#### Callsign's response

We have focussed our response on specific questions within the consultation paper. Our recommendations focus on the potential measures that could be introduced to enable Payment Service Providers (PSPs) to tackle fraud at scale and prevent APP scams from reaching consumers in the first place.

We would be delighted to discuss any elements of our submission in further detail. We look forward to continuing to engage with the PSR on this important topic.

#### **Question 1: Do you have views on the above impact of the PSR's proposals on consumers?**

We support the PSR's ambition to increase the level of protection for consumers and to support the victims of APP fraud. As well as financial losses, the negative psychological impact of social engineering on individuals can be significant. More broadly, fraudulent activity online can result in a loss of digital trust across society.

We believe, however, that a focus on reimbursement alone will not be enough to reduce levels of fraud. More should be done to detect and prevent scams upfront, before they take place.

If there is a sole focus on reimbursement, it arguably has the potential to increase certain types of fraud such as first-person fraud, with individuals looking to exploit the reimbursement process, particularly when combined with a short time window for returning funds. This is something that was observed during the Covid-19 pandemic, when emergency government support schemes were exploited by individuals making false claims to receive grants. Current reports from the National Audit Office estimate that £4.5bn of government support was claimed in error or in fraud<sup>1</sup>.

---

<sup>1</sup> <https://www.nao.org.uk/wp-content/uploads/2022/10/Summary-Delivery-of-employment-support-schemes-in-response-to-the-COVID-19-pandemic.pdf>

Whilst banks will be looking to exempt all cases of first party fraud, there is a potential situation where it becomes more costly and resource intensive to investigate suspected first party fraud cases than it is to simply process a reimbursement.

To truly reduce levels of APP scams, greater detection and upfront prevention is needed. PSPs should be encouraged to make use of technology solutions that can detect fraudulent activity and prevent scams from taking place.

Additional interventions during the payment journey, and therefore increased friction, will be needed where transactions appear suspicious. However, this should not be to the detriment of users carrying out legitimate activities.

Scam warning messages that are presented to consumers during legitimate transactions create undue friction in the user journey and have become perceived as commonplace in the payment process. This ultimately decreases users' sense of the importance of warnings, encouraging them to click through without due consideration of the message's contents. Scam warnings need to be relevant, timely and contextual to the user journey. This is discussed further in the response to question 2.

## **Question 2: Do you have views on the impact of our proposals on PSPs?**

All PSPs should be encouraged to put in place effective fraud controls and work proactively with providers of technology who can support them in the most cost-effective way.

New technology solutions can draw on multiple intelligence sources and, when a risk is identified, adjust the user journey in real time with dynamic fraud messages that are tailored to the user. Messages can be presented only when intelligence suggests that there is a suspicion of fraud to minimise the impact on the customer experience.

Where fraudulent activity is suspected, messages can be displayed including questions such as:

- "Were you expecting to make this payment today?"
- "Have you received a phone call related to this payment?"
- "Are you on the phone currently?"

The messages are dynamic, presenting follow-up questions based on the answers given. By making the alerts contextual and specific, they are more likely to be properly acknowledged. This is in comparison to the generic scam warning messages that have become commonplace in online banking journeys and their content easily ignored.

These messages can be used for several purposes, including to capture additional information on the purpose and context of the payment; provide additional user interactions for behavioural analytics; and to help the PSP and/or customers to identify that a scam is taking place. They also provide a means for the consumer to effectively "digitally sign" their confirmation for the transaction. These analytics are fed back to PSPs' transaction monitoring services to enrich their fraud models and drive operational intervention via their case management capabilities, removing the need for further portals or the duplication of generated alerts within the operational area of the bank.

As part of any consumer caution exemption claims, PSPs will need to show that they have presented effective warnings which are relevant, timely and contextual to the user journey, and that the consumer has read and acknowledged these. Collaboration with other sectors (big tech, online platforms etc) is crucial.

**Question 4: Do you have comments on our proposals?**

- that there should be a consumer caution exception to mandatory reimbursement
- to use gross negligence as the consumer caution exception
- not to provide additional guidance on gross negligence.

As outlined in the consultation paper, fraudsters' tactics and the sophistication of social engineering scams are continuously evolving. The innovative technologies designed to protect consumers are developing fast to keep up with the changing fraud landscape. Fraud prevention solutions must be dynamic and able to quickly respond to new, emerging threats. Consumer interactions and behaviours will adapt over time as a result.

It would therefore be challenging to place a static definition on a consumer exception, whether that be based on gross negligence or otherwise. PSPs should be encouraged to work closely with the Financial Ombudsmen Service (FOS) to ensure that a reasonable and fair view is taken in individual cases.

As awareness of new fraud tactics develop, PSPs will need to present targeted interventions that are tailored to individuals and their specific circumstances during their online interactions. Data review and analysis could give an indication of how the definition may need to evolve.

**Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer.**

We note that the FCA's definition of vulnerable customer, based on "personal circumstances" may not capture groups of society who are commonly targeted by scammers and therefore at a high risk of fraud. Under 35s, for example, are more likely than older age groups to have been targeted in an impersonation scam and be swayed to provide personal or financial information<sup>2</sup>, and undergraduate students are frequently targeted by sophisticated social engineering scams.

Please forward any queries relating to the above response to: [REDACTED]

---

<sup>2</sup> <https://www.ukfinance.org.uk/press/press-releases/uk-finance-people-under-35-are-more-risk-impersonation-scams-0>

# Citizens Advice Scotland



## Confirmation of Payee Consultation Citizens Advice Scotland Response

*Scotland's Citizens Advice Network is an essential community service that empowers people through our local bureaux and national services by providing free, confidential, and independent advice. We use people's real-life experiences to influence policy and drive positive change. We are on the side of people in Scotland who need help, and we change lives for the better.*

Citizens Advice Scotland agrees with the proposal to require reimbursement of Authorised Push Payment scams. The impact of scams can be devastating for our clients and the cost-of-living crisis exacerbates the consequences of losing money to a scam. Guaranteed reimbursement will therefore be a huge support to our clients who fall victim to APP scams. We also think these changes will serve as an incentive for financial service providers to prevent scams being carried out in the first place.

### **£100 minimum threshold and £35 excess**

We are concerned by PSR's proposals to allow a threshold of up to £100 and an excess of up to £35. Although APP scams under £1,000 represented only 8% of losses in 2021, losing what might be considered small amounts of money can mean being unable to put the heating on or put food on the table for low-income customers. This provision could therefore exclude consumers most at risk of the harms of scams. We therefore urge the PSR to remove the provision to introduce a minimum threshold for reimbursement.

Our statistics on 2,987 CAB clients with complex or multiple debt issues between April 2021 and March 2022 reveal an alarming picture of falling income and increased expenditure leading to an increase in clients with insufficient incomes to meet their living costs<sup>1</sup>. Nearly 1 in 2 clients did not have any disposable income after covering their essentials and many did not have enough to even cover essential bills - locking them in a monthly cycle of prioritising what to spend money on. For these clients, paying a £35 excess will mean spending less on heating, eating, or paying for other essentials, which is likely to have dangerous consequences for their health and wellbeing. We would therefore also like to see the provision for firms to be able to introduce an excess removed.

### **Gross Negligence Exception**

We think that the exception in cases of gross negligence is an appropriately high bar to set which will incentivise financial service providers to invest in scams prevention so that they can intercept and stop scams before they occur. Like PSR, we have not seen any evidence to suggest that guaranteed reimbursement will result in reduced consumer vigilance against

---

<sup>1</sup> Citizens Advice Scotland, [An Analysis of Living Standards in Complex Debt Cases](#), November 2022

scams. We also agree with the PSR's proposal to exempt vulnerable consumers from the proposed gross negligence exception, we think this will encourage PSPs to provide appropriate support to prevent vulnerable customers falling victim to a scam.

We would encourage the PSR to publish some guidance on what would not be considered gross negligence. There is a lot of shame associated with falling victim to a scam and we tend to find that consumers tend to place a disproportionate amount of blame on themselves. We therefore worry that the gross negligence exception may put some consumers off claiming reimbursement due to a misunderstanding of the term. Clear examples of what would not be considered gross negligence may provide consumers with more confidence that they can and should claim reimbursement.

### **Additional Considerations**

We understand that these changes will likely result in an increase in payments being stopped or/and an increase in security measures when making payments. It is important that measures taken by banks are inclusive and considerate of the diverse needs of their customers. For example, One Time Passcodes when making payments can be challenging for customers with limited digital literacy unless adequate support is offered by customer service teams. Additionally, we often find that clients who are digitally excluded can struggle to contact their bank when they require support. For example, their bank may not have a branch locally or telephone lines might be subject to long waiting times. Financial service providers will therefore need to offer accessible, multi-channel support for customers who have genuine payments blocked and customers struggling to adjust to additional security checks – banks should be encouraged to plan for how they will adequately meet this subsequent increase in demand.

### **Conclusion**

To conclude, we are very much in favour of the measures set out by the PSR. However, we would like to see the provisions to introduce a minimum threshold, or an excess removed as they serve to exclude and/or cause harm to banking customers on a low income.

### **For further information, please contact:**

The Financial Health team  
[financialhealth@cas.org.uk](mailto:financialhealth@cas.org.uk)

# Clear Junction

### **Question 1: Do you have views on the impact of our proposals on consumers?**

The provision of reimbursement needs to be set properly so as not to provide an incentive for consumers to act more recklessly when making APP payments. If the level of fraud decreases, this is of course a positive for consumers in terms of cost and confidence in the payment system.

Although the consultation recognises that groups that are more susceptible to APP scams should not be treated differently, such discrimination may still occur by stealth and costs for all consumers may increase to offset the losses from such susceptible groups.

By trying to reduce fraud, the PSR needs to ensure it is not restricting competition and increasing costs for consumers, essentially taking the payment system backwards.

### **Question 2: Do you have views on the impact of our proposals on PSPs?**

There is a concern that increasing the costs of reimbursement may have a number of negative consequences for the payment market and receiving PSP's more particularly.

A good example is one of a PSP that services corporate clients only, and those corporate clients may in turn service consumers. Typical examples would include remittance providers or product marketplaces.

In such circumstances, the corporate client may receive thousands of payments a day in a variety of sizes. It would therefore be incredibly difficult for the receiving PSP to determine if any single transaction (or even a series of transactions) was part of an APP fraud.

In such circumstances, the impact on receiving PSP's could include

- passing the costs on to their corporate clients thereby making both the PSP and the corporate client less competitive
- receiving PSP's who are unable to bear the costs may stop providing services altogether leading to reduced choice for businesses and consumers
- receiving PSP's reducing risk around the payments they receive by preventing receipt of large payments and/or scrutinising every payment thereby causing increased friction and time lag in the payment system
- single large frauds could cause even well capitalised PSPs to fall into liquidation if they were unable to recover from their corporate clients

### **Question 3: Do you have views on the scope we propose for our requirements on reimbursement?**

#### **Question 4: Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

Consumers should certainly not be given a perverse incentive to act negligently when making payments. On this basis a consumer caution would be necessary and set at level that is less than the proposed gross negligence level.

Gross negligence is a difficult term to determine under English law and signifies something extraordinary. Given the general public awareness of APP scams it would be reasonable to expect that consumers should consider discussing making non-vanilla payments with a family member, their PSP or trusted advisor.

It should be reasonable to expect that consumers should undertake an appropriate level of research and diligence before making payments that are large, in relation to investment products or would be outside the course of their usual spending habits.

**Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We agree that the level of caution for vulnerable consumers should be lower, however a blanket duty to reimburse may not be appropriate as this may encourage additional claims under this exemption.

**Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

The FCA definition is clearer than the CRM Code.

**Question 7: Do you have comments on our proposals that:**

- sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- any 'excess' should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

**Question 8: Do you have comments on our proposals that:**

- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?

**Question 9: Do you have comments on our proposal not to have a maximum threshold?**

A £25,000 maximum threshold could be considered reasonable.

Making a payment for over £25,000 to anyone is unlikely to be typical day-to-day transactions for most consumers – the purchase of a house, car or investment would probably be the most common scenarios. In such circumstances, it is not unreasonable to

expect the consumer to have undertaken an appropriate level of care and diligence before making the payment.

If a consumer is insisting on making such payment, even the strongest PSP safeguards aren't going to be effective and so the consumer would need to be aware of the risks they are taking.

**Question 10: Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

Having potentially unknown liabilities on a balance sheet for such a long period can be risky for businesses and may tie up liquidity.

A 6-month maximum period may be more appropriate given the time frame for discovery of such frauds and it is analogous to the standard period when chargebacks are allowed in card payments.

**Question 11: Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

Given the sending PSP will have the greatest visibility over the consumer's payment habits, it would be reasonable for them to employ the first line of defence. If this isn't robust enough, then it is reasonable that they should reimburse the consumer in the first instance. The time frame is difficult to agree to given the potential complexities that may be involved with a given APP fraud. It may be more appropriate to make this period 72 hours to allow any new information to come to light.

**Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

This would have to be on a case-by-case basis. Certainly, the consumer should be willing to provide full details of the scam as soon as possible which should allow the PSP to review and see if there was any point at which the consumer should have raised concerns

**Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

A default 50/50 split seems wholly inequitable given the relevant position and knowledge of the sending and receiving PSP

As stated in the response to Q2 and Q11, the sending PSP is likely to have the greatest visibility on the consumer and their payment patterns. The consultation paper has

referenced that - *“Receiving PSPs are providing the accounts that fraudsters control and that they use to implement APP scams. Receiving PSPs need adequate incentives to detect frauds and prevent fraud losses”* however these comments appear to be generalist and over simplistic.

As in the example in Q2, a receiving PSP may well not have provided the account to a fraudster but to a reputable company that has gone through a full diligence process. At the point where a fraudster wishes to open an account with that company, provided the fraudster has passed all relevant AML/KYC checks, it would be incredibly difficult to ascertain that they are in fact a fraudster.

The consultation paper states that the receiving PSPs need to be incentivised to prevent fraud, but there is no indication as to how they can do this given the limited information they would have regarding a payment.

Fraud is typically detected by unusual size or volume in relation to the particular account, where neither are present then how are receiving PSPs to improve their fraud detection rates? This is a pertinent question for the PSR to consider.

It would make more sense if the PSR were to provide best practice guidance on how receiving PSPs could assist in the fraud detection process. If a receiving PSP were then seen to be failing versus such best practice then it would be reasonable to apportion part of the reimbursement against them.

**Question 14: Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

PSPs should certainly have the opportunity to discuss appropriate allocation of costs outside whatever default is agreed. However, the wider point we would re-iterate is that the current 50/50 split doesn't reflect an accurate allocation of risk and responsibility.

**Question 15: Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

As stated in the response to Q13, the allocation of reimbursement should be based on the actual knowledge the relevant PSPs had at the time of the payment and to what extent they followed best practice to reduce the risk of fraud. In a multi-generational scam, it would be inequitable to have a PSP that has received what appears to be a standard payment from a corporate customer to have to consider the original source of such transfer (which could be several layers earlier). If PSPs are unable to rely on each other to have taken the appropriate level of caution and best practice, then faith in the entire payment system would be at stake.

**Question 16: Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

It would seem sensible that repatriated funds are returned pro-rata to the PSPs that have made the initial reimbursement

**Question 17: Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

It would be reasonable that all PSPs are subject to any rules regarding APP fraud. This should encourage them to join schemes such as CoP (where possible) to demonstrate their compliance with best practice.

**Question 18: Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

Provided the PSO engages with the industry with regard to future rule-setting, this would seem to be a sensible route

**Question 19: Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

**Question 20: Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

**Question 21: Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

Whatever route is taken, any such arrangements should be made clear so that all affected PSPs are fully aware of the processes

**Question 22: Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

Any additional reporting requirements should have minimal impact on day-to-day operations for PSPs given the already heavy regulatory burden they face. Pay.UK should only request the minimum information it requires, and this should be done in a format that is easily completed and can ideally be automated.

**Question 23: Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

This should take into account the additional time and cost of such reporting on PSPs, should request the minimal information required and be in a format that allows it to be automated insofar as possible.



**Question 24: Do you have views on the best option for short-term enforcement arrangements?**

**Question 25: Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

**Question 26: If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

**Question 27: Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

**Question 27. Do you have any other comments on the proposals in this consultation?**

We believe that reducing APP fraud is certainly something the PSR should assist with.

However, the currently proposed circumstances for reimbursement fall short in three main areas –

1. The burden of proof (i.e. where there hasn't been gross negligence) seems unduly weighted towards consumers in light of the level of existing public knowledge and ability for potential scams to be researched.
2. The mandatory 50/50 split between sending and receiving PSPs doesn't reflect the level of risk, knowledge and practical ability to prevent such fraud. The split should be primarily weighted towards the sending PSP unless the receiving PSP is shown to have demonstrably failed to meet best practice.
3. The PSR has provided no depth of rationale as to why receiving PSPs should be included within the mandatory reimbursement regime. Given the receiving PSPs will typically have access to the least amount of knowledge regarding a payment (versus the consumer and the sending PSP), it would seem more sensible to provide them with a best practice guide so they can assist more easily in reviewing transactions and recovering funds for high risk transactions

# ClearBank

## Authorised push payment (APP) scams: Requiring reimbursement (CP22/4)

### ClearBank Limited Responses

Question	CB Answer
1 Do you have views on the impact of our proposals on consumers?	<p><b>CB response</b></p> <p>In the short term, while all payment services providers (PSPs) must comply with Equality Act 2010 obligations to not discriminate against persons with disabilities, the increased risk requirements are likely to reduce access to payment services for consumers who are part of groups identified as “high risk” for fraud. In the longer term, fraud risk identification techniques, PSP-to-PSP information sharing facilities, and improved prevention measures should ease PSP customer restrictions. However, we are also concerned that such customer segments are likely to be served by smaller and niche PSPs. If smaller and niche PSPs leave the market because they cannot meet uncapped liability obligations this may reduce access to payment services for some vulnerable consumers in the longer term.</p>
2 Do you have views on the impact of our proposals on PSPs?	<p><b>CB response</b></p> <p>ClearBank is not a Contingent Reimbursement Model Code (CRM Code) subscriber. As such the mandatory reimbursement obligation will create a new unfunded, uncapped head of liability and require significant implementation and ongoing operational costs. The obligation will also have significant commercial impacts for us and other firms that are not CRM Code subscribers.</p> <p>Regarding costs, we refer to paragraph 3.8 of the Consultation:</p> <p><i>“If reimbursement costs were large enough for some small PSPs, this could, in principle, have prudential implications. We do not consider prudential risks would arise for larger PSPs, many of which are already CRM Code signatories. We continue to work with the FCA and the Prudential Regulation Authority (PRA) on how risks to individual small PSPs would be monitored and managed.”</i></p> <p>The financial implications will be significant for <u>all</u> PSPs that are not CRM Code subscribers, not merely the smallest PSPs. The number of CRM Code subscribers today, ten PSPs, represents only a very small number of PSPs. According to the PSR’s January 2022 Access Report (1), there are around 40 Faster Payments System (FPS) direct access PSPs, ten of which are indirect payment clearing providers and (2), 1500 indirect access PSPs in the UK market. Mandatory reimbursement will require all non-CRM Code subscribers to invest in new systems and hire additional complaints, investigations, disputes and reporting staff and the reimbursement costs will be a substantial increase to what most PSPs accrue for fraud liability today.</p> <p>For ClearBank and other new and growing banks (e.g. “Challenger Banks”) that are not CRM Code subscribers, the Prudential Regulation Authority (PRA) will likely require credit institutions to set aside additional Pillar 2 capital requirements.</p> <p>We believe that these costs and the general nature of an uncapped liability will see PSPs of all sizes leave the PSP market. This will reduce competition and provide a disincentive for firms to invest in consumer payment services, undoing much of the innovation that has flourished in the UK payments market since the introduction of the Payment Services Regulations 2017 (PSRs 2017). As such we believe that further impact analysis must be undertaken to understand the true cost to non-CRM Code subscriber firms and estimate the impact on competition in the UK payments market. We propose that the regime is tailored per the recommendations in our response to be proportionate to the 1500+ strong PSP community. Further, meaningful protections under the Online Safety Bill should also be introduced to stop scammers enabled by social media and technology firms before the mandatory reimbursement is introduced. See our response to Q9 for more details.</p> <p>Finally, if FPS direct participants are legally liable for indirect participant APP fraud, then this will require direct FPS participants to significantly drive up their credit criteria for new and existing indirect PSPs and potentially place additional funds on deposit against losses. Some PSPs will not be able to meet the raised credit criteria and this will result in many PSPs losing access to payments clearing, undermining competition and innovation in UK payments markets and reducing the downstream availability of payment services to UK consumers. This will also increase the number of POND notifications submitted to the Financial Conduct Authority (FCA) under the PSRs 2017. We note that there is no operational reason why direct participants should be liable - FPS messaging system today provides full transparency of indirect clearing PSPs that operate under their own banks</p>

and sort codes. Imposing liability on FPS direct participants via FPS rules, and not imposing liability on indirect PSPs through a Special Direction, would go against the PSR's mandate to promote effective competition and innovation in the UK payment systems.

Regarding the timing required for implementation, this will largely depend on finalisation of certain scope issues (e.g. whether FPS direct participants are operationally and financially liable for indirect participants) and the development of external industry standards and processes. It is difficult to estimate how long it will take our firm to implement, but such a project will be a complex and firm-wide exercise touching nearly every aspect of our business:

- Executive Committee
- Product Prioritisation Committee (Change management team)
- Public Policy
- Finance
- Data Strategy
- First and Second Line Financial Crime
- Compliance
- Customer care
- Legal
- Client Management
- Product
- Schemes Management
- Marketing & Customer Comms

If final regulations are not available until Q2 2023, we urge the PSR to consider implementation during 2024.

(1) *Access and governance report on interbank payment systems*, PSR, January, 2022

(2) The above report identifies nine as of December 2020, however the recently Authorised Bank of London intends to be a tenth payments clearing provider.

**3** Do you have views on the scope we propose for our requirements on reimbursement?

**CB response**

We support the following aspects of the proposed scope, subject to our comments:

**Scope of Consumers.** We endorse the “consumer” definition proposed, as this is consistent with the BCOBS definition of “banking customer” relevant to our business.

**Scope of payments.** We support the scope of reimbursement as APP scam payments made over the FSP system and On-U.s. However:

- We do not support the extension to CHAPS. This is not necessary as consumer payments are expected to migrate from CHAPS to FPS following the recent FPS limit increase from £250k to £1m. This is not proportionate, as the CRM Code firms that support this today are large PSPs that have the financial resources to reimburse for high value payments. Small and midsized firms would not be able to bear high value reimbursements. The capital requirements for electronic money firms are £350,000 (1) and capital requirements for authorised payment institutions are set even lower (2). A single high value payment could wipe out a PSP's annual profit, or even bankrupt the firm.
- We also are grateful for the proposal to exclude purchase scams, although we note the difficulty in separating APP fraud from such scams. We therefore are in favour of tailoring the threshold level to screen out average purchase scams.

**Application to directly connected as well as indirectly connected PSPs.** The obligation should apply to all account servicing payment service providers (ASPSPs). This term is defined in the PSRs 2017 as “a payment service provider providing and maintaining a payment account for a payer”, and ASPSPs have the relevant direct legal and regulatory obligations with the payment end user. Direct FPS clearing firms have no direct relationship with the payment end users of their indirect clearing customers. We further note that the application of mandatory reimbursement to indirect PSP firms is consistent with a PSP's existing statutory liability for unauthorised fraud reimbursement under regulation 76 of the Payment Services Regulation and the PSR's recent Special Directions requiring indirect clearing PSPs to adopt Confirmation of Payee. Additional considerations on the application to indirect clearing PSPs are set out under our response to Q25.

<p><b>Inclusion of a Payment Initiation Service Provider (PISP) enabled payments.</b> We would be grateful for more details of proposed conditions for liability and apportionment.</p> <p>(1) The Electronic Money Regulations 2011, regulation 19  (2) The Payment Services Regulations 2017, regulation 22</p>	
<p><b>4</b> Do you have comments on our proposals:</p> <ul style="list-style-type: none"> <li>• that there should be a consumer caution exception to mandatory reimbursement</li> <li>• to use gross negligence<sup>1</sup> as the consumer caution exception</li> <li>• not to provide additional guidance on gross negligence?</li> </ul>	<p><b>CB response</b></p> <p>We strongly support a consumer caution as an exemption to the obligation, to ensure continued consumer responsibility. However, it is important for consumers, firms and FOS to have clear guidance on the nature of the caution provided and clear guidance on the consumer conduct factors to be considered in determining when consumer behaviour in relation to APP fraud has been negligent. We believe that it will be difficult to establish a gross negligence standard and therefore support the development of a contributory negligence assessment model to provide a clear and consistent assessment standard for consumers and the industry.</p>
<p><b>5</b> Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?</p>	<p><b>CB response</b></p> <p>We agree that vulnerable consumers should be compensated, even if their behaviour indicates an aspect of contributory negligence.</p>
<p><b>6</b> Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?</p>	<p><b>CB response</b></p> <p>We note the overlapping obligation of the Consumer Duty and believe that the reimbursement obligation should likewise follow the same FCA guidance on vulnerable consumers as set out under Finalised Guidance 21/1 and related information.</p>
<p><b>7</b> Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement</li> <li>• any ‘excess’ should be set at no more than £35</li> <li>• PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?</li> </ul>	<p><b>CB response</b></p> <p>We do not believe that the excess will deter spurious claims and that it would create an administrative burden to administer. Therefore, we do not believe that it is necessary. We believe that vulnerable consumers should be exempt from the excess charge and note that firms will have the discretion to waive the excess charge under other circumstances.</p>
<p><b>8</b> Do you have comments on our proposals that:</p>	<p><b>CB response</b></p>

<sup>1</sup> Gross negligence. PSR refers to FCA Guidance on the gross negligence standard for PSD2 unauthorised fraud claims “in line with the recitals to PSD2, we interpret ‘gross negligence to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness.” <sup>1</sup>(4.24) “...What qualifies as gross negligence will depend on the precise circumstances of each case.”

<ul style="list-style-type: none"> <li>• sending PSPs should be allowed to set a minimum claim threshold</li> <li>• any threshold should be set at no more than £100</li> <li>• PSPs should be able to exempt vulnerable consumers from any threshold they set?</li> </ul>	<p>We understand that the excess can act to filter purchase scams, if set at an appropriate level. Statistical analysis should be undertaken to identify purchase scam ranges and the minimum APP fraud claim level set with consideration of this data.</p> <p>Again, we believe that minimum claim thresholds should be the same for all PSPs, with firms having discretion to waive excess charges and minimum limits.</p>
<p>9 Do you have comments on our proposal not to have a maximum threshold?</p>	<p><b>CB response</b></p> <p>The Cost Benefit Analysis in Annex II does not discuss the impacts of an unfunded, uncapped liability scheme on the 1500 PSPs that are not CRM Code subscribers. The significant financial risk being introduced to this large population of PSPs is dismissed with the following unquantified statements:</p> <ul style="list-style-type: none"> <li>• <i>“For those PSPs that do not reimburse a material share of their customers’ APP scam losses at present (as the sending PSP in the transaction), these PSPs will become liable for <u>significant new costs</u>”;</i></li> <li>• <i>“PSPs on the receiving side of transactions now account for a negligible share of reimbursement (less than 5%), and so will face <u>substantially increased</u> reimbursement costs under our proposals”.</i></li> </ul> <p>We believe that this new financial risk will have serious commercial and competition consequences for the UK markets. Further cost benefit analysis is required to (1) estimate the implementation and ongoing operational costs, (2) estimate direct loss costs for non-CRM Code firms and (3) the ability of non-CRM Code firms to bear these costs and the related considerations of the impact of competition and innovation.</p>
<p>10 Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement</li> <li>• any time-limit should be set at no less than 13 months?</li> </ul>	<p><b>CB response</b></p> <p>We agree that sending PSPs should put a time limit on claims but that the limit should be the same for all firms, to allow PSP’s to more adequately plan future exposures (accruals).</p> <p>We believe that consumers are likely to become aware of APP fraud much sooner than unauthorised payment fraud. We do not believe that 13 months is necessary and recommend a shorter period of six months from the date of the relevant transfer.</p>
<p>11 Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• the sending PSP is responsible for reimbursing the consumer</li> <li>• reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?</li> </ul>	<p><b>CB response</b></p> <p>We believe that the sending PSP should have the reimbursement obligation to the consumer, due to its close relationship with the scam victim.</p> <p>We do not believe that 48 hours is an adequate time period for PSPs to verify the details of a claim, in particular because an authorised payment fraud is likely to require more time for investigation than for an unauthorised payment. Investigation for first party fraud is likely to take several weeks, given the need for customer questioning, and confirmation of external information, and intra-bank requests for information.</p> <p>Also, two weeks allows PSPs adequate time to manage financial resources and to prepare for unforeseen liquidity requirements which may be necessary for large claims. Therefore, we recommend adopting the CRM Code 15 day for unchallenged complaints/35 day for investigated complaints as the industry standard time period, subject to a requirement for firms to issue an acceptance notice within 48 hours.</p>

<p><b>12</b> What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?</p>	<p><b><u>CB response:</u></b>  The following factors should be considered as leading to a contributory negligence assessment:</p> <ul style="list-style-type: none"> <li>• material misstatements of fact or omission during customer due diligence, notice of APP scam, or an investigation;</li> <li>• making a payment to a fraudster after reporting losses to the same payee account or payee;</li> <li>• multiple unrelated loss claims with the relevant ASPSP or other PSPs.</li> </ul> <p>As stated in our response to Q11 we endorse the current CRM Code timeframe of up to 35 days for investigation, given the likely need to undertake third party information requests and other external dependencies.</p>
<p><b>13</b> Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?</p>	<p><b><u>CB response</u></b>  We support a starting position of a fixed 50:50 liability split, subject to clear allocation rules giving rights to raise other allocation claims.</p> <p>We also endorse the industry proposal that the PSR, FCA or other body should have the right to increase the liability percentage to 60% to incentivise a poorly performing PSP to improve its performance.</p>
<p><b>14</b> Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?</p>	<p><b><u>CB response</u></b>  There is a concern that a negotiable approach will result in a substantial number of PSP-to-PSP disputes and as such we endorse that there should be a fixed allocation. However, firms should be able to bring a claim against another PSP if under an industry allocation criteria, the other firm materially failed to meet industry standards or was otherwise materially at fault in relation to an APP Scams claim.</p>
<p><b>15</b> Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?</p>	<p><b><u>CB response</u></b>  We recommend that the last PSP in a chain takes the 50% liability as the receiving PSP, but recognise the difficulty in tracing where multiple transfers are involved.</p>
<p><b>16</b> Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?</p>	<p><b><u>CB response</u></b>  We agree.</p>
<p><b>17</b> Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?</p>	<p><b><u>CB response</u></b>  Sharing costs seems a fair and sensible suggestion, but may be difficult to accrue and collect in a timely fashion. It would be helpful for guidance on which types of costs can be included and maximum timeframes for chargebacks. As with the allocation of reimbursement, this would support smaller firms which do not have the resources of the large incumbents and would help prevent these firms potentially being pushed into taking more liability.</p>
<p><b>18</b> Do you have views on our long-term vision, and our rationale for the Payment</p>	<p><b><u>CB response</u></b>  Pay.UK's purpose is to be the operator of payment systems. We do not believe that it is helpful or appropriate for Pay.UK as a market infrastructure operator to set financial crime or conduct obligations for PSPs. PSP obligations related to fraud should be set in law and directly applicable to all payment service providers that are ASPSPs, with Pay.UK</p>

Systems Operator (PSO) being the rule-setter responsible for mitigating fraud?	<p>providing a monitoring or oversight function and coordinating with the FCA as the body responsible for regulating PSPs. By analogy, market abuse rules are set in legislation, apply to all financial market participants, and the role of exchanges and other forms of market infrastructure is to monitor while the FCA is primarily responsible for supervision and enforcement over investment firms.</p> <p>Pay.UK has no skill or expertise in developing conduct, supervision and enforcement rules relating to regulated firms, and no legal basis of authority to do so. The FCA has the expertise and facilities already available, such as supervision, enforcement, regulatory reporting (REP 17 financial crime reporting), and FOS alternative dispute resolution mechanisms which could be developed rather than the cost and effort of creating new mechanisms at Pay.UK.</p> <p>Further, creating a new regulatory role for Pay.UK will further fragment an already complicated regulatory environment for payment firms. Neither the HMT consultations on the Future Regulatory Framework and the Payments Landscape Review sought to identify ways to make the payments regulatory environment easier for PSPs to navigate, with the focus on improving consumer protection outcomes. We accept this is a critical goal, however only the Kalifa Review of UK FinTech discusses the existing complexity of UK payments regulation:</p> <p style="text-align: center;"><i>“At present, numerous stakeholders have responsibility for policy and regulation that impacts the fintech sector, including Government departments (such as HM Treasury, DIT, DCMS, DWP, Cabinet Office and BEIS), the financial regulators (the Bank of England, PRA and FCA) and other regulators such as the ICO and CMA. Some of these – including HM Treasury, DIT, the Bank of the England and FCA – have dedicated fintech teams.”</i></p> <p>As such, creating a new quasi-supervisory relationship for firms is unwelcome. We instead recommend that the PSR considers how the FCA can extend its existing scope of duties and facilities to provide rule making, supervision and enforcement of APP fraud.</p>
<p>19 Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?</p>	<p><b>CB response</b></p> <p>In our view locating the APP fraud reimbursement obligation in the scheme rules is not coherent with existing statutory liability obligations on PSPs under the PSRs 2017 or likely to result in an efficient and successful implementation of the APP scams reimbursement obligation. Rather, implementation through the scheme rules is likely to have the unintended consequence of reducing access to clearing for FPS indirect clearing market participants, loss of payment services for many consumers and a reduction of the indirect clearing market for FPS direct member firms.</p> <p>We believe that the APP fraud mandatory reimbursement obligation should be located in the PSRs 2017, under the rules which require PSPs to provide reimbursement for unauthorised payment fraud, which is the corollary to authorised push payment fraud. The PSRs 2017 in regulations 90-96 also set out other liabilities for PSPs relating to customer payments. Locating APP fraud reimbursement liability on the PSRs 2017 would then sit alongside the other liabilities applicable to PSPs for customer payments, creating a clear and consistent set of statutory reimbursement obligations.</p> <p>If this approach is not possible, we recommend that the obligation is created in a Special Direction which applies to all ASPSP regardless of their direct or indirect status. We note that imposition of the liability via a Special Direction is consistent with the PSR’s use of Special Directions for other PSP obligations – the extension of CoP to 400+ PSPs (1) and the upcoming Special Direction for APP Scams reporting obligations.</p> <p>(1) Extending Confirmation of Payee Coverage PS 22/3, PSR</p>
<p>20 Do you have views on how we should exercise our powers under Financial Services (Banking Reform) Act 2013 (FSBRA) to implement our requirements?</p>	<p><b>CB response</b></p> <p>Section 54 of FSBRA authorises the PSR to give written directions to participants in regulated payment systems, either requiring or prohibiting the taking of specified action in relation to the system or setting standards to be met in relation to the system. As stated in our response to Q19, we believe that mandatory reimbursement should either be a statutory obligation, consistent with other PSP payment liabilities under the PSRs 2017, or should be imposed on all ASPSPs via a Special Direction.</p>
<p>21 Do you have views on how we propose that allocation criteria and dispute resolution</p>	<p><b>CB response</b></p> <p>We recommend that UK Finance is tasked with developing an industry allocation criteria. This role would draw on UK Finance’s roles in managing the Best Practice Standards reporting platform for the CRM Code and its financial crime workstream expertise. We do not believe that private ADR facilities should be engaged to settle disputes that cannot</p>



arrangements are developed and implemented?	be determined by the allocation criteria, as this will lead to inconsistent outcomes. Rather a specialist ADR arbitrator should be either appointed by the PSR or by UK Finance industry led allocation working group to adjudicate APP scam disputes with between PSPs. This would ensure a consistent outcome for disputes which would then inform updates to the allocation criteria.
22 Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?	<p><b>CB response</b></p> <p>We understand that UK Finance operates the BPS (Best Practice Standards) system as the reporting mechanism for CRM Code subscribers and that this currently provides real time availability of compliance management information, accountancy functions for submission of funds and liability calculations per claim. We support UK Finance's recommendation to utilise this as the APP scams reporting system, which would provide Pay.UK, the PSR and FCA real-time monitoring capabilities to oversee compliance from allocation of funds to collections between firms.</p>
23 Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?	<p><b>CB response</b></p> <p>See our response to Q22.</p>
24 Do you have views on the best option for short-term enforcement arrangements?	<p><b>CB response</b></p> <p>As a regulated firm, we believe that our performance in managing APP fraud should be a supervisory and enforcement matter for the FCA. FCA regulatory supervisors are best suited to assess a PSP's performance against the FCA regulatory authorisation requirements and related rules (e.g. the Systems and Controls Sourcebook, the Banking Conduct of Business Sourcebook, the PSRs 2017 or FCA Principles for Business). We do not believe that Pay.UK as a market infrastructure operator should be tasked with enforcement over authorised firms for conduct or governance issues. This will be costly and require significant time for Pay.UK to hire and train staff and undertaking this work would duplicate the supervision and enforcement structures that already exist.</p>
25 Do you have views on the best way to apply the rules on reimbursement to indirect participants?	<p><b>CB response</b></p> <p>As stated in other answers, we believe that the obligation should apply to all PSPs by extending the obligations under the unauthorised fraud reimbursement provisions of the PSRs 2017. A foundation in the PSRs 2017 is also consistent with other forms of liability in the PSRs 2017 (regulations 90-96) that apply to all PSPs. If this approach is not available, we believe that the PSR should, consistent with its direct instruction to PSPs for Confirmation of Payee, direct all FPS direct and indirect participants under a Special Direction.</p> <p>Imposing obligations on FPS directly raises significant implications for ClearBank and firms that are FPS clearing firms. ClearBank's core business is the provision of indirect clearing services to PSPs. As stated in the PSR's Access and Governance report, ClearBank is one of around forty FPS direct participants, and one of around ten FPS direct participants that provides indirect clearing services to approximately 1500 PSPs. Four of the FPS clearing providers are incumbent, large financial institutions. ClearBank and the other five clearing providers are Challenger Banks or FinTechs that have a growing market share of the indirect clearing market.</p> <p>Requiring FPS direct participants to be liable for APP fraud reimbursement of indirect participants would introduce an unfunded and uncapped liability on each FPS clearing provider in relation to each indirect clearing customer. Contractual reimbursement obligations are not a guarantee of repayment, and the direct provider would have the risk that some indirect PSP customers would refuse to pay or may simply declare insolvency. To protect against this credit risk, the direct participant clearing firms will need to significantly increase their credit risk criteria for each of the 1500 indirect clearing PSPs. Many indirect PSPs would not be able to meet the credit criteria or related obligations, such as holding additional reserve or collateral requirements with the clearing firm. These PSPs would lose access to clearing, reducing competition in UK markets.</p> <p>This obligation would disproportionately affect Challenger Banks and FinTech clearing firms that have entered the payments clearing market since 2017. New clearing firms have a high concentration of customers that are electronic money and payment institutions, many of which are new and innovative businesses which have powered innovation in UK payments markets or firms that struggle to have access to clearing from more established clearing businesses. The PSR cites this in the Access and Governance (2022) report:</p>

*“The new-entrant IAPs continued to take on many customers, including smaller PSPs and small money remitters, which historically had the most difficulty gaining access.” (4.12)*

The impact of imposing the obligation would therefore have a disproportionate negative impact on Challenger Banks and FinTech clearing providers relative to incumbent clearing providers.

A further burden that liability would place on clearing firms that are Challenger Banks relates to enhanced capital requirements. If a clearing bank is directly liable for the reimbursement of its clearing customers, the bank may be required to hold additional Pillar 2 capital requirements against potential indirect customer losses, as well as additional Pillar 2 capital against our own APP fraud consumer customer losses. A Pillar 2 capital requirement applies to all PRA-regulated banks, building societies, designated investment firms and all PRA approved or designated holding companies. This is a firm-specific capital requirement calculated upon the firm’s individual risks, including credit, market, operational and counterparty risk. APP scam uncapped losses are likely to require additional capital set aside as either additional credit or operational risks. Each FPS clearing bank would also need to have substantial liquidity facilities available.

In short, we believe that the operational oversight, risk and credit requirements would fundamentally change the nature of indirect clearing services.

Finally, we note that there are no operational barriers to indirect PSPs being directly responsible for reimbursement. Indirect clearing PSPs are easily identified under their Bank and Sort Codes in all FPS payment messages. By imposing FPS direct participants as intermediaries in reimbursement, all clearing firms would need to build operational systems to monitor APP fraud claims, pay-outs and repatriation of funds for each indirect clearing customer. In addition to the unnecessary cost and complexity that this would create, imposing clearing firms in APP fraud claims related to the business of indirect clearing firms is likely to lead to a substantial rise in disputes between direct and indirect clearing firms. This can all be avoided if the indirect clearing firm is directly responsible for reimbursement.

**26** If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?

**CB response**

See our response to Q25.

**27** Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?

**CB response**

The cost benefit analysis (CBA) does not provide any detail as to average APP scam losses, address implementation or ongoing operational costs, impacts on competition in the PSP industry or UK international competitiveness. We believe that more statistical analysis is required.

**APP loss statistics.** Reimbursement proposals should be based on APP fraud statistical data, such as average claim sizes. The PSR should make available much more granular data, including average loss sizes, by type of APP scam. This data is critical in developing fair and proportionate reimbursement regime. An unfunded, uncapped liability regime is imposing an insurer of last resort obligation, which is uncommercial for any industry. We refer to the UK Finance Annual Fraud Report 2022, published in July of this year. This sets out total reported figures for the eight types of APP Fraud recognised under the CRM Code.

**Implementation and ongoing operational costs.** The cost of implementation will be significant for around 1500 PSPs, requiring sophisticated new data systems, staff and operational arrangements as well as development for coordinating with new industry APP scams reporting, risk sharing and collections facilities. The scale of this project will be similar to operational systems and processes in place today for money laundering and sanctions, or potentially even larger systems and processes required given the interaction between PSPs. An average implementation and ongoing costs for PSPs of various PSP businesses should be estimated to include costs relating to relevant industry systems that are developed.

**Impact of obligation on competition.** In imposing a significant new risk and costs on the industry, the PSR must estimate the potential impact on competition. The competition impacts will be experienced in the PSP market, but also in the UK clearing market. The majority of PSP firms connect to FPS system via clearing arrangements, and therefore a reduction in the total PSP market will affect not just a reduction in competition for payment end users but also in the UK payments clearing market. The CBA should also include an assessment of the impact on international competitiveness.

**28** Do you have any other comments on the proposals in this consultation?

**CB response**

**Need for APP fraud industry standards**

The regulatory focus should be on enhancing preventative measures by introducing a common standard of customer fraud due diligence and active management. Without clear leadership from the regulator, such standards will end up being developed by the industry via the allocation criteria. It seems more straightforward for the PSR or FCA to lead on developing clear standards against which the FCA can undertake PSP specific supervision and enforcement to take action, rather than allowing poorly performing firms to be indirectly controlled via financial incentives.

**Necessity of the Online Safety Bill.** We are concerned that implementing without caps and before significant preventative measures are in place will simply incentivise first party fraudsters to focus more scams on online payments. To reduce the impact on PSPs and introduce much needed shared responsibility, we advocate for mandatory reimbursement to come into effect concurrent to the fraud provisions measures under the Online Safety Bill. We believe that the Online Safety Bill measures will have an even more meaningful impact in combatting APP fraud than reimbursement, and without the same risk of PSPs and consumers losing access to payment services.

**Implementation timing.** As noted in our response to Q2, for our firm as a non-CRM adherent the implementation will require a substantial investment and much of the systems and staffing requirements will be determined by scope rules and industry processes not yet determined. We therefore request that PSPs are given a reasonable time to implement. We recommend an implementation period of at least twelve months post completion of the final rules.

Thank you for your consideration of our response. We would be grateful to discuss with you in a bilateral meeting our responses to Questions regarding indirect clearing arrangements.

# Consumer Council

# **The Authorised push payments (APP) scams: Requiring reimbursement Consultation**

THE CONSUMER COUNCIL RESPONSE

November 2022

# CONTENTS

<b>1. EXECUTIVE SUMMARY</b> .....	3
<b>2. ABOUT US</b> .....	4
<b>3. RESPONSE TO CONSULTATION QUESTIONS</b> .....	6
<b>4. CONCLUSION</b> .....	12
<b>5. CONTACT INFORMATION</b> .....	13

## 1. EXECUTIVE SUMMARY

The Consumer Council welcomes the opportunity to respond to this consultation.

In our response to the Payment Systems Regulator's (PSR) previous consultation on Authorised Push Payment Scams<sup>1</sup> the Consumer Council noted that the current regulatory regime is not working, and reimbursement should be made mandatory. Therefore, we welcome this consultation that outlines measures requiring mandatory reimbursement of consumers who are the victims of fraudulent activity.

The Consumer Council believes that consumers should not be penalised for being scammed regardless of the amount. Therefore, we have concerns about the PRS's proposals to allow payment system providers (PSPs) to set a fixed 'excess' of £35 and a minimum threshold claim of up to £100.

In suspected cases of gross-negligence and first-hand fraud the balance of the evidence needed to investigate must be defined and a clear set of rules applied to PSPs to ensure cases are dealt with fairly and within a reasonable timeframe. The burden of proof must lie with the PSPs to establish gross negligence or fraud, it must not be the consumers responsibility to prove they have done nothing wrong given they are the victim of the fraud.

Northern Ireland is a unique market within the UK when it comes to banking. Therefore, the PSR must ensure that Northern Ireland consumers are equally protected by the introduction of these measures as consumers throughout the UK.

---

<sup>1</sup> <https://www.psr.org.uk/media/kg0bx5v3/psr-cp21-10-app-scams-consultation-paper-nov-2021.pdf>

## 2. ABOUT US

The Consumer Council is a non-departmental public body (NDPB) established through the General Consumer Council (Northern Ireland) Order (The Order) 1984. Our principal statutory duty is to promote and safeguard the interests of consumers in Northern Ireland.

We are an insight-led, evidence-based organisation:

- Providing consumers with expert advice and confidential guidance.
- Engaging with government, regulators, and consumer bodies to influence public policy.
- Empowering consumers with the information and tools to build confidence and knowledge.
- Investigating and resolving consumer complaints under statutory and non-statutory functions.
- Undertaking best practice research to identify and quantify emerging risks to consumers.
- Campaigning for market reform as an advocate for consumer choice and protection.
- We have specific statutory duties in relation to energy, postal services, transport, water and sewerage, and food affordability and accessibility. These include considering consumer complaints and enquiries, carrying out research, and educating and informing consumers.

Our non-statutory functions educate and empower consumers against unfair or discriminatory practices in any market from financial services to private parking charge notices. Across all our areas of work, we pay regard to consumers:

- who are disabled or chronically sick;
- who are of pensionable age;
- who are on low incomes; and
- who live in rural areas.

The Consumer Council uses a set of eight core principles that are commonly used by consumer organisations for working out how particular issues or policies are likely to affect consumers. These are:





The principles ensure we apply a consistent approach across our statutory and non-statutory functions, and in all our engagement with consumers and stakeholders.

They serve to protect consumers, setting out the minimum standards expected from markets when delivering products or services in Northern Ireland. They also frame our policy position and approach to resolving consumer disputes with industry, offering a straightforward checklist to analyse and validate outcomes, in particular amongst vulnerable groups.

### 3. RESPONSE TO CONSULTATION

The Consumer Council will respond only to those questions where we feel we have the evidence or expertise to do so.

#### Questions for answer:

- Q1. Do you have views on the impact of our proposals on consumers?**
- Q2. Do you have views on the impact of our proposals on PSP's?**
- Q3. Do you have views on the scope we propose for our requirements on reimbursement?**

The Consumer Council welcomes action taken to provide high levels of protection for consumers in relation to fraud and scams. However, when considering the proposals, it is important to ensure that the process is easily accessible to all consumers and developed in a format that everyone can easily understand.

The Consumer Council understands that one of the PSR's focuses is to 'identify and address fraud in the Faster Payments system' and that 'Faster Payments was used for 97% of scams.' Historically, decisions to implement policies that seek to protect consumers on a UK wide basis can result in less protection in Northern Ireland due to the differences in the banking market. In introducing these new measures, the PSR must ensure that Northern Ireland consumers receive the same level and cover of protection as consumers throughout the UK.

In principle, the Consumer Council welcomes the PSR's proposal to introduce mandatory reimbursement of consumers for all types of APP scams. However, we have concerns about the PSR's proposals to allow PSPs to set a fixed 'excess' of £35 and a minimum threshold claim of up to £100 and the impact that this will have on consumers, particularly those in vulnerable circumstances.

The Consumer Council believes that consumers should not be penalised for being scammed regardless of the amount. Whilst statistics suggest <sup>2</sup> that only 8% of APP scams are under £1,000 (Pg 19, 3.10), this 8% could represent some of the most vulnerable consumers who may not be in a position to accept this loss. The Consumer Council strongly suggests that PSR revisit this exclusion to protect the consumers and prevent any detriment to those most in need of protection. This minimum threshold of £100 may also deter PSP's from carrying out work to reduce these low-level scams as there is no obligation to reimburse consumers. In return scammers may see this as an opportunity to increase low-level scams as they are less likely to be caught.

---

<sup>2</sup> UK Finance, annual fraud report (August 2022)

We welcome the proposal for the mandate given to Pay.UK (Pg 18, 3.8) however, it would be important that the refining, monitoring, and enforcing compliance components are enabled in such a way that they can react to the fast pace and ever-changing payment systems.

The Consumer Council greatly appreciates the inclusion of the specific requirement not to exclude particular categories of customers based on risk (Pg 20, 3.3), referring specifically to their obligation under the Equality Act 2010, however this legislation is not applicable in Northern Ireland and the Consumer Council would suggest for clarity that PSR explore the devolved legislature to ensure compliance for all UK consumers.

The Consumer Council welcomes the acknowledgement that the cost of any scheme should be carried by the PSP's. To maintain the level of incentivisation, it may be prudent to explore this in more detail to ensure that the PSP's do not pass these costs on to the consumer.

Any protection for consumers is a welcome addition, and we agree that all consumers who fall victim to APP scams should be protected as your aims state (Pg 24, 4.5) however, this would appear to contradict the introduction of the minimum threshold of £100.

We also welcome the inclusion of the PRS's expectation to include on-us payments in the right to reimbursement and agree that a victim should not have less right to reimbursement if the fraudster uses an account provided by the victim's own PSP.

The Consumer Council understands that the PSR does not have the powers to regulate 'on-us' payment and the consultation states that 'if necessary, the PSR and FCA may consider what further complementary guidance or rules may be required'. The Consumer Council seeks clarification on how the PSR will monitor reimbursement of consumers affected by these types of payments to ensure that consumers affected do not face detriment in this area. Swift action must be taken by the PSR and FCA to protect consumers if it is identified that PSPs are not reimbursing impacted consumers.

**Q4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

**Q5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

**Q6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

We agree that there should be a consumer caution exception, however any exception must be fair to all parties. There must be a threshold set to protect consumers and not provide a get-out clause for PSP's.

The Consumer Council understands the reasons for not wanting to provide additional guidance on gross negligence and the reasoning that providing such guidance may allow the PSPs to manipulate or dilute the high bar, thus weakening the protection afforded to consumers and not acting within the ethos of this action.

We welcome the proposal to require PSPs to reimburse vulnerable customers even if found that they acted with gross negligence. This proposal will protect those consumers who need the most protection.

The Consumer Council understands the proposal put forward to use the FCA's definition of vulnerable customer. By doing so it will provide clarity to everyone and there can be no misinterpretation of the term.

**Q7. Do you have comments on the proposal that:**

- **Sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **Any 'excess' should be set at no more than £35**
- **PSP's should be able to exempt vulnerable consumers from any 'excess' they apply?**

As stated above The Consumer Council has concerns about the proposal allowing PSPs to set a modest fixed 'excess' to reimbursement. We recognise that consumers must exercise a level of care and attention when making transactions. However, scams have become more sophisticated in their nature making it more difficult for consumers to recognise.

We question the reasoning put forward in the consultation document that a fixed excess ‘could help provide incentives to consumers to take care when making smaller payments...’ If a consumer has acted in good faith and taken all reasonable steps to protect themselves full reimbursement should be due without being penalised by an ‘excess’ amount.

Increased consumer awareness through better education should be one of the main drivers to help prevent consumers becoming a victim of an APP scam and this requires coordinated stakeholder action. Equally, payment systems must be safe to use and consumers need to be confident in the safety and security of these systems, and the underpinning regulatory regime.

If the PSR implements its proposal to allow PSPs to apply an excess the Consumer Council believes vulnerable consumers should be exempt from any ‘excess’.

**Q8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

**Q9. Do you have any comments on our proposal not to have a maximum threshold?**

The Consumer Council believes any decision on this should have consumer interests at the forefront and tangible efforts must be made to ensure the best consumer protection. Therefore, we strongly suggest that the PSR revisits the proposal to allow PSPs to set a minimum claim threshold with the view of removing it. We believe that consumers should be entitled to full reimbursement regardless of the amount.

The consultation highlights, ‘the lowest scam value scam payments are typically the hardest for PSPs to detect and prevent, so PSPs have the least scope to mitigate the costs of mandatory reimbursement.’ Similarly, scams of this nature may also be difficult for consumers to detect and by introducing a minimum threshold it would place the risk on to consumers.

As stated earlier in our response, a minimum threshold of £100 may also deter PSP’s from carrying out work to reduce these low-level scams as there is no obligation to reimburse consumers. In return scammers may see this as an opportunity to increase low-level scams as they are less likely to be caught.

If the PSR does introduce this proposal The Consumer Council agrees that there should be an exemption clause for vulnerable consumers, meaning those most at risk should hopefully be protected.

The Consumer Council does not see any need for a maximum threshold to be set.

**Q10. Do you have any comments on our proposals that:**

- **sending PSPs should be allowed a set time-limit for claims of mandatory reimbursement**
- **Any time-limit should be set at no less than 13 months?**

The Consumer Council feels that having a set time-limit for mandatory reimbursement is acceptable, but it is important that any time-limit set should be reasonable and fair to consumers.

A minimum time-limit of 13 months may require some reconsideration particularly given it is our understanding that the 13-month time period begins from the final payment involved in the scam. The Consumer Council would ask whether a more appropriate proposal would be to set a time limit to start from the time at which the victim of the scam became aware or indeed was made aware of the fraudulent activity.

**Q11. Do you have comments on our proposals that:**

- **The sending PSP is responsible for reimbursing the consumer**
- **Reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

**Q12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The Consumer Council does not have a view on whether it is the sending or receiving PSP should be responsible for reimbursing the consumer. However, we do agree that having a single point of contact responsible for reimbursement and simplifying the process would be the right approach for consumers.

We are also in agreement that the reimbursement is as soon as possible and no later than 48 hours in the majority of claims. It is important that the consumer suffers as little detriment as possible.

The Consumer Council believes that a high threshold must be put in place for gross-negligence and first party fraud, and that the system must be robust enough to protect consumers and to provide an opportunity for the PSPs to identify and deal with disingenuous claims. The burden of proof must lie with the PSPs to establish gross negligence or fraud, it must not be the consumers responsibility to prove they have done nothing wrong given they are the victim of the fraud.

**Q18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

The Consumer Council believes that the consumer interest must be central to any reimbursement regime. In implementing these measures the PSR must ensure that any consumer protections are not diluted to ensure victims have access to swift reimbursement.

**Q22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

**Question 24: Do you have view on the best option for short-term enforcement arrangements?**

The Consumer Council believes that an effective system to monitor compliance must be in place from the outset of the introduction of mandatory reimbursement to allow swift action to be taken where non-compliance is identified. Data relating to compliance should be made publicly available to ensure openness and transparency in order to build consumer trust and confidence in the implementation of these new measures.

This goes hand in hand with a robust enforcement regime where non-compliance is fully investigated with appropriate actions being taken where non-compliance is identified. The PSR, as the regulator, should have a role within this regime.

**Q28. Do you have any other comments on the proposals in this consultation?**

The Consumer Council recognises and appreciates the importance of protecting all consumers from APP scams and in particular those consumers who are most vulnerable. Again, consumers must be at the forefront when decision-making to ensure all consumers are afforded an acceptable level of protection.

#### 4. CONCLUSION

The Consumer Council is supportive of the introduction of mandatory reimbursement for consumers who have been victim of an APP scam. However, we are concerned about the PSR's proposals around allowing a PSP to set a 'modest fixed excess' and 'minimum threshold amount'.

In considering our response it is important to understand the Northern Ireland context. Detriment and harm will have a more pronounced impact on consumers here, who are more dependent on digital markets for consumer goods and services because of a reduced 'bricks and mortar' retail presence, compared to other UK regions.

Northern Ireland, which makes up just 3% of the UK population, has consistently displayed higher levels of consumer vulnerability:

- Over a third of the population live in rural areas, which is twice the UK average, but this consumer group is impacted by the challenges of accessing reliable broadband.
- Northern Ireland consumers have higher levels of average debt, there are more people with low financial capability and more people with no cash savings. According to the Financial Lives Survey 2020, in Northern Ireland:
  - 16% of adults have no cash savings.
  - 24% of adults have low financial capability compared to 17% in the UK.
  - 26% of adults are highly confident in managing money compared to 37% in the UK.
  - The average amount of debt is £10,730 compared to £9,570 in the UK.
- Northern Ireland's lowest-earning households have seen their discretionary income decrease by 46.1% compared to last year (from £45.32 to £24.41), meaning they have less than £25 per week to spend after bills and living expenses.
- Consumer Council research into low income households found for the lowest income quartiles, 61% of UK household income is derived from social securities compared to 73% of household income in Northern Ireland.

The proposals made in the consultation are positive but substantial consideration must be given to the amount of time needed to implement these new rules and ease of the PSO in the operational requirements. Above all, the consumer must always remain at the forefront and must not suffer substantial detriment.



## 5. CONTACT INFORMATION

To discuss our response in more detail, please contact:

[REDACTED]

Senior Policy Officer – Financial Services

[REDACTED]

[REDACTED]

# Counting Up

## APP Scams

### Payment Service Regulator

12 Endeavour Square

London E20 1JN

Email: [appscam@psr.org.uk](mailto:appscam@psr.org.uk)

## To whom it may concern,

# PSR Consultation Paper CP22/4 - Counting Ltd Response

Counting Ltd ('Countingup') welcomes the opportunity to respond to the Payment Systems Regulator's ("PSR") Consultation Paper ("CP22/4") regarding Authorised Push Payment ("APP") scams: Requiring reimbursement.

Our strongest recommendation in general is to ask PSR to act in concert with other financial services regulators, government, law enforcement and industry to develop a strategic, concerted, approach to APP scam prevention. It is our position that the approach should focus on the root causes of the APP scams to drive prevention. Any changes will have impacts and ramifications not only across the Fintech ecosystem but also throughout the UK market and such consequences need to be assessed by all the key players involved.

### 1. Do you have views on the impact of our proposals on consumers?

In our opinion, mandatory reimbursement does not represent a solution but a temporary remedy for consumers that would be detrimental to PSPs and their customers (the consumers) in the medium to long term. The aim is to prevent APP fraud via scams. These scams occur between the consumer and the fraudster and often involve the gaining of trust, followed by rapid payment. The proposals do not address the issue where it is realised. Placing the burden of risk at arms-length from where the risk is realised (between the consumer and fraudster) creates an arms-length inability to prevent the scam from occurring in the first place. In the longer term this is likely to lead to:

- **Increased cost** - PSPs will bear a considerable cost in compulsory reimbursement. Not just from the reimbursements themselves but also in administering the requests, analysing and authenticating the validity of claims, gathering information

---

and data on the circumstances, etc. These costs will by necessity eventually be passed onto all consumers through increased fees. This would be in addition to (and distract from) the valuable development of stronger anti-fraud measures, better compliance and sophisticated transaction monitoring systems. For small Financial technology businesses and small PSPs it would be very difficult to manage these costs small PSPs would thus become un-competitive;

- **greater transaction monitoring would be required, this would increase red flags and block a larger number of transactions** in the attempt to prevent the risk of APP scams. This will add friction to the UK's financial network, worsening the service for the vast majority of legitimate transactions and consumers. This would naturally de-motivate customers from using the services offered by PSPs;
- **the prevention of payments** - far broader risk measures would be required in PSPs effectively tightening the risk appetite. Legitimate payments will start to look suspicious so blocking payments will become a over-used solution which would significantly impact the majority of legitimate customers;
- **cash payments would become more prevalent** (as even legitimate users will likely find these are subject to less scrutiny than faster payments would be) and offer less ability to assess source of funds to prevent Money Laundering activity, especially that of organised criminal groups;

Mandatory reimbursement is not the solution which protects customers from APP scams because - as in fact even the Consultation Paper suggests - criminals are getting more creative and sophisticated each day.

The potential impact of all the above consequences is underplayed by the Consultation, which seems to acknowledge certain "additional friction for a small proportion of payments", but this doesn't suggest that an analysis on real data/numbers has been carried out considering how many transactions might be affected, (quoting the Consultation Paper "we have not been able to quantify the likely costs of any delayed or declined payments").

The mandatory reimbursement would not stop systematic abuse from Organised Crime Groups (OCGs), PSPs would consequently be passing along the costs of compulsory reimbursement to all customers. Our customer demographic is small businesses (both sole trader and limited companies), usually newly established. These new businesses look to our services for a variety of reasons, in comparison to major banks; not least competitive fees and innovative technology.

The proposals, if implemented, would not support competition and innovation in the industry. On one hand PSPs would have to become more selective during customer onboarding and would consider many businesses as unattractive, on the other the proposals would incentivise customers to avoid PSPs which had to increase their prices because of the costs they faced to comply with the PSR's implemented measures.

This would, in turn, impact the economic landscape; stifling the innovation and entrepreneurship that fosters a fair and effective market for the wider general public. The proposals would encourage rather than discourage fraud - entirely divorcing the cost of fraud from the victim would lead customers to take a relaxed stance toward scams.

---

Without concern for the transaction consumers would be less risk-averse, more likely to succumb to financial scams and less likely to engage in preventative activity.

## **2. Do you have views on the impact of our proposals on PSPs?**

In recent years the UK has seen an increase of new PSPs entering the market. They are building their businesses on increasingly specific offerings which benefit subsets of consumers in previously underserved areas. They often have relatively high volumes of small transactions.

The PSR proposals as they stand would impose:

- high costs on PSPs to set transaction monitoring processes, to be able to prevent (only to a certain degree - though) the ever changing APP scams framework,
- compulsory reimbursements for a large number of small transactions with the result that the impact on businesses would be much larger and detrimental than the impact on a single Customer victim of an APP scam
- an overly burdensome risk, challenge and cost on these new PSPs which no longer be able to survive

This would clearly be to the detriment of the PSPs and to the consumers they are aiming to serve.

Improving transaction monitoring and preventive measures would not reduce the APP scams problem under this proposal. The compulsory reimbursement of a large number of micro transactions would impact on the growth of the UK Fintech industry, (where one APP scam of the value of £100 may not be perceived as severe for a single customer).

Transaction between newer PSPs/Fintechs (or non-traditional banks) and traditional financial institutions would result in the increase in processing times to/from these institutions driving the market towards traditional banks (blocker for some newer legitimate businesses). Mandatory reimbursement costs are estimated to represent at least a tenth of PSPs' revenue, according to the wider FinTech industry.

## **3. Do you have views on the scope we propose for our requirements on Reimbursement?**

The scope is too broad. The Consultation does not engage with each and every APP scam and how they are perpetrated. The mandatory reimbursement is a rather flat (one size fits all) solution very similar to unauthorised payments refund scheme, but these two types of fraud and how they unfold differ greatly (for example, unauthorised payments typically take place without the consumer's knowledge). This means that the existing refund regime for unauthorised payments does not necessarily provide an appropriate framework for more nuanced APP fraud refunds.

## **4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**

Consumer caution could be an appropriate exception to mandatory reimbursement, however, not as currently proposed (only in the case of gross negligence), per below.

---

- **to use gross negligence as the consumer caution exception**

The very limited scope for exclusions to mandatory reimbursement, would cause increased costs and uncertainties.

PSPs would have to have robust protocols in place to detect and prevent APP Fraud, and may also need to invest in effective investigation tools to streamline the volume of claims and to consider on a case by case what gross negligence (not clearly defined in English civil law) may be.

- **not to provide additional guidance on gross negligence?**

As already pointed out, 'gross negligence' doesn't exist in Civil Law.

In fact, if we take the Contingent Reimbursement Model Code as an example, the idea there was to reimburse customers who are not to blame for the success of the scam. The Code works on the positive assumption (of diligent behaviour) that consumers act on effective warnings provided by the PSP and have a reasonable basis for believing the transaction to be genuine if they are to be fully refunded. Under the PSR proposal, very little is expected of consumers. This appears to overlook the vital role consumers - who interact directly with the scammer - can play in preventing APP frauds.

With this in mind, exceptions to mandatory requirements need to be in place as consumer behaviour needs to be analysed more carefully, on a case by case and based on a concept (gross negligence) that is unknown in our law.

The lack of guidance on gross negligence means that the proposal would effectively require reimbursement for most domestic APP scam payments made by Faster Payment. This contradicts the approach previously taken by the CRM Code and the traditional mechanism of 'caveat emptor' or 'let the buyer beware'.

Excluding the mandatory reimbursement only in the case of gross negligence would definitely lower the level of consciousness and awareness used by consumers as they could be confident that reimbursement would be available for them. This would encourage a relaxed attitude towards payments and payment services. This reveals a lack of focus on ongoing consumer education for APP fraud which should be also an essential part of the proposals and should continue to be an important part of seeking to reduce this crime and the costs to PSPs.

Furthermore the Consultation Paper seems to only take account of complex and sophisticated APP scams. However, often a fair proportion of the scams that we see are not particularly elaborate. Lots are related to the purchase of goods online with very little due diligence being conducted, or the consumer conducting more in-depth checks after the fact once the payment has already been made.

PSPs might therefore be inclined to refuse any atypical payment instructions until they can be close to certain that an arrangement is genuine, with warnings aiming at demonstrating gross negligence on the consumers' part if they proceed notwithstanding a clear warning of a potential scam.

## **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

If the Consumer Caution Exception would be triggered by ordinary negligence, then maybe it would be reasonable to exclude the Exception in case of Vulnerable Customers. However

---

gross negligence is when for example customers **deliberately** fail to use a payment instrument in accordance with the terms and conditions governing its use. FCA defines gross negligence as “a very significant degree of carelessness”.

There is no evidence that Vulnerable Customers lack care or intention to act in compliance with the law, and to identify and assess a customer as a vulnerable person a PSP would need time and resources to (properly) investigate.

#### **6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

We agree on the definition that ‘a vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care’, but that does not exclude that a vulnerable person can act deliberately with fraudulent intentions.

#### **7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement**

We suggest that an excess would be required in order to minimise the risk of consumers disregarding their crucial role in scam avoidance. The excess would therefore support the aim of scam prevention by placing some of the cost where the crime occurs. However, this would only reduce the cost to the PSP and place a small pressure on the consumer. This would not be likely to reduce the overall level of fraud, nor the overall cost to consumers and PSPs.

- **any ‘excess’ should be set at no more than £35**

It is highly questionable whether such amounts are significant enough to encourage consumers to take the required level of care and to thoroughly question whether there is a risk that their APP is subject to fraud. This is another example of lack of emphasis in the PSR’s proposals about financial education for customers. We suggest that the excess fee should be proportional to the payment amount - a percentage rather than a nominal fee. This would encourage caution commensurate with the value of the payment

- **PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?**

This would trigger further assessment and investigations which would lead to a further increase of costs.

#### **8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**

- **any threshold should be set at no more than £100**

- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

Comments to each bullet point here reflect those on Q7.

It is questionable whether such amount is significant enough to represent a real damage to consumers' life and to encourage consumers to be careful and to thoroughly question whether there is a risk that their APP is subject to fraud. In any event PSPs should thoroughly publicise their threshold and excess amounts as part of their financial education for consumers.

---

## **9. Do you have comments on our proposal not to have a maximum threshold?**

The absence of a maximum threshold would drive increased risk in the financial institutions - PSPs intentionally set limits within their risk appetite - these are carefully considered and managed regularly with Transaction Monitoring, rules, checks and continuous maintenance. The proposal essentially ignores the limits put in place by individual PSPs and would lead to a race to the top whereby the PSPs with the biggest limits gain a competitive advantage while only bearing half of the risk. This in itself would introduce unbearable risk to the financial institutions. Particularly the smaller PSPs - many of which aim to serve the traditionally underserved segments of consumers and businesses.

We would like to seek clarification on how this maximum threshold works in relation to limits imposed by particular institutions and the 50:50 default. For example, if a victim of APP transferred £5m from PSP A to PSP B, C. How would the 50:50 default be applied? If PSP B, for example, were to have a single payment threshold of £500,000 and they did not prevent the total £500,000 from being exited, what amount would they be expected to repay to PSP A? We would anticipate that they would only be liable for the amount received and therefore, 50:50 would equate to PSP B's reimbursement of £250,000. If PSP C were able to secure the full return of the funds, how would this be allocated between PSP A and PSP B?

## **10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

A 13 month time-limit would likely require PSPs to hold liquid assets well in excess of any normal current levels. This would be required to cover any transaction that exits their accounts for a 13 month period.

- **any time-limit should be set at no less than 13 months?**

In addition, if the 50:50 rule were introduced, PSPs would need to hold further liquid assets to cover for 50% of the funds that enter their accounts. This would be a significant challenge for the UK's largest PSPs, it would be insurmountable for the smaller ones.

The majority of scams are realised within a time frame shorter than 13 months. Consumers generally become aware they have been scammed within a few hours of making most payments. Additionally, while the proposal is aimed at prevention of scams, the 13 month limit does not consider the importance of reporting and recovery on fraudsters.

Swift reporting leads to accounts being blocked/closed, and an increased likelihood of the funds being secured not only for the reporting victim but likely for various others that may not have yet become aware of the scam.

PSPs should be incentivised to report swiftly and improve the channels of reporting between FIs in order to promptly close down accounts which have directly or indirectly benefited from fraud.



---

If consumers have a longer timeframe to identify fraud, this reduces likelihood of identifying fraudulent accounts being found quickly, closing down fraudster accounts and attempting recovery of funds that are available.

The 13 month term should be reserved for more complex scams e.g flight tickets, investment or romance scams whereby often the victim's of such scams are duped on an on-going basis over a longer time period. A much shorter time frame should be imposed for less complex scams such as buying goods online or booked services not received (such as construction work). Otherwise, consumers may allow fraudsters longer timeframes before reacting, giving them the benefit of doubt. This may in turn result in the consumer being taken advantage of by the fraudster; the longer they are in communication with them, the more likely they may be convinced to send further funds or have their information passed on to "recovery" scammers. Additionally, they would lack the direction from FIs regarding securing their personal and financial information.

#### **11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**

Here the concern is that the proposals are making Payment Service Providers ("PSPs") solely responsible for compensating victims of APP fraud and this distorts incentives. The onus should be on all players in the APP scams ecosystem — including also technology and telecoms firms — to stop scams at source before they adversely impact consumers.

- **reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?** 48 hours would be highly challenging and costly for PSPs - consider for example the Christmas period in which there are several bank holidays in close succession. It would be unreasonable to expect PSPs to handle all cases with such rapidity.

Furthermore, considering an instance in which (according to the 13 month allowance proposed) the victim has submitted a claim from a complex, Christmas-related scam - they submit the claim the following Christmas - it does not seem practicable to make an assessment of a complex case after a significant period of time has passed within such short time-frames.

The requirement to refund within 48 hours fails to understand the significant complexity of many APP scams. Sometimes it may not be immediately evident whether a customer has been scammed or simply made a bad investment decision. Investigations and refunding within 48 hours, particularly across a weekend, seems unrealistic and especially if we require contact with 3rd party banks/financial institutions. There would be another considerable operational impact to support the delivery within this timeframe.

The Organised Criminal Groups are likely to benefit the most here - 48 hours ties the hands of the investigator and this is likely to be exploited by fraud rings working together to commit first party fraud.

A couple of suggestions that would make sense here would be:

- providing guidelines to assess scams by complexity and to help with evidence of suspicion, and

- 
- giving PSPs more time to investigate more complex, higher value cases, would make more sense.

The Consultation Paper as it is would end up favouring larger banks as they can dedicate time and resources to investigations (especially those with teams outside of the UK).

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

In line with the recitals to PSD2, there should be clear and convincing evidence where there is a high suspicion of an unauthorised transaction resulting from fraudulent behaviour by the payment service user and where that suspicion is based on objective grounds.

Gross negligence should mean more than mere negligence, involving conduct exhibiting a significant degree of carelessness.

The length of investigation should be agreed in accordance to the complexity of the scam.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

This is a new proposal that could impose liability on receiving PSPs even where they have no power to prevent the transaction from occurring. The PSR has indicated that the "default" 50:50 sharing of responsibility can be amended by contractual agreement between PSPs, but in a market where the majority of transaction "initiations" are carried out by a handful of major retail banks, negotiating a change from the default position would be difficult in practice.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

The requirement that the reimbursement should be split 50:50 may cause issues for PSPs, in terms of administration costs and the proposal for a dispute resolution process to adjust this allocation is likely to increase the costs of business for PSPs.

Fintechs will be at a disadvantage here; they would require teams and resources dedicated to responding to dispute resolutions. Whereas the traditional banks have large scale legal teams and would be more readily able to dedicate resources here.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

Unclear how this would work in practice, especially with the 48 hour refund timeframe. The victim's institution from where the payment was sent will bear the immediate brunt of the cost. Recovery of these funds could be a lengthy process to the sending institution's detriment.

Where some of the funds are recoverable or partially recoverable (via indemnity), it would be useful to have direction on the expectations/process anticipated for each institution in this regard. By default, the first outcome should be for institutions to return any recoverable

---

property first, before any consideration is made to reimbursement. Thereafter, the receiving institution(s) should only be liable for 50% of the amount that credited their account, rather than the total amount of the fraud. Institutions should deduct any amount it recovers from the 50% liability owed amount.

Additionally, this is very complex the further the funds are dispersed. Often by the 4th or 5th generation it is likely that the beneficiary has no knowledge of the perpetrated fraud. A number of beneficiaries, irrespective of the amount paid to them, may be legitimate (for example a business that has provided a service to a 3rd party, who has paid for this service with their fraudulently obtained funds). These scenarios would need to be carefully considered to determine a reasonable cut-off/line drawn to pursue the 50:50 allocation. It may be relevant to assign the beneficiary a role in the fraud e.g malicious (where the party would appear to be involved; by virtue of the way in which they subsequently spend these funds) vs bystander (where they would appear to be legitimate but for receiving fraudulent funds).

Payments outside of the Faster Payment Scheme should be included on a 50:50 default, as financial institutions such as cryptocurrency exchanges should be held to the same standard of fraud prevention and monitoring controls.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

This is connected with question 13. Reimbursements to the customers as well as allocations of repatriated funds should keep in consideration that receiving PSPs have no power to prevent the transaction from occurring. The default position should not be 50:50, leaving the receiving PSP the only solution to try to negotiate contractually a different allocation percentage, as this will be a further cost to manage.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

All the directly connected PSP participants (sending and receiving) should fall under the rules of allocating the cost of reimbursement, but the rules should take into consideration the costs of the use of dispute resolution process to refine the allocation of reimbursement.

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

A body which oversees and monitors the compliance to rules that address fraud risks in the system would be a necessary tool to give protection to customers.

This also would avoid that complaints re APP scams are dealt by the Financial Ombudsman Service. The flexibility afforded to the FOS has resulted in a number of claims by APP fraud victims against PSPs being upheld with additional obligations and standards being imposed on the PSP as to what is expected of them. As a result FOS could become a lawmaker.

---

However, the authority that should cover the role of making, maintaining, refining, monitoring and enforcing compliance should include the PSR too as a bridge between the Payment System Operator and the users of the said system.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement Proposals?**

No comment on this.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We understand that the focus should be on achieving the desired objectives of the reform, establishing - in consultation with industry - the most effective means of meeting those objectives and introducing agreed requirements that will lead to them. The objectives include '50. The Competition Objective', '51 The innovation objective', '52 The service-user objective'.

We do not feel that the proposal would best achieve these objectives and instead risks a reduction in competition and innovation at the detriment to the interests of users of payment systems.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

Care should be taken when developing these arrangements and the allocation criteria to take into account the resource constraints that small PSPs might have to engage in an additional dispute resolution process and further costs.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

No comment on this.

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

No comment on this.

**24. Do you have views on the best option for short-term enforcement arrangements?**

The arrangement described looks to divide the powers of enforcement between PSR and Pay.UK, this could lead to an unfair and inconsistent approach. There is a degree of subjectiveness on the particulars of cases; such as those where first party fraud is suspected. This will require clear guidance and enforcement arrangements should be defined from the outset.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

---

The first one potentially would be the most consistent and cost effective (*"The PSR gives a direction to all indirect PSPs to comply with the reimbursement rules in Faster Payments"*) as PSR is the key player in the implementation of these rules, so it should be the best body to give direction based on section 54 of FSBRA. Furthermore the other options are involving IAPs making the process longer and contentious.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

The best and most consistent solution is that PSR would direct both the IAP and indirect PSP.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

There is no serious cost benefit analysis shown at Annex 2. There is only a very high level and totally detached approach that is weighing one large cost on one side cancelled out by the same scale of benefit on the other. There is insufficient evidence that a robust cost-benefit analysis has been undertaken with respect to the impact of the proposals for start-up and scale-up PSPs.

The PSR's proposals will impact on operational costs for PSPs and a significant risk to early stage, funded businesses that do not have the financial resiliency to reimburse significant sums. Mandatory reimbursement costs are estimated to represent at least a tenth of PSPs' revenue, according to the wider FinTech ecosystem.

In terms of benefits, a few comments here below on measures 1 and 2.

There are some concerns that publishing scam data (Measure 1) will highlight to fraudsters any weaknesses in controls across the industry. Scammers would be able to learn the firms' controls, and use this to better tailor their social engineering, maybe targeting victims from one or two PSPs who have all fallen victim to similar scams. The publication of Measure 1 data creates a risk that this kind of pack mentality on the part of fraudsters is exacerbated and could drive a material increase of APP scams.

Intelligence sharing (Measure 2) will be difficult to achieve, because the principal barrier is the current legislative framework (e.g. PSPs are constrained from intelligence sharing due to confidentiality duties as well as data protection law), and legislative amendments are needed from the government to better allow firms to share intelligence about fraud.

**28. Do you have any other comments on the proposals in this consultation?**

The Consultation Paper and its proposals if implemented could trigger several consequences:

- increasing sharing of data in order to stop fraudsters opening accounts - more likely to result in unfair treatment when institutions share data;
- urgency to secure funds without fully investigating. Customers that may be suspected of committing first party fraud - even where this has not been substantiated - will likely be tarred with the same brush as fraudsters;
- increasing costs as newer PSPs will struggle to be started, without significant funding to support fraud controls and reimbursement from the outset. If the

---

proposed changes are implemented, many Fintech PSPs will not survive, immediately reducing the competition within the financial services industry to the detriment of consumers;

- access to financial services are likely to be reduced, more time-consuming and possibly unfairly restricted.

OCGs are already increasing exploitation of mules, reimbursement and data sharing may consequently incentivise this activity further.

If on one side the Consultation Paper's aim is to protect more victims of APP scams, and its implementation can be welcomed for this, on the other side the general public may not be fully aware that this is a new industry requirement, once a consumer directly experiences difficulties and barriers to complete transactions online there may be a mixture of reactions including frustration/feeling unduly targeted/discriminated against.

A further concern is that focusing on reimbursement pulls attention away from prevention on a more general scale. Evidence is that there are both financial and emotional penalties from scams, with reimbursement fixing only the former.

Also given the impact that the proposals in this consultation can have on the future of the Fintech industry, it would have been beneficial to have a more data driven analysis on aspects such as:

- the impact of the proposal on cost benefits vs costs incurred, and
- the costs to customers if PSPs introduce stronger controls (costs as a consequence of payments being queried, delayed or even declined).

Finally, the currently deteriorating macroeconomic climate needs to be taken into consideration to protect the Fintech industry and find the right balance between ensuring customer protection on one hand and increasing benefits on the other (faster services and lower costs).

Yours sincerely,

**Counting Ltd.**

# Coventry Building Society

## PSR CP22-4 APP Scams: Requiring Reimbursement

### Summary

We are extremely sympathetic to any individual who falls victim to a scam and treat our customers accordingly deploying processes and controls designed to prevent fraud and reimbursing the vast majority of victims. It is Coventry Building Society's view that Mandatory Reimbursement is unlikely to be effective in reducing the volume of APP Scams. Neither do we believe it is proportionate, and therefore we do not support the overall proposal.

We would like to highlight the need to ensure setting industry-wide parameters across each of the measures proposed – for excesses, minimum and maximum claim limits, and “time-barring” of claims should all be standardised to ensure clarity for consumers.

The impact of a scam on an individual extends far beyond the financial loss one suffers, and we are committed to addressing the risk of our customers, and all consumers, falling victim to scams. We have put in place a number of measures to reduce the likelihood of our customers falling victim, as follows:

- Direct intervention where a payment is identified as unusual or suspicious.
- Considerable investment in technology to support identification and prevention of fraud
- Ongoing Training & Development for individual staff in Customer-facing roles, within our Financial Crime Team, and the wider Society.
- A dedicated Fraud Education team working directly with Staff and customers to provide ongoing and relevant Fraud Information interventions.

We take our responsibilities in this area incredibly seriously and believe that the resource and effort of the industry should continue to focus on preventing scams through these measures, including collaboration with other stakeholders such as Government, social media, Telecoms, and wider industry. We are concerned that implementing Mandatory Reimbursement for PSPs could further disincentivise some stakeholders from preventing fraud.

#### 1. Do you have any views on the impact of our proposals on consumers?

- On a simplistic level we agree that mandatory reimbursement would of benefit to consumers, particularly on an 'individual' basis.
- It is inevitable that imposing mandatory reimbursement will result in firms introducing more challenge into the payment journey by way of scam warnings, direct questioning, delayed payments and even cancelled payments. Whilst this will have a beneficial impact on cases where a payment is subject to a scam, it is also likely to negatively impact most payments that are genuine, creating frustration for more consumers. The consultation document states that this friction is proportionate to preventing APP Scams, however this has not been quantified by the PSR.
- It is likely that mandatory reimbursement will increase fraud losses for PSPs, particularly in the short-term. PSPs may seek to recoup these costs through other methods, such as paid-for banking, increase in other bank charges and/or poorer savings interest rates. This creates a risk that consumers will end up suffering disproportionately.
- The consultation document states that “APP Scams continue to grow”. This is despite a context of increased prevention effort by PSPs, concerted education campaigns by industry, technological improvements such as Confirmation of Payee



and the CRM code. We would therefore contend that mandatory reimbursement could make the picture worse for consumers.

- We believe that mandatory reimbursement transfers incentives disproportionately from consumers to PSPs to act with care when making a payment to an extent removing to a degree the incentive for the consumer to exercise caution.
- Although the consultation states there is a lack of evidence that consumers would take less care, there is a risk that consumers will potentially be more immune to scam warnings in the event they perceive there is less risk because reimbursement is effectively guaranteed. We anticipate this being particularly relevant to purchase scams, where the consumer may be more willing to “take the risk” for an item that they wish to purchase.
  - Based on case evidence we have seen where consumers have questioned fraudsters as to whether they are scammers, we believe a move to mandatory reimbursement will lead to adoption of a tactic used by fraudsters where they convince the customer they are not taking any risks because their bank will always reimburse them, “even if they are a fraudster”.
  - Our experience across several APP Scams is that it is often incredibly hard to penetrate the ‘spell’ the fraudster has over the customer, leaving us with limited scope to prevent fraud regardless of technology and questioning. Therefore we believe strongly that considerable effort through education needs to be put into giving control and responsibility to the customer to undertake their own due diligence and thus make good, informed decisions. The risk of mandatory reimbursement is that consumers become less engaged with education initiatives as there is a perceived lesser benefit.
- We are also concerned that mandatory reimbursement will not materially reduce APP Fraud.
  - Whilst in theory it will create an incentive for firms to ‘get better’ at preventing fraud, this is not a simple ‘transition’ – we believe there are already significant incentives for firms to prevent fraud.
  - The consultation’s own evidence outlines a jump from 19% of cases reimbursed pre-CRM code to 41% post CRM code, yet outlines that Fraud continues to grow.
  - We are also concerned, based on internal case evidence that mandatory reimbursement may impact a victims willingness to co-operate with law enforcement after the event. Whilst in a reimbursement scenario, the PSP would become the ‘victim’, the testimony and information of the consumer would be essential to any meaningful investigation. This would negatively affect law enforcement investigations and lead to reduced disruption, reduced enforcement, and potentially even increased fraud levels.

## 2. Do you have views on the impact of our proposals on PSPs?

- It is correct that PSPs ‘require’ incentives- to prevent customers falling victim to scams and there are considerable and sufficient incentives that already exist:
  - Good customer outcomes (protection from harm, goodwill)
  - Customer Satisfaction and repeat/referral business

- Financial Benefit (potential reimbursement, cost of investigation)
  - Regulatory Incentives (potential for enforcement/other action)
  - We agree that mandatory reimbursement could provide positive incentives for firms to prevent scams, particularly investment in detection technology.
  - In general, the cost implication for Coventry Building Society (CBS) purely in terms of reimbursement is not likely to be material, given that we already have a strong prevention ethos with APP Fraud and we currently reimburse the vast majority of APP Claims.
  - As a Savings provider we are less transactional and have more difficulty building behavioural intelligence around our customers – this can impact our ability to identify unusual transactions effectively.
  - PSPs currently undertake detailed investigations into complex fraud, often helping Law Enforcement to disrupt Serious and Organised Crime (SOC). Whilst mandatory reimbursement may provide a greater prevention incentive, an indirect consequence is likely to be a reduction of investment in “after the fact” investigations due to the “pre-determined” outcome of a case. In contrast to the stated aims of the proposal, this is likely to negatively impact any hoped-for reduction in Scams and Fraud.
  - We would anticipate an increase in First-party fraud attempts – with reimbursement guaranteed, there is an increased incentive for individuals to commit fraud of this nature, and an increased likelihood of success.
  - Recent prevention work by CBS has led to a c.100% increase in complaint numbers where we have challenged more customers about the purpose and destination of their payment. Typically, individuals sending large amounts of money are confident and self-assured and are not happy to be challenged or questioned. That said, we have also received some positive feedback where customers have been prevented from sending money that was subject to a scam.
  - It is our view that any mandatory reimbursement scheme would have to be supported by the Financial Ombudsman Service. We have seen several case outcomes that we believe to be unjustified based on current industry guidance, and any change driven by the PSR could result in further poor outcomes for PSPs.
3. Do you have views on the scope we propose for our requirements on reimbursement?
- We do not agree that there should be any excess payable by the consumer where they are reimbursed
  - We do not believe there should be any minimum claim limit for APP Fraud
  - We do agree that all PSPs, direct or indirect, should be subject to the same rules and regulations.
4. Do you have comments on our proposals:
- That there should be a consumer caution exception to mandatory reimbursement?
    - It is essential we work within a framework where all parties are incentivised to prevent scams. This is essential to prevent loss and harm, and to prevent SOC being funded.
    - Consumers are an essential stakeholder in the prevention journey and there needs to be a framework that strongly incentivises them to take sensible and informed decisions in consultation with their PSP.
  - To use gross negligence as the customer caution exemption.

- In principle, we agree that this is an appropriate exemption to decision-making about reimbursement.
  - Not to provide additional guidance on gross negligence.
    - There is no concept in English Civil Law differentiating between “Negligence” and “Gross Negligence” - if there is no clear guidance on gross negligence, it will be very difficult to achieve consistency in respect of refusal of reimbursement.
    - It is essential that all stakeholders have clear agreement on what constitutes gross negligence, supported by case studies to illustrate how this may translate in practical terms. Our experience is that a PSPs perception of what constitutes Gross Negligence is subjective, and is different from, for example the Financial Ombudsman Service.
5. Do you have comments on our proposal to require reimbursement of vulnerable customers even if they acted with gross negligence?
- Identifying vulnerability at a point in time can be very challenging, particularly looking in “hindsight”. It is also often a subjective matter – this is particularly true when considering whether the specific vulnerability contributed to a customer falling victim to a scam.
  - We do not agree that a blanket approach is appropriate – vulnerability comes in many different forms, and whilst a customer may have some characteristics of vulnerability, it may not always be that their specific vulnerability has contributed to them falling victim or being grossly negligent. In addition not all vulnerabilities are visible.
  - Where a customer’s vulnerability is deemed to be a contributory factor in them falling victim to a scam/acting with gross negligence, we agree that reimbursement should be made.
6. Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?
- In our view to ensure consistency, it is essential that the FCA’s definition of a vulnerable customer is used across the industry.
7. Do you have comments on our proposals that:
- Sending PSPs should be allowed to apply a modest fixed excess to reimbursement?
    - In our view there is little value in applying an excess to claims. With larger APP values, any excess would be ‘immaterial’ and would not provide any incentive to customers to “take greater care”, particularly where they believe they are making a genuine transaction.
    - The PSRs 2017 allows PSPs to require that a payer is liable up to £35 for losses incurred in respect of unauthorised transactions. We do not enforce this excess, and do not believe it is widely used in the industry. It is not economical for us to enforce an excess and is not aligned with our customer focus.
    - In our view allowing the ability to apply an excess to reimbursement is contradictory to the principles behind the proposals and does not provide a proportionate benefit to PSPs or consumers, and nor does it provide any benefits in terms of reducing fraud. If a case warrants reimbursement because of the circumstances, we believe this should be in full.
  - Any ‘excess’ should be set at no more than £35?
    - No further comment

- PSPs should be able to exempt any vulnerable customers from any 'excess' they apply?
    - No further comment
8. Do you have any comments on our proposals that:
- Sending PSPs should be able to set a minimum claim threshold?
    - We agree that identifying smaller value payments is more challenging, however on principle we do not agree that there should be a minimum claim threshold – this appears to go against the principles of mandatory reimbursement i.e., protecting customers from financial loss.
    - We believe that that lower value payments disproportionately impact people at greater risk/harm as consumers with low value claims may be particularly vulnerable.
    - If a minimum claim threshold was introduced, this would remove an incentive for consumers to report lower value scams to PSPs. This would prevent opportunities for early intervention and safeguarding where customers are at risk of falling victim to higher value scams, and also identification of mule accounts being used to facilitate fraud.
    - The disincentive to report would also remove important intelligence from the industry and law enforcement that is used to prevent and detect fraud and educate consumers.
  - Any threshold should be set at no more than £100?
    - No Further comment
  - PSPs should be able to exempt any vulnerable customers from any threshold they set?
    - No further comment
9. Do you have comments on our proposals not to have a maximum threshold?
- We agree that there should **not** be a maximum threshold
10. Do you have comments on our proposals that:
- Sending PSPs should be able to set a time limit for claims for mandatory reimbursement?
    - We agree that there should be a time limit on any fraud claim, as the longer time passes since the event, the more investigative opportunities reduce, not least the consumers recollection of events.
  - Any time limit should be no less than 13 months?
    - We believe that any time limit should be established following analysis of average claim times from existing data – many scams are one-off and identifiable immediately by the victim, however others are 'ongoing', and considerable time can pass before the victim is aware.
    - Any time limit should provide adequate consideration of longer-term scams, however should not be so long as to disincentivise timely reporting by victims (timely reporting increases the likelihood of recovery and viable investigative opportunities).
    - Our current position is that we would consider any exceptional circumstances where there has been significant delay to reporting and we believe that PSPs should have the flexibility to do this particularly where there is an indication of vulnerability or where the decision not to investigate may negatively impact a consumer.
11. Do you have comments on our proposals that:

- The sending PSP is responsible for reimbursing the customer?
    - We agree in all cases where reimbursement is made, the sending PSP should be responsible for reimbursing the customer
  - Reimbursement should be made as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence
    - In principle we do not object to a time limit and we agree that reimbursement should be made within the shortest timeframe possible.
    - We believe that 48 hours is too short to establish the facts of what are often complex cases.
    - We understand the 48-hour proposal comes from the regulations around unauthorised payments, however we believe APP cases are significantly different in so far as the customer is aware they have sent the money, and therefore are likely to have accounted for not having that money at that time.
    - In our view, there would be considerable risk to such a timescale, which is likely to be exploited by First-Party Fraudsters who would look to make a claim and obtain reimbursement without a firm's ability to undertake a full investigation.
    - This risk could also lend itself to poor customer outcomes where a consumer is reimbursed, and subsequent information comes to light that leads to that reimbursement being retracted. In the scenario of an incorrect initial decision, this could also have implications for the beneficiary account – for example that account being frozen.
    - We have considerable experience under the PSR 2017 regulations, that once a consumer has been reimbursed, their level of engagement with us and law enforcement often drops significantly. We believe such a demanding timescale of reimbursement would damage the ability to investigate cases fully and therefore lead to less disruption, less enforcement and increased fraud.
    - We believe a period of 15 days would be a more appropriate timescale, with a caveat to increase to 35 days if required. This is in line with Payment Services Complaints Regulations, and provides a more appropriate timescale for understanding the position. Given that the core tenet of an investigation is engagement with the (often distressed) victim, it is vital that PSPs have appropriate opportunity to gather that first-party information without the pressure of a tight timescale adding to the distress a victim is already suffering.
12. What standard of evidence for first party fraud or gross negligence would be sufficient to enable a PSP to take more time to investigate and how long should the PSP have to investigate in those circumstances?
- For first party fraud and gross negligence it should be “reasonable grounds to suspect” i.e. a reasonable person would suspect that it could be first party fraud, or gross negligence is present
13. Do you have comments on our proposals for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?
- We agree that there is a strong need to incentivise PSPs to have robust controls to prevent money mule activity, and do agree there should be a

mechanism to ensure that where a receiving PSP contributes to financial loss, they are responsible for part of the reimbursement

- The risk of a 50:50 default allocation is that in most cases it is unlikely to reflect the level of responsibility on the sending and receiving bank and Savings providers may suffer a disproportionate impact due to the higher volume of transactions originating from current account providers.
  - Whilst we currently see very low levels of loss as the receiving PSP, this is primarily due to our “next day” payment model. The imposition of a 50% liability model could disincentivise firms from widening banking services, particularly into same day payments, as this would increase the likelihood of fraudsters taking advantage of firms like ourselves. As such, we consider this could be anti-competitive.
  - We do see some benefit where reimbursement is agreed, in a formula to define who should be responsible for reimbursement costs between sending and receiving PSPs and acknowledge that this would be difficult without strict guidance as there will often be a difference of opinion between the sending and receiving PSP.
14. Do you have views on our proposal that PSPs are able to depart from the 50:50 default allocation by negotiation, mediation, or dispute resolution based on a designated set of more tailored allocation criteria
- Where reimbursement is agreed, PSPs should be able to agree on an appropriate allocation of reimbursement costs, however we would welcome clarification as to when and how dispute resolution would work so as not to disadvantage consumers – particularly around at what point dispute resolution could be invoked.
15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?
- Any formulaic approach could be applied to multi-generational scams in the same way, regardless of number of parties, for example:
    - APP Scam £100k
      - a. Sending PSP- (1) liable for £50k, Receiving (2) £50k
      - b. (2) sends that £50k on to (3) before it leaves UK system
      - c. (2) liable for £25k, (3) Liable for £25k
      - d. Total Liability (1) - £50k (2) - £25k (3) - £25k
        - i. The same approach could be taken where multiple movement of funds etc.
16. Do you have comments on our proposal for 50:50 allocation of repatriated funds between sending and receiving PSPs?
- We believe that repatriation of funds should be allocated according to the original split/proportion of reimbursement.
  - In our view, some of the challenges raised in the consultation could be addressed by allowing firms to directly repatriate funds further down the line (e.g., in the above example with 3 links to the chain, (3) could directly reimburse to (1))
17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?
- We believe there should be a consistent approach across the industry.



18. Do you have views on our long-term vision and our rationale for the PSO being the rule-setter responsible for mitigating fraud?
  - We agree that the PSO should be the rule-setter responsible for mitigating fraud, however this needs to be in sensible consultation with industry.
19. Do you have comments on the initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?
  - No Further comment
20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?
  - No Further comment
21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?
  - Any formulaic approach to allocation criteria and dispute resolution should be developed by way of a proposal in consultation with scheme members. A full consultation document should then be issued before any final decision taken.
22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?
  - An ideal solution is to build a platform capable of managing everything digitally where all PSPs had access and could send messages between each other. This overall management environment for APP claims would then naturally contain all the information required to undertake appropriate monitoring.
23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?
  - There would be considerable benefit to implementing a system of this nature regardless of enforcement of mandatory reimbursement, however it is impossible to provide any commitment or comment without understanding costs and implementation timescales from Pay.UK
24. Do you have views on the best option for short-term enforcement arrangements?
  - No Further Comment
25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?
  - No Further Comment
26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?
  - No Further Comment
27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?
  - No Further Comment
28. Do you have any other comments on the proposals in this consultation?
  - Whilst the PSR has no jurisdiction outside PSPs, we are concerned that mandatory reimbursement and sole focus on PSPs continues to avoid a major part of the problem.
  - There are many other stakeholders in the APP process, particularly Social Media Firms and Telecoms Companies. Indeed, any organisation that holds sensitive personal data is at risk of acting in a way that enhances the

opportunity for fraudsters to commit scams. We need to create greater incentives for them to protect 'society' and prevent APP fraud.

- It is our view that any directed approach to reimbursement should be considered alongside several measures, and not in isolation. Not doing so could result in potentially poor outcomes for consumers, increased cost of banking services and reduced autonomy for consumers, all without any empirical evidence supporting the argument that this will reduce APP Fraud – in fact the quantitative evidence to date suggests the opposite.
- The APP Scam environment has become complex – particularly when it comes to Investments – more specifically Cryptocurrency. Cryptoassets are not currently regulated, and there is often a significant lack of clarity between whether a payment for this purpose is genuinely a scam, or just an 'investment gone wrong' with an unregulated or poorly run firm. We would welcome clarity on the scope of the proposals in relation to actions proposed where it fits into the latter category.
- We would welcome clarification from the PSR regarding payments from a PSP to an account in the same legal entity with another Financial Services Institution that is subsequently sent to a fraudster. It is our view that the original PSP would not be defined as an additional "sending PSP" in this scenario.



# Cyber Defence Alliance

 <p><b>CYBER DEFENCE ALLIANCE</b></p> 	<h1>PSR APP Re-imburement consultation response</h1>
<p>TLP: Amber (no attribution)</p>	<h2>NON-CONFIDENTIAL RESPONSE</h2>

[Redacted]	[Redacted]
Date Issued	31 October 2022
Author	[Redacted]

Please contact [operations@cda.financial](mailto:operations@cda.financial) with any queries or feedback regarding on this report.

## 1 Executive Summary

The Cyber Defence Alliance’s provides intelligence relating to Cyber Threat Intelligence (CTI) particularly in relation to network defence and disrupting online cybercrime.

As we collect and develop significant intelligence about fraudsters targeting UK banks and work with UK and International law enforcement to disrupt such criminals, we are able to provide insight into past and current behaviour and can predict likely changes in fraudsters tactics.

The CDA believe that the proposed changes will result in increased targeting of the UK banking refund process by fraudsters. The lack of upper limit will lead to additional significant organised criminal groups, from the UK and abroad, targeting the UK banking sector and losses will be very significant. The proposed timescales, burden and level of proof would make proving that a refund claim is fraudulent very difficult.

There is already significant organised ‘refund fraud’ activity, mainly relating to direct debit and card transactions. Evidence of this has been submitted.

## 2 Who are the Cyber Defence Alliance

- 2.1 The Cyber Defence Alliance (CDA) is a non-profit company in the UK working with 13 financial organisations. Our area of work relates to Cyber Threat Intelligence (CTI) particularly in relation to network defence and disrupting online cybercrime. CDA CEO and Dep have a combined experience in LE of 65 years and have led teams in the UK and Internationally dealing with complex cyber and fraud cases as well as widescale abuse of the financial system
- 2.2 The CDA is staffed by a number of threat intelligence analysts and a fraud and cyber investigation team (FACIT). Those FACIT staff are all former law enforcement officers and an analyst with considerable fraud/cyber investigation experience. The CDA CEO and his deputy have a combined experience in law enforcement of 65

years and have led teams in the UK and Internationally dealing with complex cyber and fraud cases as well as widescale abuse of the financial system.

- 2.3 As part of this work the CDA seek to collect and develop intelligence relating to threat actors conducting frauds against UK banks. This intelligence gives the CDA insight into criminal methodologies targeting the UK financial sector.
- 2.4 We also seek to attribute who are the offenders behind these online usernames and work with UK & International law enforcement to disrupt, arrest and prosecute such offenders. Many of our observations are from our experience of collecting and developing such intelligence.

### 3 Specific consultation questions to be answered

The CDA is not a bank or other financial organisation. Therefore our experience and ability to answer all consultation questions with confirmed intelligence or strong anecdotal indicators is limited to particular areas within the PSR consultation.

This response seeks to provide relevant intelligence to address the following three questions:

- Question 2: Do you have views on the impact of our proposals on PSPs?
- Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?
- Question 11: Do you have comments on our proposals that:
  - the sending PSP is responsible for reimbursing the consumer and
  - reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?

### 4 CDA intelligence collection relating to fraudsters who target banks and their customers

- 4.1 The CDA collects intelligence from various sources.

### 5 Case Study: Organised refund fraud activity

- 5.1 The CDA recently carried out a short investigation in response to a reported increase in refund frauds observed by a CDA member. The results provide evidence that criminals already have a history of targeting the current refund process by offering “same day refunds” in their posts. It is assessed by the CDA that the PSR proposals concerning the mandated speed of a refund will only increase this targeting.

### 6 Fraudsters targeting banks who provide assurance on reimbursement

- 6.1 The CDA are able to show that fraudsters targeted a bank who were providing reimbursement for APP fraud.

### 7 International fraudsters targeting UK banking systems

- 7.1 The CDA has sought to identify the real-life identities of the organised criminal groups (OCGs) who target UK banks to conduct APP frauds or those who provide the criminal infrastructure/services to conduct APP frauds.
- 7.2 The CDA do this to share that intelligence with law enforcement and to work collaboratively with them with the objective of disrupting, arresting and prosecuting cyber and fraud criminals. The CDA has various law

enforcement information sharing agreements and have worked collaboratively on many investigations with considerable shared successes.

7.3 It has been noticed that fraudsters from around the world target the UK banking sector.

## 8 Insufficient time to identify 'reasonable grounds for suspicion or evidence' of fraud

- 8.1 The use of complicit but genuine customers can make it difficult to identify the fraud at an early stage and within 48 hours as further account analysis is required to create "reasonable grounds for suspicion" to delay the payment.
- 8.2 The failure of a victim to respond or who vaguely answers questions regarding their claim would not provide 'reasonable grounds for suspicion' and this would become the standard advice, from the above mentioned refund fraudsters to their account holders, in order to ensure pay-out.
- 8.3 Although many criminals will continue to not use complicit account holders, others will begin to conduct application frauds or use mule accounts in order to be able to create transactions and then request refunds. These claims would be for considerable amounts. Having only 48 hours for identifying that there is reasonable grounds for suspicion or evidence of fraud for claims of 100,000's or millions of pounds will lead to very significant individual losses.
- 8.4 The CDA held meetings with all the UK banks who were tasked with processing Bounce Back Loan (BBL) applications. They were instructed to conduct all necessary security checks and make a decision within 72 hours. All banks reported that this was insufficient time to be able to realistically find reasonable grounds for suspicion or evidence of frauds. It is clear that for this reason many fraudsters targeted this product and losses have been very significant as a consequence.
- 8.5 The proposal does not detail whether the 48 hours includes bank holidays and weekends. The CDA assess that it is likely that fraudulent claims will be lodged at times which would frustrate many banks from making a balanced decision on reimbursement e.g. 6pm on a Friday; bank holiday and other times when fraud professionals able to make informed decisions are much less likely to be available or victims would be less responsive.

## 9 'Reasonable grounds for suspicion or evidence' of fraud is too high a standard of proof

- 9.1 As 'Reasonable grounds for suspicion or evidence' of fraud appears to be the same bar for which UK police could exercise their arrest powers ("*anyone whom he has reasonable grounds for suspecting ....*") therefore, the proposed changes suggest that if a bank did not have a high enough level of proof that a police officer could use to make an arrest then they cannot refuse to reimburse a customer. Therefore, the proposed changes suggest that if a customer refused to answer any questions about a refund claim they could not be refused reimbursement.
- 9.2 Combining the required level of proof required to not reimburse within 48 hours and the time constraints involved, this would effectively mean that almost all refund frauds will go unchallenged.

## 10 The lack of upper limit will attract significant OCG activity

- 10.1 If claims of losses up to 100,000s or millions of pounds are required to be settled within 48 hours of being reported this will attract very significant organised criminal group's attention. Fraudulent claims, by professional fraudsters, will be very difficult to disprove and losses will be very significant.
- 10.2 Scenario: It would be quite trivial for criminals to open an account online with false details; place significant funds into the account; transfer it to another account under their control, from where it is removed and then

to claim this transfer was as a result of an APP fraud. Disproving the claim, within 48 hours, would be near impossible.

This would be conducted at scale by these OCGs for 6 figure amounts or higher. Losses would be significant.

- 10.3 The PSR may wish to consider that mandated partial payments within set time frame in high value claims may be more proportionate. This mitigates hardship in genuine refund cases and allows a detailed investigation to continue for value refund cases.

## 11 Summary of findings

- 11.1 The UK criminal marketplace already includes many fraudsters whose main criminality is to encourage and assist bank account holders to make false refund claims. Currently, these refunds claim are mainly for card transactions and direct debits. The proposed changes will lead to an increase in false refund claims for APP frauds.
- 11.2 The proposed change relating to timescale to find reasonable suspicion or evidence of frauds will make detecting such activity more difficult, if not impossible. Such fraudsters are very professional and will circulate best practice to avoid suspicion. The less time that banks have to investigate will lead to an increase in fraudulent claims.
- 11.3 The required standard of proof that a refund claim is fraudulent will lead to almost all fraudulent claims being authorised. Combine this with the above time constraints and an extremely low number of fraudulent claims will be refused.
- 11.4 We expect to see the application frauds being combined with APP refund scams to defraud banks out of considerable funds. APP reimbursement values will be very significant. The fraudulent refunds amounts will also be significant.
- 11.5 Any bank that is identified as being more likely to provide reimbursement will become the target of increased fraudulent activity. Any league table of best banks for providing reimbursement will be used by fraudsters to determine which banks they will target.
- 11.6 The lack of upper limit will attract the attention of organised criminal groups.
- 11.7 The proposed changes will attract more foreign national criminals to target the UK banking sector.

# CYBERA

## PSR Consultation from CYBERA

Cybera Global Group: Cybera Global Ltd (UK), Cybera Global Inc. (USA), Cybera Global AG (Switzerland)  
www.cybera.io

### Consultation Feedback, 18<sup>th</sup> of November 2022

#### 1. Do you have views on the impact of our proposals on consumers?

Aligning incentives is key to ensuring further fraud investments, so overall these proposals should help consumers, provided PSPs do make the investments they need to. This should both reduce losses to consumers, and lead to fewer successful fraud cases.

However, given the scope of the proposals, it is likely to cause a shift in the way the frauds are perpetuated. We have already seen this with the introduction of Confirmation of Payee (COP) so that non-COP beneficiaries are used more. Further a move away from invoice and mandate scams that are harder to accomplish with COP in place. Whilst firms are likely to leverage investments across the other payment types such as Swift and Crypto, the controls will not be as rich and, therefore, we may see a shift if controls indeed result in reducing the successful incidents of scams.

Frauds may shift payment rails as follows:

- Increase in payments to existing beneficiaries with social engineering of the end users to get the funds
- Increase in non-FPS/CHAPs payments methods:
  - use of gift card purchases to receive the funds – Presumably, this would not be refunded.
  - in SWIFT payments on the first leg - partially Romance Scams and Investment scams that can more easily fit the story.
  - in Crypto payments on the first leg.

In all cases, this really opens up differences in protection depending on the payment method used within the UK. Admittedly this is a problem for another day, but it should be recognized at this time. Global data sharing of known mules across fiat and Crypto can assist with this.

The outcome of the increased investments also means that genuine customers will start to see even more impacts on their banking and payments. This will be done in two main ways:

- More friction in the journey for new beneficiaries and other non-regular payments
- Increased closure of accounts, either just to avoid costs and risk, but also where there are real signs of potential mule behaviour.

Further, with the current economic headwinds, especially in the UK, we will see more people becoming money mules, both wittingly and unwittingly, including some mules who have been victims of account takeover or had their friends/family abuse their account

As with all these things, there will be false positives and therefore some people will have their accounts closed when they shouldn't. There is the potential for real negative impacts on consumers here in terms of their ability to have banking or banking-like services and potential hardship.

## 2. Do you have views on the impact of our proposals on PSPs?

As with much regulation, this will likely help large banks and be harder for some smaller PSPs, so might have the effect of reducing competition in the future but is the right thing to do. If some firms' business models are built on easy account opening, with insufficient controls, such that it causes a large level of money mules, frauds & scams, then this externality should be closed off. The fraud costs to society are likely much higher cost than any savings gained through competition.

There is a very real risk of first-party abuse here, so it is key that there is a sensible way to allow PSPs to delay paying out in certain circumstances. Aligning with PSD2 which allows a delay for unauthorized frauds where a SAR is provided may help. Clearly, monitoring for firms overusing this should be in place.

Firms will need to ensure they understand how to utilize DAML SARs correctly to avoid tipping off when dealing with beneficiary mule accounts. This may need support and clarity at an industry level.

## 3. Do you have views on the scope we propose for our requirements on reimbursement?

Steps should be taken to close the circle as much as possible on Crypto and Swift payments. Recognizing that this is out of the scope of the PSRs remit, nevertheless, there should be an expectation that all PSPs operating in the UK, including crypto exchanges and custodians, should meet these rules and apply the right level of controls on outbound payments in line with this. UK-based crypto firms should also need to meet the same beneficiary standards.

## 4. Do you have comments on our proposals:

### • that there should be a consumer caution exception to mandatory reimbursement

Yes, this is sensible and FCA, PSR and the industry should be taking steps through education and awareness campaigns to make people aware of:

- The scams that are happening and that these are facilitated by money mules.
- The seriousness of the potential impacts on themselves of being a money mule.
- That consumers will be refunded provided they are not complicit or negligent.

### • to use gross negligence as the consumer caution exception

Yes, this makes sense, subject to the points noted below.

### • not to provide additional guidance on gross negligence?

There needs to be some steer here over the high bar element, especially as to how this fits with First Party Fraud (FPF) prevention. Without more guidance, this will be the area of argument by either sender or beneficiary bank. Guidance to reduce the size of this grey area is required, e.g., what is defiantly not Gross Negligence. Examples that would need clarity are:

- Responding to a phishing email
- Providing an OTP



- Moving funds to a safe account
- Moving ahead with a payment despite a COP result that is not a straight match
- Ignoring clear warnings from the PSP that this is likely a scam

## **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

This is morally correct, but it does call out how refunds for this group should be funded and what wider controls need to be put in place. It is likely that this requirement could reduce the services available to the vulnerable customer population or result in increased charges for this group or for all customers to fund this through higher charges elsewhere. The PSR should work with the FCA and industry to avoid wholesale de-risking of these accounts.

In addition, attempt to influence increased law enforcement response to increase the chances of freezing funds and recovery, including cross border.

## **6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

This is sensible. There is no need for any further different definitions.

## **7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**

This seems a sensible approach subject to the caveats outlined below.

- **any 'excess' should be set at no more than £35**

The interplay between the excess and minimum threshold should be viewed as the current proposal means that if I suffer a scam of £120, I will be refunded £85, yes if I suffer a scam of £99 I will be refunded nothing. Is there a better way to achieve the aims, for example, align at £100 or £50 for both?

- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

Whilst coming from a good place, this doesn't feel quite right. The requirements already provide vulnerable customers with greater protection than other consumers. Having a level playing field on the costs would seem fairer and simpler.

## **8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**

This seems a sensible approach to keep the overall administration costs down.

- **any threshold should be set at no more than £100**

This again fits with the customer caution element and will help protect the rest of the UK consumer base to some extent from the higher costs of the whole scheme.

- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

See previous comments on Q7 above.

## 9. Do you have comments on our proposal not to have a maximum threshold?

The Consumer Credit Act (CCA) does have a maximum threshold; however, APP frauds are very different to the CCA. Whilst meaning there is an unlimited liability here, it helps align the incentives for PSPs and prevent cliff edges, In practice, the banks' own limits will restrict the liability to a large extent.

## 10. Do you have comments on our proposals that:

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

This is a sensible approach and helps ensure that there are incentives on customers to check their payments after the fact. It helps ensure there are decent records to aid investigation too.

- **any time-limit should be set at no less than 13 months?**

The likely impact of the time limit is that relatives of investment fraud victims, who only become aware a long time after the fact. This might mean helping to identify victims proactively as frauds are highlighted.

A further consideration is to be given to post-payment customer messaging to highlight cases earlier and avoid the time-outs.

Greater data sharing of confirmed mules could be used by firms to highlight customers for proactive contact, but they may require additional incentives for firms to undertake this activity.

## 11. Do you have comments on our proposals that:

- **the sending PSP is responsible for reimbursing the consumer**

This makes the most sense as it allows the refund to be clearly separated from the PSP that is agreeing to their liability levels. It could mean that some PSPs are exposed to the risk of other PSPs not being able to repay the funds due. Correct levels of controls and insurance should be in place at all PSPs, especially at those without deep pockets.

- **reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

There is a very real risk of first-party abuse here, so it is key that there is a sensible way to allow PSPs to delay paying out in certain circumstances. See the response to Q2 regarding alignment with PSD2.

## 12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?

There is a very real risk of first-party abuse here, so it is key that there is a sensible way to allow PSPs to delay paying out in certain circumstances.

## 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

This is a sensible starting point, but some consideration of how the dialogue between the PSPs can be supported would be sensible. For example, will UK Finance be the conduit? How will firms be able to demonstrate to each other the level of controls that are in place and if they worked?

Will stats on levels of fraud in be available to help show, say a beneficiary bank has lax controls and should, therefore, have higher percentages? What evidence can a receiving bank show that there was literally nothing they could have done?

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

This is sensible as 50/50 won't be the right split in every case. Clearly, there needs to be a mechanism and rules set to underpin this. For example, the levels of controls at both banks, whether they worked effectively at that time, the level of mule accounts, real-time inbound profiling at ben banks, etc. Consideration for no-fault mules should be given too

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

There are several points regarding multi-generational scams. Whilst the principle that the beneficiary bank should have some liability to improve their incentives, is also clear that the first-generation mule account is undertaking money laundering and the payment(s) made are not in and of themselves APP frauds. Therefore, it is that PSP that needs the incentive to prevent onward transmission, being able to offset that onto the next PSP, may not assist in this effort.

The focus should be on actions to aid freezing and increase opportunities for repatriation of funds, rather than adding complexity and costs to further 50/50 sharing or 60/40 etc. Fast multi-generational tracing using

- The improved data sharing put in place by UK Banks
- Vocalink mule tracing capabilities,
- Additional global data sharing and tracing tools could also assist here bringing in law enforcement and international sharing/tracing.

We also need to consider the overlap of different types of fraud that flow through mule accounts, for example where a mule has funds from both unauthorised and authorised cases and the incentives for the beneficiary banks to use the funds to repatriate APP over unauthorised at the expense of the paying bank. Will Claytons Case (Wadsley & Penn, 2000, p. 345 ) be used to ensure this isn't abused?

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

50/50 should be the starting point and it follows that repatriation levels are split in line with refund levels. However, consideration should be given to a slight increase for beneficiary PSPs in order to encourage greater effort in freezing and recovery including crypto and overseas.

Global reporting and freezing can help here.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

Yes, this is as it should be. Consideration should be given to how to prevent a shift to Crypto and Swift payments. By engaging with other regulators, law enforcement, and industry to provide alignment and increase global data sharing to assist with international and Crypto for example E.g. sharing of known mule accounts/wallets and their identifying data.

See the previous answer to Question 3.

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

This aligns with Card Schemes, in that the regulator sets the framework and the implementation is with the Scheme or PSO.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

This should include similar positions as in cards schemes where those with excessive fraud/mule levels are subject to greater scrutiny and a potential shift in the 50/50 default allocation.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

No comment.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

No further comments to those made in Q14-17.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

This makes sense and can be used to help tweak the rules and guidance as it beds down.

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

The benefits of introducing a monitoring solution are:

- A clear understanding of which PSPs are making efforts, and which are not
- Ability to focus enforcement action appropriately
- Evidence to support amendments to any of the key parts of the proposals
- Evidence that it is improving APP prevention

Provided the overall costs are low and are not taking investment away from prevention, the benefits will outweigh the costs.

**24. Do you have views on the best option for short-term enforcement arrangements?**

Option C would be the best way forward as it provides the closest alignment to Cards Schemes that are in use today by the majority of FPS Participants.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

Provided the IAPs are on the hook to provide indirect PSPs with the toolkit to take the necessary steps, this should fall to the Indirect Participants.

Outbound payment profiling can sit with the indirect PSP or whatever service they use to do this.

Inbound profiling may prove harder but should still be possible.

Monitoring should be undertaken by PSO even for indirect participants and therefore IAP's should assist in providing relevant data. See answer to Q 22.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

If necessary, the direction should apply to indirect PSPs as these are regulated entities in their own right.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

There has been a clear externality for PSPs to avoid costs at onboarding and mule prevention, which this helps remove. Further incentives to invest in methods to freeze funds faster and seek repatriation of funds is key, as this helps removed funds from the organised crime groups (OCGs), limiting further harm, not just the harm to the initial victim.

The funds transferred for APP are money laundering and it is time to put a bigger dent in those funds that are lost to OCGs.

Whilst this is not only a UK phenomenon, it is key the UK take a lead to show what can be done as well as provide confidence in the UK payment systems.

**28. Do you have any other comments on the proposals in this consultation?**

No mention is given here about some scenarios, which could be some of the larger cases. Those such as a house purchase/sale and involves a third party such as a solicitor. There should be some clarity given here.

An example that has been seen previously is:

Solicitor is provided with a false request to change the account details for the sale proceeds, whether it was their email or the customer's email that was compromised, and pays these funds to a mule account.

In many cases, the solicitor's firm will not be covered by this regulation and so may not be able to seek a refund in order to then refund the consumer.

In such an instance the Solicitor has not acted on the customer's instruction and so they should be making the consumer right. They may be seen as the victim of an APP scam and if they meet the criteria, be refunded as such.

# CYBERA™

Whilst the PSR does not cover solicitors, we need to ensure that the regulation does not create gaps in coverage where possible. It should be put to the PSPs, similar to the 'on-us' argument that similar levels of controls should be in place across all customer bases, albeit reflecting the different levels of controls that larger businesses and corporates should have in place to protect themselves, E.g. solicitors having sensible conditions such as not accepting instructions in insecure manners such as email.

In a similar vein, this regulation is in large part about aligning the incentives of beneficiary PSPs to do more to stop their accounts from being used for money mule activity. As we have seen the current situation in the UK is poor given that most funds are transferred via UK domestic payments systems to UK domestic retail accounts. These are viewed as low-risk from an AML transaction monitoring point of view, and so we see the level of abuse shown in the APP numbers.

We should see the publication of mule account volumes at an industry level, with the regulators seeing the PSPs split. This should be for all types of money mule, whether it was APP or unauthorised fraud. Consideration is given to further analysis where practicable in terms of witting, unwitting etc.

The focus on beneficiary banks to do more to not open, and prevent fraud on mule accounts should be there irrespective of the type of victim, e.g., they should still have incentives even if the victim was a large corporate, but their bank received the funds in to a mule account. This should also be the case for unauthorised frauds.

Consider those that are very poor to have top up 'fines' that can be used to fund the vulnerable customer refunds etc.

Consideration, by the PSR & FCA, should be given to how to protect those innocents of being a money mule (from having their banking removed), when their account has been taken over by fraudsters, without their involvement or other edge cases, e.g., family member abuse of the account.

## About CYBERA

At CYBERA we're on a mission to stop money laundering and help protect customers from scams and other financial cybercrimes. We close gaps that allow cyber criminals to thrive by sharing actionable information in real-time with financial institutions, fintech, and crypto exchanges, and coordinating a global legal response to support victims of financial cybercrime. Backed by top US & Swiss Venture Capital Investors such as Founder Collective, Converge VC, NNV, Serpentine VC, and others. Headquartered in New York City, CYBERA has a remote work culture and real-life presence in Seattle, New York, Los Angeles, Zurich, London, Melbourne, Ukraine, and Dubai.

Our two initial solutions focus on providing victims with a quick response mechanism, and then a global watchlist that allows information to be securely shared with our clients across the financial system to ensure funds and accounts can be quickly flagged and addressed. This is a fully scalable, secure solution and addresses key regulatory concerns. We have already flagged over two thousand problematic accounts and wallets to authorities and helped to freeze hundreds of thousands of dollars, saving a multiple of that amount in further legal and reimbursement costs.

# CYBERA™

CYBERA was created to address these two clear gaps in the market – logging and sharing victim reports and creating a global watchlist for problematic accounts. The international scope and complexity of these scams often link financial institutions, private businesses, technology companies, and international, federal, state, and local law enforcement agencies, so enforcement and assigning responsibility have become very difficult.

Find out more about how CYBERA can help protect your institution and its customers from financial cybercrime at [www.cybera.io](http://www.cybera.io).

# Electronic Money Association





**Electronic Money Association**  
Crescent House  
5 The Crescent  
Surbiton, Surrey  
KT6 4BN  
United Kingdom  
Telephone: +44 (0) 20 8399 2066  
[www.e-ma.org](http://www.e-ma.org)

APP scams team  
Payment Systems Regulator  
12 Endeavour Square  
London E20 1JN

By email: [appscams@psr.org.uk](mailto:appscams@psr.org.uk)

25 November 2022

Dear [REDACTED]

**Re: PSR CP21/10 Authorised Push Payment (APP) Scams Consultation Paper**

The EMA is the UK trade body representing electronic money issuers and payment service providers. Our members include leading payments and e-commerce businesses worldwide, providing online payments, card-based products, electronic vouchers, and mobile payment instruments. A list of current EMA members is provided at the end of this document for reference.

We welcome the opportunity to comment on the PSR's proposals for reimbursement of APP scams. We consider that the impact of these proposals may be significant, with a particularly acute impact on smaller and payment-specialist PSPs, so we very much hope the PSR will be able to take our views into consideration.

Yours sincerely,

[REDACTED]

Chief Executive Officer  
Electronic Money Association

[REDACTED]

## EMA response:

---

### Overarching comments

We welcome the opportunity to respond to the PSR CP 22/4 on APP Scams and the proposals to require PSPs to reimburse victims of APP scams. We are supportive of the PSR's objective to ensure a consistent approach to reimbursement and ensure that firms are doing everything they reasonably can to prevent customers from falling victim to APP scams. The prevention of APP scams and protection of customers are key priorities for all segments of the payments industry.

Our response addresses the questions in the consultation below. However before addressing the detailed questions, we wish to re-state our view on the overarching principle and impact of mandatory reimbursement, and concern about the impact of these proposals. Placing full liability on PSPs for losses incurred by victims of APPs is inappropriate for the following reasons:

- (i) it incentivises fraud by providing easily accessible compensation and encourages criminals from elsewhere to target the UK;
- (ii) it is contrary to principles of English law and to the expectations of natural justice, where compensation would be expected to flow from fault and where liability is generally incurred through fault;
- (iii) it will be detrimental to the operating of the Faster Payments Scheme (FPS); and
- (iv) it creates a disincentive for third party actors who have the ability to reduce such risk – such as the accountants or dating website providers, to act to reduce the risk; and
- (v) it leaves the underlying fraud problem, a law enforcement and government policy matter, unaddressed.

Applying mandatory reimbursement through the FPS rules removes the ability to set a standard of care for consumers, and moves more directly towards a complete underwriting of fraud by the PSP industry. It is also not in the interests of users, whether consumers or businesses, to address fraud risk through underwriting; it simply shifts the cost of the fraud back to users who will have to pay through higher fees, and fails to address the vulnerabilities in the ecosystem that give rise to the fraud in the first place.

The EMA previously recommended that the PSR take a number of steps prior to implementing any measures: (1) carry out a consultation on the underlying assumptions behind mandatory reimbursement, and (2) conduct a proper impact assessment on the effects of mandatory reimbursement. The measures proposed may have detrimental consequences (both economic and competition consequences) on the payments market.

As the PSR's objectives are to promote the interests of all the businesses that use the payment systems, as well as ensure effective competition in the markets for payment systems and services, and to promote the development of and innovation in payment systems, we consider it to be the role of the PSR to ensure their policies will not damage the market for which they are responsible.

The EMA recommended that such a consultation explore the desirability of requiring PSPs and specialist PSPs in particular, to underwrite wider community fraud where PSPs have met their duty of care, and the impact on incentives for PSPs and other stakeholders to reduce the incidence of such APP scams. The consultation should consider the merits of penalising PSPs that have met their standard of care, the distinctions and relative contributions of direct and indirect participants, and the disproportionate impact that FPS rules may have on new specialist and innovative PSPs.

We note that, to date, neither of these actions seem to have been conducted, or even considered.

We strongly support the House of Lord's Fraud Act 2006 and Digital Fraud Committee's recommendations<sup>1</sup> that the PSR and Government further explore the long, and short term, risks of a blanket reimbursement policy and pursue a solution that achieves a level playing field for all customers and PSPs. As the report concludes "***the last link in the fraud chain ...cannot be expected to foot the fraud bill alone***".

## Consultation questions

### 1. Do you have views on the impact of our proposals on consumers?

Yes, the PSR's proposals will change consumers' behaviour.

As set out in the [EMA response to PSR CP 21/10 on APP scams](#), we consider that the proposals will lead to consumers taking less care when authorising a payment.

We believe that reimbursement is only one dimension of consumer protection and that a wholesale mandatory reimbursement policy may introduce risks that consumers lack the incentive to guard against the possibility of fraud, and may even lead to new opportunities for reimbursement fraud emerging. We note that the Financial Secretary to the Treasury when giving evidence to the Treasury Committee in October 2022, told MPs that the PSR should "*come forward and engage with industry because there is a moral*

---

<sup>1</sup> <https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf>

*hazard piece and we have to get that right balance*<sup>2</sup>, and further that the recent House of Lord's report<sup>1</sup> endorses this point and recommends that these risks are fully explored before finalising the reimbursement policy.

However so far, the Payment Systems Regulator has provided **no evidence** that the reimbursement requirement will not result in customers taking less care, and there does not appear to be any evidence that the UK will not be viewed as an easy target for further fraudulent activity. The Payment Systems Regulator's recent consultation CP 21/10 states: *We have seen no compelling evidence that mandatory reimbursement will cause customers to be careless with their payments. In fact, PSPs that have introduced blanket victim reimbursement policies have told us that this did not result in any increase in claims* [paragraph 3.45; CP21.10]

Since then, it does not appear that the PSR has conducted any research in this area. As a competition regulator, such research should have been done as a matter of course, and would provide a much stronger basis on which the PSR might substantiate such a significant change in the law.

Instead, reliance has been placed on anecdotal evidence - "Payment Service Providers (PSPs) have told us". The assertion that reimbursement will not inform the customer's behaviour has only been assessed with respect to customers of PSPs who have a blanket reimbursement policy. There is no evidence that this behaviour is representative of customers in general, or in circumstances where it is widely publicised at national level that all scam payments will be refunded. The customers of the PSP that had the blanket reimbursement policy may not have even known about the policy – the blanket reimbursement policy likely did not inform their behaviour whatsoever.

The reimbursement requirement will likely increase the (already disproportionately high) numbers of fraudsters specifically targeting the UK over other countries for easy money. EMA members operating at a global level have provided evidence that this trend is already occurring. Despite repeated recommendations to investigate these concerns, the PSR has not provided any evidence that this will not happen.

We strongly urge the PSR to gather sufficient evidence on the likely impact of blanket reimbursement on consumer behaviour so that proportionate and balanced measures for reimbursement can be devised.

## **2. Do you have views on the impact of our proposals on PSPs?**

Yes, we are concerned with the impact of mandatory reimbursement on smaller and non-bank PSPs' commercial viability.

### ***Cost of reimbursement:***

---

<sup>2</sup> [Oral evidence taken before the Treasury Committee on 11 October 2022 \(Session 2022–23\) – Andrew Griffin \(Q75\)](#)

The PSR state: *We have not considered the direct costs of PSPs increasing their rates of reimbursement as being a relevant cost for this cost benefit analysis. We have not taken the approach of directly balancing the costs of increased reimbursement that PSPs will face against the benefits of increased reimbursement that victims will receive. That approach would simply find a large cost on one side cancelled out by the same scale of benefit on the other.* [2.40]

We recognize that mandatory reimbursement measures are intended to incentivize PSPs to have stronger anti-fraud measures in place. However, Members of the EMA are principally specialist payment providers who are proscribed from lending the funds of users, and therefore are restricted in the revenue that they generate to transaction-related income streams. The impact of any increase in cost is felt much more by these PSPs (i.e. non-bank PSPs), as they do not benefit from the cross-subsidisation afforded by banks. Whilst they may be able to put in place technical and operational measures that reduce the risk that their customers might suffer from APP scams, it is much harder for them to absorb the cost of an APP scam, or the cost increase of FPS scheme fees.

As an example, if the total revenue generated by a PSP was in the region of 1% of the value of a transaction (which is generally at the high end), from which its cost of doing business must be extracted. Hence it would have to process at least 100 equivalent size transaction to recover the loss on a single claim of fraud. Once the costs of doing business are taken into account, this is likely to increase to perhaps 1000 transactions.

The PSR have further said: *Respondents to our November consultation highlighted the potential cost implications of our reimbursement proposals for small PSPs and for certain business models. If reimbursement costs were large enough for some small PSPs, this could, in principle, have prudential implications – for instance, where firms face the cost of reimbursement and may not have the capacity to invest in fraud detection and prevention to combat the problem effectively. As set out in chapter 3, we continue to work with the FCA and the Prudential Regulation Authority (PRA) on how risks to individual small PSPs would be monitored and managed.* [2.65]

We strongly urge the PSR to reconsider the assessment of direct PSP costs of implementing the reimbursement proposals in light of the potential impact on indirect FPS participants, and small and non-bank PSPs.

**Increased costs for use of the Faster Payments Scheme:** Under the PSR's proposals Pay.UK will be directed to facilitate reimbursement. They will be required to put in place a cost allocation mechanism, a dispute resolution mechanism and a real time transaction monitoring mechanism. Putting in place all of these mechanisms and systems will require significant initial and on-going investment by Pay.UK.

Pay.UK will have to seek to recover these costs from Scheme participants. Accordingly, it is likely that all PSPs will pay more for participating in the Faster Payments Scheme (directly, or indirectly) and making Faster Payments.

The PSR has said: *Our proposed policy is likely to lead to PSPs incurring additional costs that they do not face at present, although we have not been able to quantify these.* [2.52]

We are concerned that if the increase in Faster Payment cost is not adequately quantified it may create a net negative effect where competition is stifled as only the largest providers in the UK will be able to participate in the Scheme.

We **urge the PSR to fully quantify the cost** to Pay.UK of managing the reimbursement scheme **before publishing the draft Direction** in order to measure the impact on the cost of Faster Payments scheme and the wider impact this may have.

Increased costs for use of the Faster Payments Scheme may result in scheme participants (i.e. generally banks) increasing the costs of banking services overall which will affect consumers and businesses alike.

Many EMA members are customers of banks; payments and e-money businesses rely on banking partners to provide safeguarding accounts, which are a regulatory requirement. These firms will face an increase in the cost of doing business. EMIs are already subject to de-risking, and banking services are at a premium – we are concerned that the PSR’s proposals are going to exacerbate this situation.

***Impact on Payment initiation service providers (“PISPs”) will be disproportionate:***

We note that the PSR’s analysis has not considered the downstream impact of the reimbursement measures on providers within the payment chain; most notably payment initiation providers (PISPs).

PSPs may have an incentive to become more risk averse to PISP initiated transactions (open banking payments) because they may have to reimburse a fraud without any recourse to the PISP who initiated the transaction. Unlike other PSPs, there is no feasible way to flow down liability to the PISP for reimbursement because there may not be a contract in place, and/or the PISP may not be in the flow of funds (and therefore have limited capacity to offset increased fraud liabilities that may occur). The Payment Services Regulations 2017 do not require the PISP to have a contract in place, nor for the PISP to be in the flow of funds.

Fraud controls designed to safeguard Faster Payments transactions against APP fraud, such as transaction limits, are already impacting the success of PIS because the controls applied do not reflect the risk profile of open banking payments i.e. usually to a known payee who is under contract with the FCA-authorized PISP. As we discuss in our response to Q9, the uncapped liability that the PSR propose for PSPs may exacerbate this issue even further, as PSPs may be even less willing to extend transactions limits for Faster Payment transactions.

We cannot reconcile the likely effect of the reimbursement proposals on the commercial viability of the PISP business model, with the PSR’s wider objective that account payments should become a viable alternative to card payments in the UK market. PISPs are at the heart of the PSR’s intention to drive competition in the payments market, yet the increased cost of Faster Payments, coupled with the cost of reimbursement, is likely to undermine the whole sector. We have set out our views in more detail in our earlier response to the PSR CP



As a result, we urge the PSR to fully consider the effect of mandatory reimbursement on the nascent open banking PISP market, and the wider competitive objectives of the UK payments strategy, before finalizing the proposals.

### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

#### Payers

Yes, reimbursement requirements should extend to customers that are consumers only. Micro-enterprises and charities should not be within scope of the reimbursement requirements.

The PSR has included micro-enterprises and charities within scope of the proposed reimbursement requirements because the PSR is applying the same scope as Part 6 and 7 of the Payment Services Regulations; however, this is unsubstantiated. The reimbursement requirements have little to do with payments regulation; they are, instead, a consumer protection measure and, other than requiring payment service providers to underwrite fraud, have little to do with payments at all.

To explain, the fraud takes place on a separate platform, for example, a dating website. Correspondence is exchanged between the fraudster and the victim on that separate platform; this could be over a long time. Payment service providers are only involved at the very last stage of the fraud when the victim uses their payment account to transfer funds to the fraudster. If the fraudster did not demand money but, instead, demanded the victim sign over the deeds to their house, it would not follow that a reimbursement requirement in this case would be classed as real estate / real property regulation. Accordingly it is unclear on what basis the scope of core payments regulation should be applied to the reimbursement requirements.

An additional unintended consequence of extending the scope to include micro-enterprises and small charities is that their ability to obtain payment services or specific products would decrease. Some PSP business models are primarily developed for, and utilised by, corporate customers, including micro businesses, which benefit from access to such services. However, under these proposals microbusinesses will only remain a relatively small part of overall revenue, whilst representing an increased risk and cost profile to the payments firm, increasing the risk that they will be excluded from such product offerings.

To summarise, the scope should be limited to consumers only.

#### Indirect participants

Indirect participants have no control over scheme rules and otherwise have no influence over them; indirect participants are merely bound by the contract they have in place with the direct participant. Accordingly, the governance of Pay.UK would have to change in order to allow for indirect participants to have a say in terms of scheme rules.

### APP scams in scope

We note that the definition of APP fraud is ambiguous in the consultation.

The APP scams in scope should include only those scams that involve social engineering. Scams that involve family members defrauding one another or other situations where the fraudster is otherwise known to the victim should not be included within scope. Otherwise the risk is that PSPs become involved in family disputes etc. which are squarely a civil matter and not related to the PSR's objectives.

In multi-generational scams, where the fraudster convinces the victim to move the funds more than once, the final payment to the fraudster must be the only payment that qualifies for reimbursement, and not any interim payments between the victim's own accounts, or accounts over which they hold control.

#### **4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**

Yes, this is essential.

- **to use gross negligence as the consumer caution exception**

Gross negligence is too low a standard; it is considerably below the standard that persons are required to conduct themselves in the course of everyday life. In the course of everyday life in order to avoid being held liable for loss sustained by another, a person must, generally speaking, conduct themselves to the standard of a reasonably prudent person acting in similar circumstances.

### Regulation 77(3) of the Payment Services Regulations 2017

We have established in the response to question three that the reimbursement requirement proposed by the PSR is not a payments requirement – it is a consumer protection measure that requires entities that provide payment services to underwrite fraud. Accordingly, references to the Payment Services Regulations 2017 are not persuasive and should not be used as a justification for using gross negligence as a standard.

### CRM Code

Whilst the CRM Code is a comparable mechanism to the reimbursement requirements proposed by the PSR, the CRM Code also includes several other exceptions to reimbursement, which are not present here. For example, the customer ignored effective warnings. Accordingly, referencing the CRM Code as using gross negligence as a standard is only justified if the PSR were to include all of the other exceptions to reimbursement that are present in the CRM Code.

### Impact on PSP incentives



We understand that the PSR's objective in placing liability on PSPs is the hope that this may increase the incentive on PSPs to reduce the instance of APP scams. However, if the only consumer exception is an undefined threshold of gross negligence, the proposed approach will penalise PSPs that have met their standard of care. If PSPs are unable to take any actions to reduce their liability in individual cases, their incentive – or even ability - to address such fraud - apart from refusing to process transactions over a certain value or to certain jurisdictions – is not apparent.

- **not to provide additional guidance on gross negligence?**

This will lead to not only uncertainty but disputes over the standard of conduct.

### **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

Even for vulnerable customers the standard of gross negligence is too low. As stated in our response to question 4, it departs too far from the standard of conduct a person is required to hold themselves to in everyday life (i.e. the reasonable person standard). The next standard below gross negligence is criminal.

Accordingly, the exception of gross negligence must apply to all customers including vulnerable customers.

### **6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

The FCA's definition of vulnerable customer (as set out in paragraph 2.5 of FG21-1) is too broad to apply to rules relating to APP-scam reimbursement. It is too broad in general; however, it is certainly too broad for rules as onerous as those proposed by the PSR in this consultation.

Paragraph 2.19 of FG21-1 sets out some examples of harm and disadvantage that firms should be alert to:

- heightened stress levels due to difficult, or different, personal circumstances
- increasing time pressures due to additional responsibilities
- increasing pre-occupation ('brain is elsewhere') limiting their ability to manage
- lack of perspective especially when experiencing something for the first time, not fully understanding the broader implications; being unable to make comparisons, or see the 'bigger picture'
- changing attitudes towards taking risks; people often become more 'reckless' and/or careless when under stress.

Under the vulnerable customer guidance [FG21-1], these examples of harm and disadvantage mean that the customer should be subject to the heightened standard of care as set out in the vulnerable customer guidance.

Under the PSR's proposed APP-scam reimbursement rules, these examples of harm and disadvantage operate as justifications for a customer acting grossly negligent.

The vulnerable customer guidance and APP-scam reimbursement rules are completely different contexts; accordingly, the PSR should define vulnerability in objective terms leaving no room for dispute.

#### **7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**

Yes, firms should be permitted to apply an excess.

- **any 'excess' should be set at no more than £35**

We disagree with GBP 35 excess. The excess should be at least GBP 100. The alignment with the unauthorised transactions rules in the Payment Services Regulations 2017 is not relevant; in our response to Q3, we have established that the PSR's proposed reimbursement rules are not payment rules – they are instead a consumer protection measure and, other than requiring payment service providers to underwrite fraud, have little to do with payments at all. It is unclear why an alignment with the Payment Services Regulations 2017 is necessary. Instead, comparisons should be made with home or motor insurance policies (as the PSR proposals are closer in nature to an insurance policy against social engineering fraud), which usually carry a minimum excess of over £100, and in many cases several £100s.

Finally, we would also question whether, even with a raised excess limit, consumers will be genuinely incentivised to exercise greater caution when initiating payments in many APP scam scenarios. As noted in our response to Q1, the PSR has limited evidence on the impact of mandatory reimbursement on consumer behaviour. We again urge the PSR to gather and assess robust evidence of the impact of reimbursement on consumer behaviour.

- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

No, on the basis that PSPs still incur costs when providing services to customers even where the customer is considered vulnerable. The PSR has stated above that the excess will be "modest" in any case.

#### **8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**

Yes, this is essential.

- **any threshold should be set at no more than £100**

No, the minimum threshold should be raised to between GBP 500 and GBP 1000.

We understand the PSR's rationale for including a minimum threshold is to account for the basic operational costs a PSP will incur when facilitating reimbursement. We consider that the basic operational costs that a PSP incurs from reimbursing a customer will exceed GBP 100. In order to facilitate reimbursement, PSPs will have to, for example, deploy a global training programme in order to train staff on the PSR's new measures. This training will not be limited to the staff members handling the claim but will also include, for example, training for customer support representatives. We therefore consider the minimum threshold should be raised to between GBP 500 and GBP 1000 to account for such costs.

**• PSPs should be able to exempt vulnerable consumers from any threshold they set?**

No, on the basis that PSPs still incur costs when providing services to customers even where the customer is considered vulnerable.

**9. Do you have comments on our proposal not to have a maximum threshold?**

We believe this is unreasonable and not commercially viable. No business can accept uncapped liability; especially when the standard of conduct is so uncertain.

The PSR state: *We would expect PSPs typically to have the strongest safeguards in place for the largest payments. Given this, if a PSP allowed a very large payment to proceed, it should be liable if the payment is an APP scam (subject to exceptions for first party fraud and gross negligence) [4.47]*

Please note that a maximum threshold may not be engaged if the customer were to make "a very large payment" – it may be engaged when the customer makes many payments of small amounts over time.

The PSR further note: *In practice most PSPs' Faster Payments transactions limits are very well below £1 million. [4.47].* Therefore, a liability cap of "very well below GBP 1 million" should be reasonable.

The maximum threshold should align with section 75 of the Consumer Credit Act 1975 (i.e. GBP 30,000). As the PSR have already established parallels with Section 75, there is precedent for capped liability at this level – unlimited liability is unsubstantiated.

Our proposed GBP 30,000 cap aligning with section 75 rights under the Consumer Credit Act 1975 should be the cap applied to the entire claim and not merely one payment. This is because fraudsters will become aware of any per transaction cap and tailor their practises to convince the customer to make several payments below the threshold rather than one large payment that will exceed it. The PSR should therefore apply an overall cap to an entire claim to ensure the PSR's proposals do not further enhance fraud.

**10. Do you have comments on our proposals that:**

██████████

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

Sending PSPs should definitely be allowed to set a time limit for claims of reimbursement. This should be a basic tenet for any prudent business.

- **any time-limit should be set at no less than 13 months?**

#### Time limit is too long

The time limit should be lessened to six months. The 13-month time limit in the PSR for the customer to notify the PSP of an unauthorised transaction is so long because the customer is not involved in the unauthorised transaction and may therefore not know about it.

An APP scam is completely different in nature to an unauthorised transaction in that it directly involves the customer. The customer is aware the transaction has taken place; they gave their authorisation for the payment order to be executed.

Whilst both types of fraud, unauthorised transactions are not comparable to APP scams (i.e. authorised payments). Accordingly, there is no basis to use the same lengthy time period.

In any case, consumers usually report a scam or fraud within days if not hours of becoming a victim.

#### How the time period is defined is incorrect

The PSR has proposed “*a time-limit of no less than 13 months from the final payment involved in the APP scam*”; however, this means that numerous payments could take place over the course of years and the customer notifies the PSP that they have in fact been scammed within 13 months of making the final (of many) payments.

All of the payments that the PSR expects the PSP to reimburse must take place within the time limit. PSPs do not agree to underwriting fraud that may have been perpetuated over a series of years. Even the crime of the fraud itself is subject to a statute of limitations.

### **11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**

No specific comments.

- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We do not agree with the “no later than 48 hours after a claim is made” timeline. This is far too short a time for a PSP to properly investigate the matter. A fraudster may have spent months or even years perpetrating the fraud. For the most sophisticated of scams, the fraudster may have spent a considerable amount of time laying the foundation in

order to socially engineer the victim; it may not be a simple matter that can be dealt with in 48 hours.

Further, 48 hours is two working days which is seven hours times two – this is not sufficient time to fully investigate a claim.

The timeframe also needs take into account the customer's willingness to cooperate. In other words, the clock must not start ticking until the customer has provided every piece of information that PSP has requested in order to investigate the claim.

Permitting a PSP was given all relevant information by the customer in order for the PSP to thoroughly investigate, and, depending on the sophistication of the fraud at hand, a realistic timeframe to investigate the claim and be in a position to make an informed decision as to whether it is a valid claim is no less than one week. 48 hours will put pressure on staff to rush investigations and decisions which will lead to inaccuracy. In particular this will affect smaller PSPs that are unable to provide staffing to cover such activity over the weekend.

We propose the PSR extend the time limit to reimburse to five working days. Please note that the time limit must be expressed in 'working days' as to not necessitate smaller PSPs allocating resource during the course of a weekend, as discussed above.

Please further note that the time limit should be expressed in a 'stop / start' clock. To demonstrate, when the customer formally submits a claim, the clock starts. The clock then stops until the customer provides all information requested by the PSP; the customer must not be able to 'buy time' or wait out the five-day time limit by not cooperating or otherwise not providing information.

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

We suggest a standard of "reasonable suspicion based on articulatable facts".

Please note that whether it is considered evidence of gross negligence or fraud (or not), PSPs must be permitted to extend the time for investigation indefinitely in cases where the customer (i) refuses to provide the PSP with any information requested by the PSP relating to the claim, (ii) tries to mislead the PSP, or (iii) does not otherwise fully cooperate with the PSP following a claim.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

We understand the rationale behind the 50:50 default allocation of reimbursement costs, as a relatively simple way to attribute liability between PSPs. However we are aware of at least one alternative being proposed, and would invite the PSR to consider such alternatives before adopting the 50:50 liability option.

For example one approach that would allow PSPs to reduce their fraud liability and better manage their risk would be to automatically allocate liability based on historical APP scam related data. The APP scam data that PSPs will be required to report to the PSR under Measure 1 could be used to score PSPs for fraud, and the liability ratio between sending and receiving PSP be applied in line with their relative APP scam risk score. This would provide a clear liability allocation, and incentivise PSPs to reduce their risk score.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

The allocation criteria must take into account the relative bargaining power of the PSPs. Large banks have significant resources – they will always be in a position to challenge the default 50/50 position and force smaller PSPs to dispute resolution. Smaller PSPs will not have the resources to continuously keep defending these challenges.

In addition, smaller PSPs may be relying on the larger bank or PSPs for other services (banking services, safeguarding, payment processing, etc) with whom they are disputing a reimbursement allocation. The effect on the commercial relationship could be affected and result in unintended consequences for the smaller PSP, such as being de-risked.

Accordingly, the PSR must direct Pay.UK to take into account the relative size and bargaining power of the PSPs in the allocation criteria.

Further, the allocation criteria should empower the receiving PSPs to challenge a classification of a given transaction as fraudulent - prior to the repayment to the victim – and to allow the receiving PSP to provide evidence to the sending PSP that the payment was legitimate. The sending PSP has no insight into the fraudster's use of payment services and should therefore not be permitted to unilaterally classify a transaction as fraudulent (thereby levying 50% of the liability on the receiving PSP).

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

The final payment to the fraudster must be the only payment that qualifies for reimbursement.

The PSR states:

*The 'end to end' journey of some APP scams involves more than one payment. In one example, the fraudster may 'socially engineer' the consumer to transfer money from their bank account to an account they hold at a different PSP (or perhaps persuade them to open a new account in their own name). The fraudster then persuades the consumer to transfer the money from that account into the account under the fraudster's control. [5.10]*

*In some cases that second payment may be a transfer using Faster Payments to an account held at a PSP. In other cases, the second payment may be to a different type of*



*account, such as a crypto wallet, which does not happen over Faster Payments, but uses another, for example, a card or a crypto-based, payment system. [5.11]*

In the example given by the PSR, the first payment from one account held by the customer to another account (not yet to the fraudster but to another account held by the customer) must not qualify for reimbursement. The customer, by transferring funds to themselves, has not sustained any loss at this stage and therefore the PSP cannot incur liability.

Using the same example given by the PSR, the customer then makes a second payment to a crypto wallet. The PSR expressly states this transaction does not take place over Faster Payments.

Accordingly, this second transaction should not be within scope of the reimbursement rules proposed by the PSR. The scope of these proposed rules is confined to Faster Payments.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

The PSPs must be made whole for the loss they have suffered from reimbursing the customer.

The PSR state: *We propose that, as a default, repatriated funds should be shared 50:50 between the sending and receiving PSPs to defray their costs of liability for reimbursement. [5.16]*

This makes sense to the extent that liability was apportioned 50/50 in the first instance.

The PSR further note: *Any repatriated funds remaining after the PSPs have fully defrayed their reimbursement costs would go to the victim. [5.16]*

Please note that even if repatriated funds do exceed reimbursement costs (although it is unclear how this could be the case), the customer must not be able to profit from the scam. The funds paid to the customer by the PSP must be no more than the loss the customer sustained as a result of the scam.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

The PSR intends to levy reimbursement costs on both direct and indirect participants. However, indirect participants do not have any control over scheme rules, they are subject to the terms of the contract they have in place with the direct participant.

If the PSR intend indirect participants bear the same liability as direct participants, indirect participants must be given the same rights as direct participants in terms of influence scheme rules that relate to APP scams. Anything less than complete equality between direct participants and indirect participants in terms of their ability to influence scheme rules would be unfair as direct participants and indirect participants bear the same liability under the rules.

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

As we have discussed above, the PSR must establish the cost of the reimbursement proposals before embarking on it.

If Pay.UK are going to be directed to facilitate reimbursement. They are going to be required to put in place a cost allocation mechanism, a dispute resolution mechanism and a real time transaction monitoring mechanism.

Putting in place all of these mechanisms and systems is going to cost Pay.UK significantly and these costs will be passed on to PSPs.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

The rules are not appropriate generally, and, as a result, the minimum initial set of rules are not appropriate. The rules are uncertain and ambiguous on important points. For example, the standard of conduct required by both the customer and the PSP, in different circumstances, is not settled (for example, gross negligence, or the standard of evidence a PSP must produce to be permitted to take extra time to investigate). The scheme cannot implement rules based on PSR requirements that need to be clarified.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

No specific comments.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

There is not enough detail in the consultation to answer this question. The dispute resolution process appears to be cumbersome and onerous. Would disputing a 50/50 allocation under the proposed dispute resolution arrangements incur a fee? If so, what is it? Are there options for a PSP to reimburse the customer unilaterally and not engage in dispute resolution?

In relation to the “set of standards for preventing and detecting APP scams” and that the PSR expects “future arrangements to build on the achievements of the CRM Code”, we consider that if PSPs are liable for reimbursement, then PSPs should be free to determine their own standard of conduct in terms of detecting and preventing APP scams. The PSP is the party bearing all risk of loss; it should be able to mitigate this risk on its own terms.



**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

Reporting seems unnecessarily onerous. If PSPs were not complying with scheme rules and not reimbursing customers, would this not elicit complaints to higher authorities such as the FOS or a court (e.g. Philips v Barclays)?

**23. Do you have views on the costs and benefits of Pay.UK implementing a real time compliance monitoring system and when it could be introduced?**

The PSR must establish how much this monitoring system will cost Pay.UK as this cost will be passed on to PSPs. In particular it is likely to have a disproportionate impact on payments-specialist PSPs and smaller PSPs.

The PSR have said: *Respondents to our November consultation highlighted the potential cost implications of our reimbursement proposals for small PSPs and for certain business models. If reimbursement costs were large enough for some small PSPs, this could, in principle, have prudential implications – for instance, where firms face the cost of reimbursement and may not have the capacity to invest in fraud detection and prevention to combat the problem effectively. As set out in chapter 3, we continue to work with the FCA and the Prudential Regulation Authority (PRA) on how **risks to individual small PSPs** would be monitored and managed. [2.65]*

As discussed in our response to Q2, it is imperative that the PSR conduct a full cost analysis of Pay.UK implementing the reimbursement measures.

**24. Do you have views on the best option for short-term enforcement arrangements?**

The EMA considers Option A - with short-term enforcement managed by Pay.UK, and avoiding the PSR's intervention - is the correct approach for short-term enforcement.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

Indirect participants have no control over scheme rules and otherwise have no influence over them; indirect participants are merely bound by the contract they have in place with the direct participant.

Accordingly, the governance of Pay.UK would have to change in order to allow for indirect participants to have a say in terms of scheme rules.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

If it were necessary for the PSR to give such a directive, a direction on indirect participants rather than indirect access providers would be more appropriate in the circumstances.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

We consider that the cost benefit analysis is unsubstantiated as it does not contain analysis of any costs (as discussed above).

Section 104(3) of FSBRA requires the PSR to provide a “cost benefit analysis” with draft proposed requirements.

Section 104(7) provides:

*(7) For the purposes of this section a “cost benefit analysis” is—*

*(a) an analysis of the costs together with an analysis of the benefits that will arise—*

*(i) if the proposed requirement is imposed, or*

*(ii) if subsection (6) applies, from the requirement imposed, and*

*(b) subject to subsection (8), an estimate of those costs and of those benefits.*

The PSR have not provided what is described in section 104(7) as a “cost benefit analysis” because there are no costs set out in Annex 2. There are some examples figures which do not appear to reach the threshold.

Section 104 (8) of FSBRA provides:

*(8) If, in the opinion of the Payment Systems Regulator—*

*(a) the costs or benefits referred to in subsection (7) cannot reasonably be estimated, or*

*(b) it is not reasonably practicable to produce an estimate, the cost benefit analysis need not estimate them, but must include a statement of the Payment Systems Regulator’s opinion and an explanation of it.*

We consider that the cost to Pay.UK of facilitating the reimbursement rules (which will then be passed on to PSPs) can reasonably be estimated; however, the PSR have said in Annex 2:

- *We cannot quantify the likely scale of the costs to PSPs [2.49]*
- *Our proposed policy is likely to lead to PSPs incurring additional costs that they do not face at present, although we have not been able to quantify these; and [2.52]*
- *We have not sought to quantify the potential costs, if any, of any such migration [2.64]*

However the CBA does not appear to provide a rationale for why the quantification of these costs has not been sought.

We consider that the document published at Annex 2 is lacking in detail such that it does not discharge the PSR's obligation in section 104(3) of FSBRA to provide a cost analysis.

**28. Do you have any other comments on the proposals in this consultation?**

We urge the PSR to not only quantify the costs of their proposals as set out above in the response to question 27, but to also analyse in more detail the cost to the faster payment system and the potential for delayed and rejected payments due to the need to investigate potential scam payments. We do not consider the effect of delayed and / or rejected payments on both PSPs and consumers has been sufficiently analysed in the consultation; we therefore that the PSR provide this analysis.

## Members of the EMA, as of November 2022

[AAVE LIMITED](#)  
[Account Technologies](#)  
[Airbnb Inc](#)  
[Airwallex \(UK\) Limited](#)  
[Allegro Group](#)  
[Amazon](#)  
[American Express](#)  
[ArcaPay Ltd](#)  
[Azimo Limited](#)  
[Banked](#)  
[Bitstamp](#)  
[BlaBla Connect UK Ltd](#)  
[Blackhawk Network Ltd](#)  
[Boku Inc](#)  
[Booking Holdings Financial Services International Limited](#)  
[CashFlows](#)  
[Checkout Ltd](#)  
[Circle](#)  
[Citadel Commerce UK Ltd](#)  
[Contis](#)  
[Corner Banca SA](#)  
[Crypto.com](#)  
[Curve](#)  
[eBay Sarl](#)  
[ECOMMPAY Limited](#)  
[Em@ney Plc](#)  
[emerchantpay Group Ltd](#)  
[Etsy Ireland UC](#)  
[Euronet Worldwide Inc](#)  
[Facebook Payments International Ltd](#)  
[Financial House Limited](#)  
[First Rate Exchange Services](#)  
[FIS](#)  
[Flex-e-card](#)  
[Flywire](#)  
[Gemini](#)  
[Global Currency Exchange Network Limited](#)  
[Globepay Limited](#)  
[GoCardless Ltd](#)  
[Google Payment Ltd](#)  
[HUBUC](#)  
[IDT Financial Services Limited](#)  
[Imagor SA](#)  
[Ixaris Systems Ltd](#)  
[MANGOPAY](#)  
[Modulr FS Europe Limited](#)  
[MONAVATE](#)  
[Moneyhub Financial Technology Ltd](#)  
[Moorwand](#)  
[MuchBetter](#)  
[myPOS Payments Ltd](#)  
[NOELSE PAY](#)  
[NoFrixion Ltd](#)  
[Nuvei Financial Services Ltd](#)  
[OFX](#)  
[OKTO](#)  
[One Money Mail Ltd](#)  
[OpenPayd](#)  
[Own.Solutions](#)  
[Park Card Services Limited](#)  
[Paymentsense Limited](#)  
[Paynt](#)  
[Payoneer Europe Limited](#)  
[PayPal Europe Ltd](#)  
[Paysafe Group](#)  
[Plaid](#)  
[PPRO Financial Ltd](#)  
[PPS](#)  
[Ramp Swaps Ltd](#)  
[Remitly](#)  
[Revolut](#)  
[Ripple](#)  
[Sable International FX Limited](#)  
[Securiclick Limited](#)  
[Skrill Limited](#)  
[Soldo Financial Services Ireland DAC](#)  
[Square](#)  
[Stripe](#)  
[SumUp Limited](#)  
[Syspay Ltd](#)  
[Transact Payments Limited](#)  
[TransferMate Global Payments](#)  
[TrueLayer Limited](#)  
[Trustly Group AB](#)  
[Uber BV](#)  
[VallettaPay](#)  
[Vitesse PSP Ltd](#)  
[Viva Payments SA](#)  
[Weavr Limited](#)  
[WEX Europe UK Limited](#)  
[Wirex Limited](#)  
[Wise](#)  
[WorldFirst](#)  
[WorldRemit LTD](#)  
[Yapily Ltd](#)

Experian

## Experian response to PSR consultation CP22/4: Authorised push payment (APP) scams: Requiring reimbursement

We welcome the opportunity to respond to PSR's Authorised Push Payment (APP) Fraud Reimbursement consultation.

Experian operates as a Fraud Prevention Agency and is the largest Credit Reference Agency in the UK. Our data and advanced fraud technology helped prevent £1.8 billion in fraudulent transactions in the UK and at least US\$11bn globally during the last 12 months. Experian also supports on average 174k fraud victims each year through our Victim of Fraud support helpdesk. Our firm has just been named as the leading global provider of online payment fraud solutions by Juniper Research.

As we are not a PSP, and do not represent any consumer advocacy groups, the specific APP rules will not apply to us directly. Nevertheless, we have some high-level observations from our perspective as a Fraud Prevention Agency and a technology provider within this market and have decided to provide an overall view on the proposal instead of answering individual questions.

We believe the new regime is the right step towards protecting and reimbursing consumers involved in APP scam. However, the proposed changes are likely to be insufficient on their own, and further collaboration and innovation in the fields of data sharing and technology is required from all market participants to develop new tools and processes.

- 1. Expanding the Confirmation of Payee to around 400 PSPs in a "networked" architecture will introduce considerable burden, especially on smaller PSPs. Other existing bank verification solutions similar to Confirmation of Payee (CoP) can offer much needed innovation and flexibility to enable PSPs to comply faster.**

The PSR estimates that it currently takes between 9 to 12 months for a group of around 40 to 50 PSPs to deliver CoP, and it has found that current processes are not as fast and effortless to onboard as originally envisaged. Unless there is active innovation in the industry, the current proposed implementation timescales may not be feasible.

Whilst established PSPs will have the resources to build the required APIs and matching algorithms to implement CoP, it is likely that smaller challenger/start-up PSPs will seek off the shelf hosted solutions (potentially third party hosted/centralised) to enable quicker and more agile deployment.

Such solutions already exist in the market, including that offered by Experian, and could speed up adoption, given they are very quickly implemented through existing APIs. These solutions are already used by some PSPs that aren't yet onboarded onto CoP scheme formally. Introducing competition in the market will also drive innovation around improving name matching and scoring algorithms, additional data elements and broader coverage with other account types, such as credit cards etc.

2. **Information sharing in the payment journey between PSPs on sending and receiving accounts is the right step forward but will not be sufficient, as fraudsters might be hiding suspicious behaviour on other open accounts not involved in the immediate transaction.**

Due to the complex nature of APP fraud and different consumer interaction points involved, (e.g. social media, texts, banking applications) there is a need for greater information sharing between various service providers.

For example, to move from detective to preventative controls, we believe that it is necessary for a more holistic picture of the accounts of suspected fraudsters and not just the sending and receiving accounts – it would be desirable for PSPs to have the ability to query other PSPs on the nature of the relationship and historical transactions generated by suspected fraudsters across various accounts.

Through the Credit Account Information Sharing (CAIS) scheme, Experian provides access to credit data from 400 banks, lenders, insurers and utility and telecoms companies, which provides a more holistic view on consumer's past credit behaviour. Based on the recent proof of concept that we conducted, CAIS data alone can help detect a significant amount of "money mule" activity up to three months before APP fraud occurs, using predictive risk indicators such as age of open credit accounts, total number of accounts, credit utilisation, arrears and defaults etc.

CAIS data sharing is a well-established existing scheme that can enhance information sharing for PSPs with lower level of effort required and can serve as a blueprint for an APP fraud specific data sharing scheme between PSPs.

3. **PSPs should be encouraged to access existing fraud sharing schemes, demographics, and vulnerability data to effectively comply with the new regime. Also, the latest advances in Artificial Intelligence could offer better personalized interventions with minimum friction added.**

Experian as a global company has been seeing success in preventing fraud using some of the technology and data mentioned below.

- a. Pay.UK future fraud intelligence sharing should utilise existing successful fraud sharing databases (e.g. National Hunter, National Fraud Initiative, CIFAS, ) that have effectively prevented a significant amount of fraud in the past.
- b. Sharing demographics data of APP scam participants may also be helpful as it has proven effective in predicting the likelihood of someone falling victim of APP fraud. As per Experian [Quarterly Fraud Index Report](#), *"First party fraud is concentrated within those groups that are associated with low disposable income or people at the start of their careers. The older generations are much less likely to be driven to first party fraud, likely due to increased financial stability."*
- c. PSPs should be encouraged to leverage existing central data registers of vulnerable people, helping PSPs to identify vulnerability and treat them fairly when they fall victim of APP scam (not applying gross negligence exception).

- d. Organisations need to be able to offer greater personalised interventions with minimum friction introduced in the faster payments process. As an example, the latest developments in Machine Learning Large Language Models that use GPT-3 (a neural network ML model trained using internet data to generate any type of text) technology can help re-create in a chatbot setting a typical interaction that a fraud victim and fraud helpdesk human agent would usually have over the phone. This may enable PSPs to engage greater numbers of susceptible individuals in an educational and fraud awareness conversation without leaving the banking app itself. Machine learning trained fraud models have also proven to be much more robust in detecting new cases of unseen fraudulent behaviours with higher accuracy compared to traditional rules-based models.

Thank you for the opportunity to share our views on this important subject. We will gladly make ourselves available to engage and discuss further the points above.



# Featurespace

# Featurespace response to PSR consultation on Authorised Push Payment (APP) scams requiring reimbursement

Featurespace welcomes the opportunity to respond the Payment System Regulator (PSR) in its call for input on its proposed reforms to Authorised push payment (APP) scams, requiring reimbursement for victims.

This document contains both the Featurespace response to the specific questions posed by the PSR under [CP22/4: Authorised push payment \(APP\) scams: Requiring reimbursement](#), as well as Featurespace's position on the wider aims of the proposed regulatory reform to UK financial services.

Featurespace on the State of Fraud in the UK.....	3
Regulating for collaboration.....	3
Missing innovation .....	4
Future expansion.....	5
Driving down the total cost of fraud .....	6
Changing customer behaviour.....	6
Unreported scam volumes .....	7
Inbound transaction monitoring .....	7
Thresholds clarity and relevance .....	7
Making the UK a safer place to transact.....	8
Response to CP22/4: Authorised push payment (APP) scams: Requiring reimbursement....	8
Question 1: Do you have views on the impact of our proposals on consumers?.....	8
Question 2: Do you have views on the impact of our proposals on PSPs? .....	8
Question 3: Do you have views on the scope we propose for our requirements on reimbursement? .....	9
Question 4: Do you have comments on our proposals:.....	9
Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence? .....	9

Question 6: Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?.....	9
Question 7: Do you have comments on our proposals that:.....	10
Question 8: Do you have comments on our proposals that:.....	10
Question 9: Do you have comments on our proposal not to have a maximum threshold?.....	10
Question 10: Do you have comments on our proposals that:.....	11
Question 11: Do you have comments on our proposals that:.....	11
Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?.....	11
Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?.....	12
Question 14: Do you have views on our proposal that PSPs are able to choose to ..... depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?.....	12
Question 15: Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?.....	12
Question 16: Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?.....	13
Question 17: Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?.....	13
Question 18: Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?.....	13
Question 19: Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?.....	13
Question 20: Do you have views on how we should exercise our powers under FSBRA to implement our requirements?.....	14
Question 21: Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?.....	14
Question 22: Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?.....	14
Question 23: Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?.....	14
Question 24: Do you have views on the best option for short-term enforcement arrangements?.....	14

Question 25: Do you have views on the best way to apply the rules on reimbursement to indirect participants? ..... 15

Question 26: If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?..... 15

Question 27: Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis? ..... 15

### Featurespace on the State of Fraud in the UK

The PSR has long recognised the need for improvement in making the UK a safer place to transact. Fraud has grown to become the largest contributor to crime in the UK. Authorised Push Payments (APP) represent a significant proportion of UK fraud, more than 40% of total fraud values. In the first half of 2022 criminals stole a total of £609.8 million through authorised and unauthorised fraud, with £249.1 million lost to APP scams<sup>1</sup>. Although the number of cases has decreased by about six percent, there remains much to be done when it comes to limiting the negative impact of fraud on the consumer. The number of fraud cases in which consumers were refunded is rising and the speed at which this is resolved is accelerating, which shows a strong commitment from the financial services industry to limit the impact on consumers. However, despite these improvements and acts of good faith, as the Contingent Reimbursement Model (CRM) is voluntary just 56 percent of consumers were refunded in the first half of 2022. This clearly evidences the need to apply more regulatory pressure to ensure a fair and consistent approach to consumer protections in the face of fraud.

### Regulating for collaboration

The proposed mandates are right and fair in that they ensure the swift refund to victims of fraud. But it does appear that in the pursuit of consumer protection, there is a danger that additional operational complexity, technology overhead, and resource requirements are being created as a burden for financial institutions (FIs). The provision for adjustments to loss allocation through arbitration seems contrary to the overall aim: to fight back against fraud. Creating the provision for disputes between sending and receiving financial institutions could perhaps detract from the positive industry collaboration we have seen to date. And has the potential to divert attention and resource from innovations that could drive down fraud in its entirety, not just ensure refunds.

Consistently splitting the cost of consumer refunds equally between both sending and receiving parties is a blunt mechanism, but could ultimately create efficiencies in operations for all participants and drive an intensified focus on fraud reduction from both sending and receiving FIs. Creating a more active role for 'receiving only' FIs, often smaller Payments Service Providers (PSPs), brings their fraud prevention responsibilities in line with their access to financial services licensing and the payment systems under Open Banking and the New Access Model. To combat rising fraud operations by organised criminals there is a need

---

<sup>1</sup> 2022 Half Year Fraud Update, UK Finance

to perform fraud prevention on both outbound and inbound payments, and the inclusion of all PSPs in this proposal is a great step towards achieving this end-to-end fraud prevention approach in the UK ecosystem.

But achieving complete fraud prevention is not limited to FIs. Even in the proposed updates, there is not as yet any responsibility for those organizations on whose platforms' fraud is executed. With APP in particular, social engineering is often conducted through social and telecom networks yet there is no explicit provision for these organisations to participate in these anti-fraud measures.

### Missing innovation

Regulated reimbursement treats the symptoms of fraud, but does not go far enough in tackling the disease itself. There are several clear gaps in the proposal.

### *Data collection and sharing*

Early iterations of the consultation process indicated that centralised reporting, collection, and even publishing of fraud data would be a part of the framework. This version appears to discount this from the proposal. It is important to remember that fraud prevention is not a competitive differentiator for banks, and that the aim is to ensure that the ecosystem and economy is protected, but it is near impossible to effectively tackle fraud when there is no register of the true size and shape of the problem.

Card schemes have historically always collected fraud data in order to support members who are struggling with new trends and typologies. This would be an important role for the PSR to play in supporting its member to understand best practice.

### *Technology for transparency*

Under the current proposal there is no provision for the technical payment flow for cost sharing of the reimbursement from the receiving bank. There exists the opportunity to leverage both existing technical capability within the UK Faster Payments System (FPS) and future functionality planned under the New Payments Architecture (NPA).

The Request to Pay (R2P) messaging system could be leveraged by sending banks to facilitate the retrieval and reconciliation of 50 percent of refunds provided to victims of fraud, from receiving FIs. R2P was purpose built to improve the ease of reconciliation of inbound FPS, and many UK FIs have already completed the technical integration to the system. Additionally, Pay.UK would be able to easily count and report on this category of R2P on behalf of the PSR.

In the future when the migration to ISO 20022 has been completed under the NPA, this rich, structured data messaging-standard could be leveraged to create more transparency from receiving FIs in relation to transactions declined on suspicion of APP. Reason codes could be populated into the returned message that enable sending banks to augment their fraud strategies. With this enhanced transparency sending FIs would create efficiencies in fraud prevention strategies, as well as reduce the need for manual investigations, and ultimately improve the consumer experience.

### *Liability practicalities*

There is some discussion within the financial services community as to whether the split of liability on fraud losses could in fact be removed from the proposal all together, in favour of beneficiary banks retaining 100 percent of recovered funds. This could reduce the complexity and overhead of refunds and loss-sharing, but perhaps does not meet the aims around equal participation in this anti-fraud initiative from all FIs. Receive-only PSPs who would be motivated to tackle their mule accounts under liability sharing, would in fact feel a significant benefit of retaining those as long they were able to prevent the fraudulent funds leaving their institution toward their final destination. Obviously, all UK FIs want to tackle this national issue of fraud, but the proposal needs to be fair in its division of responsibility and cost to ensure that we move as one ecosystem.

Featurespace would not recommend repatriation of funds throughout an entire fraudulent transaction flow. The complexity of this and the diminishing returns of cost-sharing 50 percent of fraud losses throughout an entire disbursement tree would again create inefficiencies and detract from the higher purpose of preventing fraud. Instead, simplifying the scheme rules to provide an equal split on the fraud losses of each individual transaction between the sending and receiving bank would be more practical.

### *Future expansion*

This nationwide initiative to focus the community on tackling fraud is critical. Featurespace sees this initiative on reimbursement as the first step in a much broader set of necessary reforms. Future phases would need to consider other types of users and customers, as well as other payment systems.

### *Business users*

FPS is widely used by both consumers and businesses as a fast and efficient way to transact. But under the proposal there is no reimbursement protection for business users. For large corporations this may be simple to administer, but for small businesses often serviced by the retail arm of the bank it may prove challenging for FIs to enforce this from a customer service perspective. It is likely that independent traders and small business owners will expect the same Service Level Agreement (SLA) of protection for their personal and professional transactions.

If the reimbursement regulation is viewed primarily as a quick measure to protect consumers whilst the industry works to get fraud under control, then this may not prove to be a sticking issue in the long term. But it is possible that even business users would expect the same protections to be extended to their transactions on the same payment system eventually. This could present a very different risk profile for FIs in relation to potential reimbursement costs, as the transaction limit for FPS has been lifted to £1 million.

### *Payment types*

Much of the proposal on fraud reimbursement could easily be applied to other UK payment schemes such as BACS and CHAPS, which prompts the question as to why these rails are not considered holistically within the PSR's proposal. Historically, fraud has migrated from payment type to payment type, avoiding each new effort to stamp out fraud on a payment rail.

There is a possibility that current fraud conducted via APP will simply migrate to other rails if criminals deem it a more 'profitable' approach. If this should happen, those large banks that offer the full spectrum of payment services to their customers could once again be left bearing a disproportionate amount of the total cost of UK fraud.

#### Driving down the total cost of fraud

The cost of fraud reimbursement for consumers has to be funded from somewhere within the UK economy. There is a risk that inadvertently the consumer will end up paying this cost.

Larger banks who are members of the voluntary CRM code have already invested extensively, but the changes will still require further investment. There is a risk of some UK PSPs and fintechs being unable to bear this increased burden which may not be relative to the current size of their revenues. The UK has a thriving fintech scene, with more than 250 licensed PSPs (Electronic Money Institutions) (the highest number in Europe), which creates competition in financial services and choice for consumers. In theory these fintechs should be able to quickly adapt and create solutions to reduce fraud rates and therefore liability. But if this does not happen in practice, the cost of fraud reimbursement could collapse this fintech sector, and the choice of services will be restricted for consumers.

As FIs recalculate the total cost of fraud to include increased reimbursement, this may by default create an increase in the cost of financial services for consumers. This could be directly in the form of increased charges for services, or as indirectly as limited investment in innovation by FIs.

#### Changing customer behaviour

One factor that has been clearly evidenced since the launch of FPS, is the role of customer education in understanding the benefits and potential risks of a new payment system. Many larger FIs have moved to provide proactive and continuous education to their consumers. There should perhaps be a component of the proposal which includes a mandate to educate consumers. The burden of education is currently disproportionately born by banks.

There is rightfully some concern that we may see an increase in first-party fraud once the regulation is well publicised. But more concerning is the increased possibility of collusion in a cost-of-living crisis, with criminal networks looking to recruit consumers into their schemes, likely as money mules. Financially vulnerable consumers may become targets for criminal recruitment.

Within the realm of consumer behaviour, there is not a clearly defined framework for the gross negligence exception that the proposal allows for. Leaving this too open to interpretation risks placing the most vulnerable consumers at risk, in contradiction of UK financial inclusion policy aims. Any consumer can be vulnerable at any point in their financial services relationship.

There is some discussion of whether there will be a diminished sense of responsibilities from consumers once they no longer carry the risk of scams losses. However, the reality is that it is not the responsibility of the consumer to prevent scams. It is a broader policymaker, law

enforcement, and private industry responsibility to safeguard the financial ecosystem and the economy at large.

### Unreported scam volumes

What is likely is that with the change in reimbursement entitlement, that the industry will see a change in fraud rates. Romance scams in particular are likely vastly underreported, as victims feel embarrassed and unwilling to go through the turmoil of seeking reimbursement without a guarantee. With the legislation change, currently unreported scams will surface. As an industry we currently only see the tip of the iceberg, and it would be advisable for FIs to increase their fraud prevention budgets for 2023 onwards. Perhaps seeing the true extent of the problem in relation to the bottom line will support fraud teams in achieving sign off for their business case.

### Inbound transaction monitoring

The extension of liability for fraud losses to receiving banks is an important step. But the question remains whether the proposal goes far enough in preventing criminals from accessing stolen funds.

*"Repatriation of APP scam losses occurs where the receiving PSP is able to detect, freeze and return funds stolen as part of an APP scam. Rapid and effective communication from the sending PSP may aid receiving PSPs in detecting and freezing fraudulent funds."*

Transaction monitoring on inbound payments for the purposes of fraud prevention would be more effective in preventing criminal networks from profiting from scams, and simplify the repatriation and reimbursement process. There could be guidance from the PSR to include inbound transaction monitoring as a recommended line of defence against APP.

### Thresholds clarity and relevance

The provision of thresholds in terms of both a minimum limit and excess complicates reimbursement understanding for consumers. If the excess is £35 and the minimum limit is £100, will a consumer claiming for £135 believe they will receive nothing? This could be simplified by expressing the excess as a percentage of the claim rather than applying both and would also make the limits fairer for consumers who may only lose £50, but it was their total account balance. A 5% excess in this case would be enough to illicit caution in future in the same way a 5% excess for a much larger claim would. The excess or lost cost for the consumer should be proportional to the total fraud if the aim is to both protect customers and encourage vigilance against scams.

There is a potential downside to defining thresholds, in that they could have the unanticipated consequences in driving fraudsters to adapt their tactics to target scams beneath these thresholds in order to avoid the investigative scrutiny of FIs, and their pursuit of funds for recovery. Or, if thresholds are applied across cases rather than individual transactions there is a possibility of creating first-party fraud, where customers may benefit from sending another scam payment so that their claim is over the threshold.



## Making the UK a safer place to transact

As an industry it is necessary to address the current impact APP is having on consumers. It is neither right nor fair that consumers are bearing the costs of rampant fraud in the UK. But the proposal in its current form appears a fairly blunt instrument. It may or may not eventually reduce the overall fraud levels in the UK. The missing element is the focus on making the UK a safer place to transact. Featurespace would welcome more specific mandates on driving down fraud rates, perhaps taking inspiration from the low-risk thresholds applied in Strong Customer Authentication (SCA) exemptions under the Revised Payments Services Directive (PSD2), as this incentivises low fraud rates. Complexities will of course arise as this consultation becomes policy in UK payments, and Featurespace is confident that the PSR will look to continually optimise APP fraud prevention measures as the practicalities play out and the market needs evolve.

All of this creates a massive incentive for UK FIs to invest in fraud controls, and particularly in technologies which can outsmart criminals. As an industry there is a lot of opportunity to apply machine learning, and in particular deep learning techniques to improve fraud prevention rates on both outbound and inbound payments.

Working with one large UK bank we have been able to deliver a huge reduction in false positives (over 90%) and massive improvement in the Value Detection Rate (~250%) for APP scam detection.

## Response to CP22/4: Authorised push payment (APP) scams: Requiring reimbursement

### Question 1: Do you have views on the impact of our proposals on consumers?

At a high level, the proposals will incentivise increased focus on fraud prevention, and support fraud teams in securing investment for proven solutions to improve detection and increase protection for consumers.

Consumers not suffering fraud may experience increased friction, but assuming investment is sufficient, the friction will be significantly targeted, and processes will develop to ensure the net outcome is very positive for consumers. Increasing expectations of refunds will reduce stress and other detriment that consumers could suffer if they are victims of APP. However, those who are victims of lower-value APP fraud may suffer more than under the current voluntary CRM code. If their claims fall below the new thresholds, they may not receive any refund.

### Question 2: Do you have views on the impact of our proposals on PSPs?

The obvious impact to PSPs is increased costs due to increased refunds and implementing new processes to manage the arbitration requirements. The indirect impact will be the response of investing in processes to make them efficient and consumer friendly, whilst also investing to reduce the number of victims and mule accounts. Regulatory pressure and compliance requirements should support building the business case within PSPs, and may

even help PSPs support changes that fraud teams had on roadmap to reduce fraud and improve customer experience. This assumes any regulatory enforcement would outweigh the cost of development. Smaller PSPs may see impacts that are disproportionate to their relative revenues, but they are also likely to develop solutions more quickly and efficiently than larger PSPs.

Question 3: Do you have views on the scope we propose for our requirements on reimbursement?

Limiting scope to FPS may lead to fraudsters targeting other payment types (even if this will be harder for criminals to facilitate), and that fraud does not reduce as much as expected. If scope could be extended to cash withdrawals, CHAPS, and international payments, then consumer understanding and expectation would be better, and the fraud migration risk would be minimised.

Question 4: Do you have comments on our proposals:

- that there should be a consumer caution exception to mandatory reimbursement
- to use gross negligence as the consumer caution exception
- not to provide additional guidance on gross negligence?

It is reasonable that consumers should exercise some caution in initiating transactions, in line with information and guidance from their FI. Fraud prevention can be strengthened with consumer awareness. But in reality, a single consumer who is the target of a sophisticated scam from an organised criminal network cannot be reasonably expected to spot this. It is right that the burden of prevention and protection be placed on FIs who have the resources, expertise, and technology to outsmart this risk.

Gross negligence may seem a reasonable measure for liability, but defining that gross negligence is challenging. Proving whether a customer exercised any caution has been challenging in unauthorised fraud cases, and would be the same for APP.

Additional guidance should be provided by the PSR providing clear examples and scenarios, with a focus on what the customer believed to try and avoid Financial Ombudsman Service (FOS) disputes. For example, would previous APP claims be evidence of gross negligence? At this stage it seems this may be assumed by some PSPs.

Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?

There is a duty of care that should be exhibited by FIs in relation to vulnerable customers who may become victims of these sophisticated manipulation and impersonation scams, even if a less vulnerable customer may have been able to avoid this. Vulnerability may be both permanent and transient depending on the customer and the moment in time.

Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?

Current FCA definitions of vulnerability appear to be working in other types of fraud cases.

#### Question 7: Do you have comments on our proposals that:

- sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- any 'excess' should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

If customer is classified as vulnerable, then applying an excess amount should not be valid.

The provision for both an excess and a minimum threshold seems to disproportionately impact financially vulnerable customers, for whom £35 is a significant amount to lose in excess. Although the intent is likely to encourage customer caution, most consumers are not aware they are a victim of a scam until after the fact. This is the element that makes APP fraud so successful for criminals and so difficult to prevent. If the excess were a percentage of the total claim, it may have an increased impact and a fairer impact on customers with varying sizes of claim and varying balance before the fraud. For example, 5% may work better so that customers with fewer funds and smaller claims are less impacted, but larger claims resultant from higher net-worth individuals would still have an impact and lead to increased caution.

PSPs may only apply the excess to cases with some level of negligence, or certain scam types such as investment and purchase, as well as potentially applying to repeat claimants. Negligence would be challenging to prove on an individual customer basis, as the customer would not be aware that other consumers had fallen for same scam.

The approach may provide a balance in relation to caution shown by consumers and whether the consumer was looking to make a financial gain when they became a victim. The key is that not all cases should be viewed as the same, even if the typology appears similar.

#### Question 8: Do you have comments on our proposals that:

- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?

PSPs may quickly realise that they have a lot more vulnerable customers than anticipated. Once the regulation becomes public domain, advisors to victims will look to apply vulnerability every time it is relevant.

Similarly to applying an excess of £35, minimum claims could discriminate against customers with low account balances and low claim values. It may be better not to have a minimum claim and just have an excess that is a percentage of claim. This would be simpler and remove the potential discrimination against the lower value claimants. The excess would cover the cost of processing the claims. Whether it was an excess or a limit, vulnerable customers should have claims refunded in full regardless.

#### Question 9: Do you have comments on our proposal not to have a maximum threshold?

No maximum threshold should not be needed as it is not relevant to the scam risk. PSPs and customers should be acting with increased caution with very high transaction values. The current proposal is focused only on consumers, however given the transaction value limit of FPS (up to £1 million) and the likelihood that similar regulation will be required for all transactions on the scheme, as well as other payment systems, beginning this regulatory reform without a maximum threshold seems prudent.

Question 10: Do you have comments on our proposals that:

- sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
- any time-limit should be set at no less than 13 months?

It seems reasonable to provide a guideline on length of time as it can become difficult to investigate a claim that is more than a year old, and for most APP, FIs could expect a customer to recognise and report a scam within these timescales. Thirteen months appears reasonable and aligns with unauthorised fraud regulations.

The challenge would be longer running scams, such as investment scams where customers think they are investing for the longer term. Or romance scams which usually happen over a long period of time, and only after larger payments do victims realise it's a scam. There is usually a long tail on romance scams and the customer is emotionally vulnerable. In these scenarios exemptions to the time limit could be offered.

Question 11: Do you have comments on our proposals that:

- the sending PSP is responsible for reimbursing the consumer
- reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?

This ensures the timely reimbursement of the consumer in cases of APP which is a positive improvement.

Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?

Gross negligence is likely going to be very rare and challenging to prove. It would be better for the industry to focus preventing fraud rather than trying to shift liability back to the consumer. However, identifying whether a consumer received a targeted warning and/or data suggests a consumer is lying should be quick and could trigger several days more time to collect information and assess the case further.

Gross negligence would mean that the FI did everything within its power to identify potential fraud and advised their customer, who understood the warning and still opted to complete the transaction anyway, believing or not caring whether they would be refunded if it turned out to be fraud. For this to work there would need to be a definition of 'everything within its power', this may include a requirement for a human interaction between the consumer and an experienced fraud analyst, something beyond an automated notification.

During scams the criminal is often on the phone with customer, instilling a sense of urgency and pressure. Criminals are aware of the FI systems and are talking victims through the process to make it happen quickly. Applying holds or cooling off periods to payments during the interaction between the fraud analyst and the consumer will be key to allowing consumers to come to terms with the reality of the scam.

In cases of first party fraud, the burden of proof would be the same as for authorised fraud cases. FIs would look to evidence that the customer has contradicted themselves in their account of the fraud and it does not align with the FI data, whilst also looking to identify links

to other claims that therefore suggest organised and systematic exploitation of the claims process

Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

We would support a default allocation without the provision to contest between sending and receiving FIs. This shares the burden of APP more fairly across the entire financial services industry whilst providing an incentive to reduce fraud and the associated losses.

Question 14: Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?

There should not be a process for negotiation, mediation, or dispute as this will be time consuming and deliver unsatisfactory results. The time and cost should be saved by having one allocation that applies to all APP cases.

The option to deviate from the default allocation creates a lot of operational overhead for FIs, without any indication as to the capacity requirement for processing disputes. The split could be debated for a long time overall or on every case as they occur. The 50:50 split is a sensible starting point and should be applicable in all cases unless reassessed at a future point. Debating for individual cases would be time consuming and won't deliver clear and fair outcomes either.

It could be viewed that creating the dispute process creates an incentive for those PSPs who are 'receive only' for FPS to dispute every APP case in order to minimise their loss exposure. There may be a need to apply the 50:50 split to unauthorised as well as authorised fraud to avoid PSPs looking to share losses with receiving banks, by saying their customer authorised the payment.

Question 15: Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?

This is a very complicated concept and would need to be divided into logic that applies to each claim, and still can flow back to the original transaction and the originating claim. In this proposal each step or generation would need to be assessed independently and then funds repatriated back to the start in some kind of tree with transactional branches. It would be more practical to treat each transaction as an individual case for allocation and avoid multi-generational liability allocations, or even remove the repatriation and allow the final FI in the chain to keep any recovered funds

As an example of the complexity of multi-generational scam refunds: funding an account in the customer's own name would result in 50% of loss coming from the sender and 50% from the receiver. This may be the same PSP in some cases. If funds are then moved on by a fraudster from the new account, then the PSP would be liable for 100% of the fraud and could then return funds to the initial PSP to remediate the situation. If funds are moved on by the customer, then a second claim is started and treated individually. If payments aren't FPS and

there is no refund, then no further action is taken. If a refund is paid from a card claim, then funds can be returned. If a refund is paid by FPS, then loss would be split again. This would then lead to the second and third PSPs sharing the loss and then passing the funds back, as shared liability and shared repatriation benefit to the first to fund the claim, and mean that the first PSP doesn't have a loss. The key element would be that the refund of the middle account means full funds are available to be repatriated.

**Question 16: Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

50:50 allocation for repatriated funds is common sense when the refund is 50:50, but this becomes very complicated and may even have to be completed in specific order to reverse a sequence of payments. It would seem to be possible for a system to utilise API calls to notify FIs about fraud claims and trigger automated payments to pay claims and split repatriation funds.

There is a potential for the repatriation of funds to be incredibly complex, there is no existing system to facilitate this, and it would be challenging and costly to build a central exchange system or require individual APIs as bilateral agreements between FIs. Sending FIs would not be aware that funds were recovered, so the onus would be on receiving banks to send the repatriated funds as refunds back through the transaction flow. This is mimicking the historical complexity of correspondent banking chains, which the transaction and cross-border payments teams are working to eradicate.

**Question 17: Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

Directly connected PSP participants and PSPs indirectly sending and receiving payments need to be allocated losses based on their customers sending and receiving fraudulent funds, regardless of whether they are direct or indirect participants.

**Question 18: Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

The PSO has more ability than the PSR to be flexible and dynamic as these changes are rolled out. Scheme rules are more adaptable rather than regulation. As new niche cases emerge these rules can be added to the ruleset, and lessons learnt can be applied.

**Question 19: Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

It is positive that anti-fraud innovations are to be integrated into the payment rules directly. Approaches need to be standardised where possible to help embed with consumers and ensure fairness regardless of who they bank with. The standardisation needs to still allow for innovation towards a best in industry solution. Rules around the standard of evidence must not be open to interpretation. Additionally, designated arrangements to depart from default allocation are not needed initially and may not be needed at all.

Question 20: Do you have views on how we should exercise our powers under FSBRA to implement our requirements?

N/A

Question 21: Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?

If the allocation is introduced as 50:50 and not open to individual debate or dispute, then the process will be much simpler and work better in practice. The application of the CRM code shows what happens when inconsistency is created in the system: not all FIs are members, those who are members are refunding at different levels, and there is no clarity from the consumer point of view.

This approach will raise the bar terms of fraud controls. The logic behind avoiding disputes is to encourage collaboration and consistency as much as possible.

Question 22: Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?

A reporting requirement is a crucial aspect of enabling the industry to get a better control of APP fraud. Industry data is confidentially shared between FIs, because fraud prevention is a non-competitive aspect of their operations. Centralising this reporting and creating consistency in reporting requirements will help combat historical challenges around individual banks becoming the target for APP scams, with better visibility on how fraud trends shift in the ecosystem.

Accurate and useful fraud data requires honesty from reporting members and a requirement to publish these numbers. FPS could be used to split claims and return funds, thus giving Pay.UK visibility of some of the process to help with monitoring and compliance.

Question 23: Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?

Centralised reporting and compliance monitoring could be very beneficial for PSPs who will need to agree on claims and return funds. It is very difficult to assess the costs and benefits of a real-time compliance monitoring system, and the current proposal requires many assumptions. It is unlikely that anything would be designed and built in less than twelve months and therefore would not be ready for use in 2023.

Question 24: Do you have views on the best option for short-term enforcement arrangements?

Initially encouragement rather than enforcement might be the best approach. Publishing performance ratings privately to members has been shown to encourage participants in FPS to meet SLAs around uptime and clearing windows. Perhaps a similar leader board could encourage compliance rather than needing to threaten fines or exclusion from FPS. But in the



longer-term enforcement via fines or increased fees seems reasonable, and echo the fraud performance metrics managed card networks.

**Question 25: Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

Indirect participants are still licensed financial entities under the FCA. If they have agency access, transactions associated with their own sort codes can be subjected to the same reimbursement rules as any direct participant. For non-agency participants who share a sort code with other indirect PSPs, the sponsor entity would need a mechanism to pass the liability through to the PSP. In this scenario the indirect access providers (IAPs) would need to factor this into their business model. In this way all participants can be held to the same standards through their sponsoring banks.

**Question 26: If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

There should be direction to ensure consistency. The aim is to reduce fraud. Without direction indirect participants and IAPs risk becoming the weak link in the anti-fraud defences.

**Question 27: Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

The analysis is very general in its approach at this stage. There are no built-in growth projections neither for FPS transactions nor levels of scams, and there is no underlying baseline from which to forecast these accurately. There is currently a large volume of unreported APP fraud which will become evident as reimbursements become mandatory. Those FIs who currently do not leverage some APP-prevention capabilities and could take a significant time to develop them, could see their rates increase by an order of magnitude. Particularly for new players in the ecosystem and indirect PSPs who have not previously borne any liability these costs could be unbearable.

If you have any questions about this response, please contact:

████████████████████

Head of Product  
Marketing

██

████████████████

████████████████

████████████████

Fraud Subject Matter  
Expert

██

████████

████████████████

████████████████

Fraud Subject Matter  
Expert

██

████████

████████████████



# Financial Services Consumer Panel

Telephone: 020 7066 9346

Email: [enquiries@fs-cp.org.uk](mailto:enquiries@fs-cp.org.uk)

25 November 2022

Submitted online: [appscams@psr.org.uk](mailto:appscams@psr.org.uk)

Dear Sir / Madam,

**Financial Services Consumer Panel response to CP22/4 Authorised push payment (APP) scams Requiring Reimbursement consultation paper**

The Financial Services Consumer Panel is an independent statutory body. We represent the interests of individual and small business consumers in the development of policy and regulation of financial services in the UK.

The Consumer Panel strongly welcomes the PSR's proposal to make reimbursements mandatory for victims of APP fraud. We support the two key outcomes the PSR wishes to achieve, namely: to protect people who have experienced APP scams and to identify and address fraud in the Faster Payments System. Both outcomes are necessary to ensure confidence in the payments system.

The growing nature of the APP threat requires the regulator and industry to swiftly address gaps which allow APP fraud to occur. Consumers are suffering undue harm because of the lack of industry-wide commitment and coordination to tackle such scams as well as the uneven distribution of efforts to combat fraud and to reimburse victims. The introduction of the mandatory reimbursement requirement, in conjunction with the PSR's proposed 50:50 default allocation of costs between sending and receiving Payment Service Providers (PSPs) will, we believe, help galvanise the industry into action, increasing the amount of information sharing and collective fraud detection and prevention work.

We expect that parts of industry will push back on the PSR's proposals, arguing for longer implementation timelines. We strongly encourage the PSR to stick with its calendar and resist this pressure. We, like the PSR, would like to see reimbursements mandatory as soon as possible and believe that the proposed end deadline of 2024 gives the industry ample time to implement them. The deadline should help to stimulate concerted action right across the industry and reduce the amount of harm suffered by consumers. The timeline will also give the industry sufficient time to devise more granular means of allocating costs reflecting sending/receiving PSPs' efforts to detect and prevent fraud.

If the industry determines to re-calibrate the cost allocations, penalising those PSPs that fail to take preventative measures, the measures will even further incentivise poorly performing PSPs to address their fraud controls. We fully recognise that more complex cost-allocation rules will need to be devised for multi-generational scams, however this consideration should not delay implementation of the mandatory reimbursement – it is clearly only by putting the cost onus on the industry and scheme operators that such rules will be devised and made operational.

Having robust and effective fraud controls in place should be a condition of operating in UK payment systems. Payments *must* be safe, and they *must* be trusted. Payments are not optional nice-to-have products used only by a sophisticated subset of consumers. All consumers throughout the United Kingdom have to make and receive payments and they need to have confidence in the payments system as well as in their ability to access and use it. With the increased use of e-commerce, the declining availability and acceptance of cash and the closure of bank branches, more and more consumers are required to use Faster Payments. These factors, along with the PSR's stated strategic priority of unlocking account-to-account payments and the move to open banking-initiated account-to-account payments, require all consumers to be able to use the system with confidence.

We have concerns about the £100 lower limit for mandatory reimbursement and oppose the £35 "excess" that the PSR propose consumers could bear. We understand that firms may disapply these limits, but in the interests of protecting every user of the system, we would prefer regulation to maximise coverage. The inconvenience and stress of a misplaced payment, and the importance of smaller sums to many people, particularly those in vulnerable circumstances, may place unnecessary burdens on consumers, deterring them from reporting incidents or seeking redress. The impacts may be detrimental, especially for those who are vulnerable.

Preventing fraud within the payment system is key to ensuring consumer confidence, to minimising consumer harm as well as to reducing criminality overall. By making reimbursements mandatory the PSR will help to restore and maintain consumer confidence, to protect consumers and to help to minimise the extent of fraud within the system.

Our responses are included at Annex A below.

Yours sincerely

██████████

Chair, Financial Services Consumer Panel

## **Annex A – Response to Questions**

### **1. Do you have views on the impact of our proposals on consumers?**

We believe that implementation of the proposals will have an immediate and significant positive impact on consumers, resulting in a much greater proportion of consumers' losses being reimbursed, increased levels of consumer certainty overall and a reduction in psychological harm being suffered by victims of fraud. Over the longer term the move to mandatory reimbursements should lead to a reduction in the number of successful scams as PSPs individually and collectively step up their efforts to combat fraudsters. In turn this should lead to greater consumer confidence in the system and more uptake of account-to-account payments.

In the near term, as PSPs put more checks in place and stop more 'suspicious' transactions, consumers may face more interrupted payment journeys. We, like the PSR, believe that the benefits of preventing consumer harm outweigh any inconvenience that may be caused and concur with its view that these methods will be fine-tuned and improve over time as systems are refined.

The PSR notes in its consultation that there is a risk that the measures might cause some PSPs to consider restricting services to certain consumers, such as older consumers, because they may be perceived as more likely to become victims of APP scams. The PSR should monitor for this ensuring that PSPs treat current and prospective customers according to their obligations in the Equality Act 2010.

### **2. Do you have views on the impact of our proposals on PSPs?**

Like the PSR, we believe that the prospect of mandatory reimbursements will increase the cost of APP scams for PSPs and therefore incentivise prevention. In all likelihood, we will see more detection and prevention tools emerge and greater intelligence sharing between PSPs.

By redistributing the costs across both sending and receiving PSPs *and* allowing the industry to fine tune the cost allocations we would expect the worst-performing PSPs – in particular those that receive the most scam payments – to face the greatest costs and therefore the greatest incentives to improve their responses and stop more scam payments.

As we stated in our introduction to this response, we expect that parts of industry will push back on the PSR's proposals, arguing for longer implementation timelines. We strongly encourage the PSR to stick with its timelines and resist this pressure. We, like the PSR, would like to see reimbursements become mandatory as soon as possible and believe that the proposed end deadline of 2024 gives the industry ample time to implement them. The deadline should help to stimulate concerted action right across the industry and reduce the harm suffered by consumers. The timeline will also allow the industry plenty of time to devise (should it wish to do so) more granular means of allocating costs reflecting sending/receiving PSPs' efforts to detect and prevent fraud. It should thereby also serve as a timely incentive for poorly performing PSPs to address their fraud controls.

### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

The PSR has proposed that the reimbursement requirements cover all payers who are consumers, micro-enterprises or charities, as defined in regulation 2(1) of the Payment Systems Regulation 2017. The PSR rightly observes that larger business payers can be expected to have greater capability to protect themselves from APP scams, and it would not be proportionate to require PSPs to reimburse such businesses for their losses. Consideration should therefore be urgently given to this extensive and important cohort, including any charities not covered in the PSR's definition, and how they can best be protected and supported.

While we recognise that the PSR is applying the reimbursement requirement to the same coverage of payers covered by the CRM code, we would caution that it ignores the significant number of businesses that are neither micro-enterprises nor larger businesses. Micro-enterprises are defined to be enterprises that employ fewer than ten persons and whose annual turnover and/or annual balance sheet total does not exceed €2 million. Large businesses (those who could be expected to protect themselves or bear reasonable losses) are meanwhile commonly defined as businesses with more than 250 employees. According to the BEIS annual statistics, there are some 247,000 businesses with a combined annual turnover of more than £1,160 billion in the UK that sit between the two categories and who would be unprotected by the proposed measures. Corporates are by no means immune to APP scams, and these middle-size businesses are no exception. They will not enjoy the same resources as their larger peers and will very possibly become the targets of fraudsters given the scope of the new arrangements. Consideration should therefore be urgently given to this extensive and important cohort and how they can best be protected and supported.

We support the PSR's proposals to include all PSPs (whether directed or indirect payment system participants), all Faster Payments and all CHAPs payments. We also support the PSR's expectation that PSPs should reimburse 'on-us' APP scam payments in the same way as payments made via Faster Payments and would encourage the regulator to monitor this area closely to ensure these expectations are met.

As regards the value in scope. As stated in our introductory comments, we would encourage the PSR to consider whether a lower threshold than £100 might be appropriate, and we would discourage the PSR from allowing PSPs to levy an excess on reimbursements. We hope and expect that there will be positive competition between PSPs in both respects, however we would also caution that this competition may not ultimately benefit those most needy of the fuller reimbursements and is far likelier to be targeted at more affluent consumers.

- #### **4. Do you have comments on our proposals:**
- **that there should be a consumer caution exception to mandatory reimbursement**
  - **to use gross negligence as the consumer caution exception**
  - **not to provide additional guidance on gross negligence?**

While we would agree in theory with the PSR that there could be a consumer caution exception to mandatory reimbursement, provided that it could only be triggered where the consumer acts with 'gross negligence' and that 'gross negligence' remains a high bar, we have severe reservations about this provision.

Firstly, the PSR would need to provide clarity on 'gross negligence' within their guidance to prevent misuse. Secondly, each fraud would need to be judged on an individual, case-

by-case basis taking into account both the form of the payment and the individual circumstances of the customer. Thirdly, there is the potential for a large number of disputes to arise – disputes that will add to the Ombudsman’s (FOS) caseload and cause consumers further distress and harm.

A final concern here relates to payment journeys and how these are changing. PSPs are designing consumer journeys to be ever smoother, faster, and less visible and the payment process ever less experiential to payers. Given this, we would question whether there *could* be circumstances in which it would be fair to argue the consumer had been grossly negligent.

In summary, the Panel recommends that the PSR should: consider the proposal in light of the prevailing payment trends including the move to embedded payments; provide a clear definition of ‘gross negligence’; and consider what could mitigate the risk of PSPs initiating unfair disputes.

## **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

The Panel supports a fair and flexible response which takes into account the wide range of different needs, characteristics, and circumstances that individuals may have. Since the needs of individuals can differ, a tailored approach should be required, as a one-size-fits-all approach would not be effective, nor would it lead to positive outcomes. Firms will need to ensure that they have sufficient knowledge of the risk factors and impacts of vulnerability, which should also be embedded throughout the organisation (including frontline staff), so that there is better understanding of the challenges that are being faced by consumers. This should allow for a fair decision to take place.

The FCA published its Vulnerability Guidance under section 139A of the Financial Services and Market Act 2000<sup>1</sup>, setting out its view of what firms should do. Firms should comply with their obligation under the Principles to ensure that the treatment of vulnerable customers is fair. In April 2022 the British Standards Institution (BSI group) published BS ISO 22458: Consumer Vulnerability<sup>2</sup> - an international standard that provides guidance for service providers on how to implement inclusive service and how to understand, identify and support vulnerable consumers. The Panel would encourage firms to utilise the guidance. Although the standard is voluntary it can be certified by an independent third party and BSI states that firms who chose to comply with BS ISO 22458 are demonstrating their commitment to ‘doing the right thing’ for all consumers.

The term ‘gross negligence’ within the question infers that the consumer is at fault. It is possible that the consumer could have vulnerable traits such as cognitive impairment or a developmental condition – it is likely, then, that they would be less capable of clearly understanding information, communicating, and making informed decisions. We suggest that the PSR consider rephrasing this wording in their final guidance.

---

<sup>1</sup> <https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf>

<sup>2</sup> [https://www.bsigroup.com/globalassets/documents/about-bsi/nsb/cpin/bsi\\_cpin-consumer-vulnerability-brochure\\_digital2.pdf](https://www.bsigroup.com/globalassets/documents/about-bsi/nsb/cpin/bsi_cpin-consumer-vulnerability-brochure_digital2.pdf)

In findings from the FCA's latest Financial Lives Survey<sup>3</sup>, in May 2022, 47% of UK adults showed 1 or more characteristics of vulnerability, up from 46% in February 2020 – this equates to an increase of 0.9 million adults from 24.0 million to 24.9 million over that period. Evidence from Action Fraud<sup>4</sup> shows that increasing numbers of fraudsters are exploiting recent events and current economic conditions to target consumers with scams.

The Panel's view is that given the ubiquity of payments usage, it would be a reasonable regulatory starting point that in at least 47% of APP scam incidents the consumer might be vulnerable. Firms should take this into account when assessing negligence and regulators should question firms about how they are applying a 'vulnerability lens' to assessments and how this is influencing reimbursement decisions.

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

The FCA's definition<sup>5</sup> of a vulnerable customer is "*someone who due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.*" The Panel acknowledges the FCA definition, however this must be underpinned by more detail about the wide range of factors that can contribute to vulnerability, the impact that this has on an individual's ability to interact with organisations and how firms can best identify and respond.

However, firms cannot work from the FCA's definition alone and will need to understand how to practically apply this within their own businesses. As mentioned in Q5, BS ISO 22458 provides detailed guidance to service providers on how to understand, identify, and support vulnerable customers. The PSR could encourage firms to apply this guidance to demonstrate their support for all consumers in vulnerable situations.

**7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

The Panel does not believe there is a need for an excess and does not agree with the rationale the PSR sets out for having an excess hold. The Panel believes that instead there should be a much lower, zero and/or minimum limit as opposed to the £35 excess hold.

**8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**

---

<sup>3</sup> <https://www.fca.org.uk/data/financial-lives-2022-early-survey-insights-vulnerability-financial-resilience>

<sup>4</sup> <https://www.actionfraud.police.uk/news>

<sup>5</sup> <https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf>

- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

The Panel understands the rationale for setting a minimum threshold – namely keeping administrative costs ‘proportionate’ for PSPs and limiting the caseload of APP scam claims that need to be processed. The Panel would however encourage the PSR to consider setting a lower threshold, possibly as low as zero, bearing in mind that *all* UK households – including those on very low incomes – use payments. For many of those, the loss of £100 will be unaffordable. There is also the risk that fraudsters will migrate to areas where protections are weakest, so the effect of a £100 minimum will be fraudsters targeting sub £100 transactions.

The Panel would hope that there will be competition in this area with some PSPs not setting any threshold, however we would caution that the competition may target more affluent consumers not the most in need of this service. The PSR could perhaps consider whether PSPs providing services to consumers with lower balances/ lower monthly payment values could calibrate down (or altogether eliminate) the thresholds.

**9. Do you have comments on our proposal not to have a maximum threshold?**

The Panel support this proposal. PSPs should exercise caution on all payments, particularly higher value payments – and most especially payments that are of sufficient size to have prudential implications for them.

**10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

The Panel supports the proposed 13-month minimum time limit, on the understanding that customers would have recourse to the FOS if they believe the time limit has been unfairly applied. This time limit should not be shortened.

**11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

The Panel supports the proposal that the sending PSP should be responsible for reimbursing the consumer as well as the 48-hour time limit set for that reimbursement. Extending the time limit could have a significant impact on consumers on low incomes as this may compromise their abilities to pay bills or do essential food shops. This time limit should not be extended.

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The standard of evidence for ‘gross negligence’ or first party fraud should be set sufficiently high to dissuade PSPs raising unnecessary, harmful, and costly disputes which will lead to consumer psychological harm. The investigation should be time-limited to ensure that honest victims of fraud can secure quick reimbursement. To mitigate against first-party fraud and avoid the risk of proliferation of first-party fraudsters we



would recommend the PSR further encourages information-sharing between PSPs as well as close cooperation with law enforcement.

We would welcome further clarity from the PSR about the experience consumers can expect in cases where a PSP suspects they have been grossly negligent. As well as limiting how long investigations can take, the PSR should offer rules or guidance on what communications consumers can expect. Firms need to avoid people feeling stigmatised or even "criminalised" at a time when they may be feeling vulnerable. Communications and service in this area should meet the high standards expected under the FCA's new consumer duty.

As referred in question 4, when dealing with gross negligence each fraud should be judged on an individual case-by-case basis as individual circumstances will differ. Clarity should be provided within the PSR's guidance by outlining a clear definition to prevent misuse.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

Yes. We strongly support the default allocation of reimbursement costs and fully expect that the industry will, over time, evolve more sophisticated models that will more strongly penalise the less careful PSPs thereby leading to improvements in the safety and security of the system overall.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

Yes, we support this, but would stress that any such arrangements (or disputes) should not affect the consumer. The consumer should, as proposed, have certainty they will be reimbursed by the sending PSP within 48 hours.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

No, but as stated in our introduction and under Q14, the complexities involved in allocating costs between the PSPs involved in such scams should not result in uncertainty or consumer detriment. Victims of such scams should be afforded the same certainties and the same 48-hour pay-out from sending PSPs as victims of any other frauds. The onus should be on the industry to devise and implement the cost allocation solution to support such pay-outs that it determines is most appropriate – including perhaps by taking a flexible cost allocation approach.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

The Panel have no particular view on this proposal but would encourage the PSR to monitor how the model incentivises/disincentivises PSPs from seeking to freeze and repatriate funds.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

No, but the Panel would encourage the PSR to monitor how the model incentivises/disincentivises PSPs from improving their protection and detection measures.

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

The PSR's vision is for Pay.UK, as payment system operator (PSO), to run Faster Payments so that consumers are protected, and fraud is prevented from entering the system. In line with that vision, Pay.UK would be the appropriate body, in the long-term, to undertake the role of making, maintaining, refining, monitoring, and enforcing compliance with, comprehensive scheme rules that address fraud risks in the system.

The Panel supports this vision so long as Pay.UK has and gives appropriate voice to consumer representation on its Board and its advisory councils, and capacity to undertake consumer research as part of monitoring outcomes. It must also have sufficient authority over direct and indirect system participants and be able to move with sufficient pace to keep up with the pace of fraud.

**19. Do you have any other comments on the proposals in this consultation?**

We have welcomed all the PSR's efforts to reduce the risk of and harm caused by APP fraud and noted the recent improvement in both fraud and reimbursement rates – improvements that we believe can be directly attributed to the measures that have been put in place thus far. But more still needs to be done. Reducing the risk of consumer harm, ensuring consumer trust in, and eliminating crime from the payments system are all critical to UK consumers, the UK economy and UK society more widely. Given consumers' increasing dependence on Faster Payments *and* the rapidly increasing complexity of frauds being perpetrated, we would emphasise the urgency of the introduction of the proposed measures and strongly discourage the PSR from extending the proposed implementation timeline in response to industry demands. The industry has been on notice about APP scams for a significant period of time and consumers have been bearing the brunt of the costs involved. The severity of the harms being caused requires urgent remedy.

In parallel, the PSR, the FCA and others need to ensure urgent progress on consumer protection against faulty or non-delivered goods and services (para 4.13 of the consultation paper). This remains a significant imbalance between Faster Payments, including Open Banking payments and cards, and needs to be fixed before the industry is allowed to grow Open Banking payments as it currently intends. Even more urgently, the PSR needs to stop providers from interrupting consumers' card payment journeys and encouraging them to use account-to-account payments without giving clear information on the associated loss of protection. Such providers must make it clear that by choosing to use account-to-account payments, consumers will not be protected in the same way they would be using credit cards.

# FINTRAIL & RUSI



## PSR Consultation Paper

### Authorised Push Payment scams: Requiring reimbursement

#### **Introduction**

The Royal United Services Institute's (RUSI) Centre for Financial Crime and Security Studies (CFCS) and FINTRAIL welcome the Payment Systems Regulator's Consultation on Authorised push payment (APP) scams: Requiring reimbursement.

In 2022, the CFCS and FINTRAIL established a FinTech FinCrime Policy Group. This brings together senior FinTech compliance professionals to discuss the policy and regulatory issues they face and seek to find solutions to them.

This submission reflects the key themes from a discussion that the FinTech FinCrime Policy Group had with the Payment Systems Regulator (PSR) and other stakeholders on the topic of customer reimbursement and the views of research team members who have contributed their expertise to this submission. It does not represent the views of the individual member organisations, RUSI or FINTRAIL.

Any questions about this response should be directed to Kathryn Westmore, RUSI and Ciara Aitchison, FINTRAIL.

#### **Executive Summary**

It is widely agreed that much more action is needed across, but not limited to, the financial sector to tackle fraud in the UK, and drive down the rate of authorised push payment (APP) scams. The impact for affected individuals and organisations can be

devastating and destructive, and the financial services community has a pivotal role to play in ensuring it safeguards its customers. With increasing sophistication used by criminals to determine who, how, and where they target victims, financial services firms need to ensure they have the right set of tools and controls to deter and detect this activity.

It is also recognised that a number of initiatives across the industry needs to be deployed to collectively tackle this issue. The interdependencies of deliverables such as Confirmation of Payee and data sharing, along with increased consumer awareness are all needed in the effort to drive APP scams volumes down.

Furthermore, the responsibility does not sit with financial services firms alone, the role of big tech, telecommunications firms and social media companies as a key enabler of these crimes needs to be addressed. And while The Online Safety Bill sits outside the scope of this consultation, it is a key component in holding upstream polutter to account.

RUSI and FINTRAIL have not responded to all the questions in the consultation paper, we have selected those that reflect the Group's discussions and which we feel may have greater impact on the FinTech community.

## **Responses to individual questions**

*Question 2: Do you have views on the impact of our proposals on PSPs?*

It is clear that the CRM Code has not, to date, generated the expected outcomes. Its application has been inconsistent across participating payment services providers (PSPs) and it does not seem to have delivered a reduction in the level of fraud in the UK through the mooted incentivisation to increase investment in fraud prevention and detection controls.

We, therefore, broadly welcome the PSR's proposals and the benefit that customer reimbursement will have for consumers. We are, however, concerned about how elements of the PSR's proposal will be implemented, the proposed timescales and, in particular, the disproportionate impact on smaller PSPs, including FinTechs. The scale and complexity of the roll out of a scheme may present significant capacity, cost

and resource challenges for smaller PSPs. There should be consideration in adopting a phased roll out to allow smaller PSPs to successfully scale to meet scheme requirements. Furthermore, this model will likely result in material cost implications for smaller FinTechs, which could be a deterrent for new entrants and force existing firms out of the market. The impact this has on competition should be acknowledged.

Of particular concern is the potential knock-on effect on financial inclusion if the impact on FinTechs is disproportionate, resulting in them declining business or withdrawing services from certain customers, for example vulnerable or disadvantaged groups. There is also concern that one of the unintended consequences of the scheme is that certain banks or PSPs are 'blacklisted' by other financial institutions if it is felt that they do not have strong enough controls in place which will also have an impact on financial inclusion. This will further limit the competitiveness of the market, and again serve as a deterrent for new entrants.

We also note that a successful implementation of the scheme has a wider dependency on other initiatives, including Confirmation of Payee and work on data-sharing. The latter has a fundamental role in the proposed success of this scheme. For PSPs to work together to tackle APP scams, the ability to share data in a timely and efficient manner will be essential to facilitate decision making and risk-based controls. It is essential that FinTechs and smaller firms are actively engaged in those workstreams and their associated requirements.

The impact that the scheme would have on the facilitation of payments should be acknowledged. As implementation starts it will likely increase the friction seen across the payments process, particularly for higher value payments. This should be highlighted by the PSR as an accepted risk as associated complaint volumes may increase.

*Question 4: Do you have comments on our proposals:*

- *that there should be a consumer caution exception to mandatory reimbursement*
- *to use gross negligence as the consumer caution exception*
- *not to provide additional guidance on gross negligence?*

We are concerned about the PSR's position that no additional guidance will be provided on gross negligence and how it will be determined. At the very least, a framework or set of principles for establishing gross negligence across different fraud typologies would be beneficial. We are particularly concerned about the role that gross negligence will play in any disputes over the allocation of liability between the sending and receiving institution and the disproportionate burden that any such dispute will place on smaller organisations. Without a framework or set of principles, circumstances may likely arise that the sending and receiving PSPs have their own standards on what would constitute gross negligence which will prolong and exacerbate the dispute process.

*Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?*

*Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?*

We are in agreement that the FCA's definition of a vulnerable customer should be used. Having multiple definitions of vulnerability would become overly complicated and confusing both in terms of implementation and from a consumer's perspective. However, the FCA's definition of customer vulnerability remains vague and problematic. When it comes to fraud in particular, different types of vulnerabilities will impair decision making to a different extent. Vulnerability may also be different in relation to different types of fraud and will need to be assessed on a case-by-case basis.

It is not clear, however, at what stage in a scam vulnerability will be determined, how firms will seek to determine this and what will happen if there is a difference in view as to a customer's vulnerability between a sending and receiving PSP. It may also need to be considered that vulnerability may be dealt with differently across PSPs, and that the definition, particularly, in an economic downturn, is fluid and often will be circumstantial. There is an alternative that vulnerability may be dealt with on a case-by-case basis, and not an automatic reimbursement as proposed.

*Question 9: Do you have comments on our proposal not to have a maximum threshold?*

There may be merit in aligning the maximum threshold for reimbursement to the Financial Services Compensation Scheme and, therefore, setting the maximum threshold at £85,000. There may also be consideration in applying a cumulative threshold on the number of scams that an individual can claim for as in certain circumstances lends towards the position on gross negligence.

*Question 10: Do you have comments on our proposals that:*

- *sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement*
- *any time-limit should be set at no less than 13 months?*

It may be beneficial to have a tiered approach to timeframes based on different types of APP fraud. It may, for example, take longer than 13 months for a victim of investment fraud or romance fraud to realise that they have been defrauded. With other types of fraud, such as impersonation fraud, a shorter time limit may be reasonable.

*Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?*

*Question 14: Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?*

At this stage, the mechanisms for departing from the 50:50 allocation are not clear, nor how this will tie with other aspects of the model, e.g. gross negligence or vulnerability. For this to work effectively it should be a priority deliverable at the outset of the scheme to avoid confusion and prolonged dispute amongst PSPs,



resulting in unnecessary delays for customers and excessive costs for PSPs. There is also the concern that a lack of consistency in definitions and understanding of key concepts that underpin the scheme will disproportionately impact smaller firms, along with the resource constraints that they may experience to deal with these disputes.

If strength of controls is a factor in the allocation of liability, the PSR must consider how this will work in practice. What information will firms be equipped with to make that assessment independently? APP scam data will only be collected from the largest financial institutions, therefore what will form the basis of assessment for those not required to collect and publish this information? There is a concern of the risk of downward pressure on smaller PSPs to bear a disproportionate burden of reimbursement due to the perception that their controls are weaker.

To reduce the burden, it may be sensible to consider a minimum threshold for disputes, ensuring that the limited resources and time that some PSPs may have are allocated proportionally to deal with disputes that carry a higher value. The dependency on robust information is very acute in this area; PSPs will need the right mechanisms and support is in place to ensure that information is shared consistently and in a timely fashion. The need for real time, or near to real time, information sharing will be a vital component in driving down APP scams volumes and reducing associated disputes on liability should a claim be raised.

*Question 28: Do you have any other comments on the proposals in this consultation?*

At the heart of the PSR's proposals is the need for institutions to make effective risk-based decisions. That requires banks to have access to reliable and timely information to make decisions about customer behaviour and have appropriate controls in place, including the training of models. We have heard concern that there are still barriers to communicating between institutions, particularly smaller firms which are not part of existing industry initiatives.

Whilst we recognise that the scope of the PSR responsibilities is restricted to payment services activities, we strongly believe that the need to deal with 'upstream polluters'

is a fundamental component in the overarching success of driving down scam rates. The role of big tech, social media and telecoms in facilitation of scam activity should be further addressed. Their accountable and, perhaps, contributions to reimbursement should be factored in future discussions. Until the broader ecosystem comes together to fight this as a collective, the inroads that are needed to curtail this activity will not be enough.

Fire



**Objective** | To outline summary feedback on the PSR consultation on APP scams.

### 1 Background

Fire is a regulated provider of digital accounts in the UK & EU. Our accounts support a range of payment services – faster payments, Bacs, direct debits, open banking, FX and debit cards. We sell to SME, corporate and enterprise clients. The latter include some large financial institutions whom we enable to go to market with new and innovative products – such as open banking payment acceptance. We are a scaling business with 35 staff spread between our offices in London and Dublin.

Our founder and CEO, Colm Lyon, is a fintech and payments expert. Colm has built businesses, is an active investor in the sector and is very involved in industry groups. Colm represents non-bank financial institutions on the UK Finance Payments, Products and Services Board, the Strategic Participant Group for the NPA (Pay.UK), the Digital PSP Group and he is an active member of numerous other groups. Colm founded the Payments Ireland networking group and was chairperson of the Fintech & Payments Association of Ireland.

### 2 Our Most Worrying Concern

Notwithstanding that the PSR has outlined questions and set the agenda for the debate on APP scams, there is in our view a fundamental concern relating to the decision to implement a solution for APP scam in the heart of the UK payments clearing system.

Naturally we believe that APP scams should be addressed. However, we believe that the solution must not be implemented within the core clearing scheme for the industry – FPS and NPA in the future. To do so will inhibit the development of new payment applications, arrangements and agreements as these are layered over the scheme. We as investors and operators in the sector are concerned with this approach. There is also a broader industry risk that traffic will migrate from the core clearing systems to other “on us” style networks.

We would like to see regulators outline their (APP management) expectations for the development of payment arrangements built over the scheme. Such arrangements may then come to market, compete for customers, offer different choices and apply different rules for different scenarios. For example, certain payment arrangements may work best in customer present situations, others online, others in specific verticals or channels etc. Open banking payments could be considered a payment arrangement. This approach would both address the issue of APP scams while also developing a competitive and innovative payments market, particularly important in a post Brexit era.

### 3 Consultation process

With respect to the consultation process we note that the amount of time available and the bandwidth required to formulate a response is very limited – especially so for smaller firms. The process is taking place while other very significant consultation processes are also underway – particularly the JROC Open Banking process.

We are concerned that the voice of smaller firms is not as clearly represented as it might be. These consultation processes should recognise the broad makeup of the payments ecosystem.

Colm Lyon - fire.com – 9th Dec 2022

# Fraud Advisory Panel

## AUTHORISED PUSH PAYMENT (APP) SCAMS: REQUIRING REIMBURSEMENT

Issued: 25 November 2022

The Fraud Advisory Panel welcomes the opportunity to comment on the Payment Systems Regulator's consultation CP22/4 on authorised push payment scams: requiring reimbursement, published on 29 September 2022, a copy of which is available from this [link](#).

The Fraud Advisory Panel (the 'Panel') is the UK's leading counter fraud charity. We act as the collective voice of the counter fraud profession and provide practical support to more than 200 corporate and individual members. Our members come from a wide range of professions and sectors who are united in their determination to stop fraud.

We're happy to discuss any of our comments and to take part in all further inquiries on the issues we've highlighted in our response.

© Fraud Advisory Panel 2022

All rights reserved.

This document may be reproduced without specific permission, in whole or in part, free of charge and in any format or medium, subject to the conditions that:

- it is appropriately attributed, replicated accurately and is not used in a misleading context;
- the source of the extract or document is acknowledged and the title and Fraud Advisory Panel reference number are quoted.

Where third-party copyright material has been identified application for permission must be made to the copyright holder. For more information email: [info@fraudadvisorypanel.org](mailto:info@fraudadvisorypanel.org)

## POTENTIAL IMPACT OF PROPOSALS

### Question 1

Do you have views on the impact of our proposals on consumers?

1. We are pleased to see further consideration given to the implementation and contents of the CRM Code. We agree there needs to be revision of the application of the CRM Code. At present there is too little protection for customers and too much inconsistency in approach between Payment Service Providers ('PSPs'). There is a tendency for PSPs to rely too heavily on the possibility of avoiding repayment. Customers are often challenged about not following effective warnings or gross negligence, thereby leading to either a percentage refund or no offer of a refund under the Code, which was not the intention. We understand that the CRM Code will run in parallel with the PSR liability split proposal, and that the PSR liability split proposal is intended to supersede the CRM Code.
2. It is our opinion that the discretion provided to PSPs has resulted in inconsistent outcomes for customers. We therefore fully support the need for a revision to the Code to give customers consistent protection and a clear understanding of what is expected of them and what they can expect from a PSP.
3. We agree that the payment chain is likely to take longer as a result of increased customer protection, but this is a necessary evil to reduce consumer detriment. PSPs should work on ways of improving the balance between speed and consumer protection.
4. In relation to vulnerable people, we agree that it would not be ethical or sensible to restrict services. We suggest instead that PSPs ensure they identify their vulnerable customers and give them effective warnings that are meaningful and actionable to make it more likely these customers will check the transaction they intend to make. It is likely such customers will appreciate a human touch and consider it good service.
5. It is noted that consumers are still limited to individuals, micro-enterprises and charities. More active engagement with those customers outside of the scope of the CRM Code to educate them on the types of APP fraud they are most likely to fall victim to, how they can prevent it, and what they can do to protect themselves (including, for example, insuring themselves against this type of loss) would be helpful.

### Question 2

Do you have any views on the impact of our proposals on PSPs?

6. We agree strongly that the proposed measures provide better fraud education initiatives and controls for customers. The design of the proposals will ensure that recipient banks share the costs of reimbursement more equally and should incentivise them to do more to stop fraud.

7. We also welcome the proposal to split costs between both sending and receiving PSPs.
8. We consider that there may be an increase in first-party fraud due to the mandatory nature of the reimbursement.
9. We also suggest that banks need to collaborate more and industry bodies, such as Pay UK and UK Finance, should help facilitate data-sharing.

## PART A: THE REIMBURSEMENT REQUIREMENTS

### Question 3

Do you have views on the scope we propose for our requirements on reimbursement?

10. We agree that the CRM Code should cover all Faster Payments and CHAPS transactions as well as payments where the sending and receiving PSPs are part of the same group.
11. We consider that large companies should have their own checks and procedures in place (a control framework to manage fraud risk) but that some commitment towards assisting with education would be welcomed. Larger companies outside the scope of the CRM Code could be advised as to what good governance looks like and encouraged to explore insuring against the risk.

### Question 4

Do you have comments on our proposals:

- that there should be a consumer caution exception to mandatory reimbursement;
- to use gross negligence as the consumer caution exception; and
- not to provide additional guidance on gross negligence?

### There should be a consumer caution exception to mandatory reimbursement

12. We agree that unqualified reimbursement is unfair on PSPs and would in effect allow customers to abdicate any responsibility to follow effective warnings. We also agree with the proposal to keep the threshold high (discussed further below). The premise in the report that consumers will take no less care just because there is greater chance of reimbursement seems realistic. The report rightly highlights that '*people do not want to be scammed and falling victim is distressing*'. In addition, many consumers are not aware of the existence of the CRM Code until they are a victim of a scam.
13. We consider that there should be an exception or customers may think there is no need to protect themselves, but this should be a very high bar if using gross negligence (i.e., the '*significantly careless*' level of fault).



### **Use of gross negligence as the consumer caution exception**

14. The 'gross negligence' threshold is a sensible one, provided PSPs do not overuse the opportunity to seek to decline refund requests (or to reduce the sum refunded) on the basis of gross negligence.
15. In our view the FCA Guidance risks not setting the bar high enough. When seeking to offer guidance on what 'gross negligence' is, it turns instead to softer language by defining it as 'a very significant degree of carelessness'. Careless implies a lower standard than negligence, when in fact, the negligence itself should be 'gross'. Guidance on the difference between simple 'negligence' and 'gross negligence' would be more helpful in ensuring the high bar intended is set in practice.

### **Not to provide additional guidance on gross negligence**

16. Paragraph 4.30 of the consultation paper recognises that the lack of definition of gross negligence may lead to a degree of uncertainty in the application of the concept which in turn may lead to disputes. We agree that this is a very real risk; but if we can identify it, we should consider what more can be done to avoid it.
17. We appreciate the reluctance to provide a definition which would create 'a tick box' exercise, but where a principle needs to be applied there also needs to be a set of criteria to be met. We do not think this should prevent attempts to provide greater clarity over what does and does not constitute gross negligence.
18. Further, given the manner in which decisions as to gross negligence are taken in practice, it would be helpful to ensure standardised guidance is given to firms so that PSP case workers (across all PSPs) dealing with reimbursement requests have a common understanding of the principle of gross negligence to avoid inconsistency of outcomes for consumers.
19. In addition, it may be worth considering if the Financial Ombudsman Service ('FOS') could have additional sanctions made available to them in order to hold PSPs to account when they have made an incorrect assessment of 'gross negligence'. This could be by way of additional financial penalties for PSPs/compensation for consumers, where claims are initially rejected by a PSP on this basis and where the FOS later find against the PSP/in favour of the consumer. This may incentivise PSPs to ensure the rejection (or reduction) of a claim on the grounds of gross negligence is an exception.
20. Examples of findings of 'gross negligence' by FOS could be set out by PSPs to their customers so to get a sense of the expectation on customers and PSPs.

#### **Question 5**

Do you have any comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?

21. We agree with this approach – which should not be onerous for PSPs – as gross negligence should be an exceptional basis for rejection, so circumstances in which the PSPs need to move on to consider whether a consumer was ‘vulnerable’, should be rare.
22. However, the key to the effectiveness of this exception to the gross negligence rule, is who decides ‘vulnerability’. As touched upon in our answers above, decision-makers are likely to be claims handlers at the PSPs who will require adequate guidance and training on what constitutes a ‘vulnerable customer’. There is already a difference in definition between the CRM Code and the FCA’s definition. It would be helpful to know if the FCA’s definition will be used, as suggested. As is observed in market commentary, ‘vulnerable’ can be young, elderly, a person with learning disabilities, language difficulties etc – clarity is needed on what is the adopted universal assessment to accept a customer is ‘vulnerable’. Without this clarity of understanding of ‘vulnerability’ there is a significant risk of inconsistent outcomes from consumer to consumer and between PSP and PSP.
23. PSPs who fail to identify a consumer as vulnerable, thereby denying them of a refund to which they would be entitled, should risk additional penalties/compensation awards being made against them by the FOS.

#### **Question 6**

Do you have any comments on our proposal to use the FCA’s definition of a vulnerable customer?

24. See our response to Question 5.

#### **Question 7**

- Do you have comments on our proposals that:
- sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement
- any ‘excess’ should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?

#### **Sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement**

25. As the consultation paper highlights, the approach is consistent with other reimbursement schemes, and we accept that it allows some risk sharing between PSPs and consumers.
26. We believe that £35 will certainly be charged by the banks, so will be effectively a fraud levy.

#### **Any ‘excess’ should be set at no more than £35**

27. A £35 ‘excess’ limit is consistent with other reimbursement schemes.

### **PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply**

28. The current wording of the report suggests the exemption of requiring an excess in the case of vulnerable consumers will be discretionary. It is not clear if this means the exemption will be discretionary on a case-by-case basis, or as a matter of policy. A PSP could decide never to offer an excess exemption.
29. The same potential issues with regards to classification and definition of a vulnerable consumer (as discussed above) also apply.
30. To balance the interests of those involved, if a vulnerable customer is refunded despite a finding of ‘gross negligence’, it would be reasonable for the £35 levy to apply nevertheless.

#### **Question 8**

- Do you have comments on our proposals that:
- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?

### **Sending PSPs should be allowed to set a minimum claim threshold**

31. We agree that a minimum figure of £100 is reasonable, given that APP fraud below £1,000 accounts for just 7% of such fraud.
32. We understand the reasoning behind the suggestion of a minimum threshold and agree these lower value APPs are likely to be harder for PSPs to detect and prevent. Further, we accept that PSPs could be inundated with small requests and that the administrative costs of dealing with high-volume low-value refund requests would likely to be disproportionate.

### **Any threshold should be set at no more than £100**

33. Agreed. See our comments above.

### **PSPs should be able to exempt vulnerable consumers from any threshold they set**

34. As indicated above, additional protection for vulnerable consumers is welcome via the exemption of the £100 minimum threshold for vulnerable consumers. The same potential issues with regard to classification and definition of a vulnerable consumer, as discussed above, would apply.

#### **Question 9**

Do you have comments on our proposal not to have a maximum threshold?

35. We agree that there are good reasons not to have a maximum threshold. We share the views expressed in the consultation paper that the larger the payment, the more stringent the counter-fraud measures the consumer should expect to be in place to prevent an APP occurring.
36. It is noted that most APP frauds fall well within TSB's £1,000,000 maximum threshold. The £30,000 threshold under section 75 of the Consumer Credit Act is woefully low in this area where total loss to consumers is regularly seen to be higher. We consider too many consumers would find themselves excluded from full reimbursement.

#### **Question 10**

Do you have comments on our proposals that:

- sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
- any time-limit should be set at no less than 13 months?

#### **Sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

37. We agree that PSPs ought to be able to set a time limit for claims but consider time should not start to 'run' for the purposes of bringing a claim for reimbursement until the date of discovery of the APP (or the date by which the consumer should reasonably have become aware). This would be consistent with:
  - a. the basis of the setting of a time limit by the Financial Ombudsman, and
  - b. the basis of calculating limitation for commencing court proceedings for fraud claims, in accordance with s.32 of The Limitation Act 1980.

#### **Any time-limit should be set at no less than 13 months**

38. We disagree that 13 months from the date of the transaction is a reasonable time limit.
39. It is far preferable to have consistency with both the Financial Ombudsman and the Limitation Act 1980 which would see a time limit of 6 years from the date when the consumer knew, or ought reasonably to have become aware.
40. In our experience a significant number of APPs are not discovered within 13 months of the transaction. Investment fraud is one example, where the fraud is not uncovered until after the investment is due to mature. This can often be several years after the transfer has occurred: when the investment fails to mature and the victim realises the investment was a scam.
41. This would also resolve the conundrum of a consumer having to complain to the FOS as they did not discover the fraud within the time limit and asking the FOS to order the PSP to reimburse outside of the time limit. This could lead to friction between the FOS

and PSP's and the FOS being inundated with claims that could easily have been dealt with by the PSP if it was reported within the time limit.

42. We note that FOS maximum award is £355,000. Limiting any claim to 13 months effectively means that those customers who have lost more than this sum are having a threshold imposed on them.

#### Question 11

Do you have comments on our proposals that:

- the sending PSP is responsible for reimbursing the consumer
- reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?

#### The sending PSP is responsible for reimbursing the consumer

43. We agree with the suggestion that given the direct nature of the relationship between the consumer and the sending PSP, the sending PSP should be responsible for reimbursing the consumer.

#### Reimbursement should be made as soon as possible, but no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence

44. Creating an obligation to reimburse a consumer within 48 hours of their claim being made looks positive, but we feel it is unrealistic. However, the consultation is right to consider (at question 12) the standard a PSP has to reach to justify withholding reimbursement on the grounds of first-party fraud or gross negligence. We address these considerations below. Given that banks may sometimes submit suspicious activity reports 45 days or more after a suspicious transaction, a 14 – 28-day period to reimburse seems more realistic, though we note that card refunds for fraud are typically made between 3–7 days.

#### Question 12

What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?

45. The standard of evidence for first-party fraud should be that there is a prima facie case, on the balance of probability (i.e., the evidence suggests that it is more likely than not that the consumer seeking the reimbursement was a party to the fraud). This would align the standard of evidence with the civil justice system's standard for bringing a claim.
46. Setting a standard of evidence for gross negligence is more difficult, because the report fails to provide any definition of gross negligence. We are concerned that a delay in

reimbursement on the grounds of suspicion of gross negligence will lead to too many claims being delayed for this reason. Very clear guidance on what will be considered gross negligence should be provided, especially if it is to be used as a basis to investigate and delay reimbursement.

47. We consider that the time periods for investigating first-party fraud and gross negligence can be different. The standard of evidence to be satisfied of first-party fraud may well take longer to gather, as it may be more likely to require liaising with recipient banks to identify links between parties. As such, a period of no longer than 3 months seems reasonable. This aligns with the court's expectation in 'complex' claims pursuant to the Civil Procedure Rules Practice Direction for Pre-Action Conduct and Protocols. An allegation of gross negligence is likely to be subjective and unique to that consumer's personal conduct during the course of the transaction. As such, it should be quicker and more straight forward to investigate. Any additional information should be requested from the consumer within 7 days and a decision to reimburse should be provided within 21 days of the PSP's receipt of that information. The PSP should be discouraged from making multiple requests for information and a long stop of 56 days on a final decision should be imposed.
48. During any further period of investigation, the consumer seeking reimbursement should have the opportunity to engage with the investigation and an opportunity to allay concerns and/or present further evidence to support their claim. The consumer should receive a short weekly or fortnightly update on what steps have been taken since the last update, and what further steps are required before a decision to reimburse can be taken. The consumer should also receive detailed reasoning as to why they are considered to be grossly negligent by the PSP if reimbursement is to be refused.

### **Question 13**

Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

49. We consider the proposal for a 50:50 default allocation of reimbursement between the sending and receiving PSPs to be a positive step forward.
50. It gives receiving PSPs more incentive to prevent their accounts being used as mule accounts / repositories for fraudulent receipts. The Fraud Advisory Panel has previously encouraged the introduction of greater shared responsibility which this default allocation would appear to address.

### **Question 14**

Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?

51. We recognise that in some cases it will be easier for receiving PSPs to identify the fraud and freeze the incoming payment where it seems unusual given the history of the account, or the nature of the account holder.

**Question 15**

Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?

52. The idea of seeking to include multi-generational scams within the reimbursement model is welcome and offers consumers a greater degree of protection than simply with APPs that occur through a single transactional journey. At present, our experience has been that it is unclear whether each respective PSP will consider reimbursement of a multi-generational scam leading to unpredictability and inconsistency of outcome. Clearer guidance on whether they are intended to be included is welcome.
53. Under the 50:50 default allocation provisions, it would appear to be the intention for PSPs to be able to mediate a variation of the default liability split and this would lend itself well to multi-generational APPs which are more likely to be easier to detect by the different PSPs involved.
54. We see no reason why a split between all PSPs within the chain cannot be negotiated, reflecting their respective (missed) opportunities to detect the fraud.

**Question 16**

Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?

55. A 50:50 default allocation of repatriated funds between sending and receiving PSPs seems fair on the basis that liability has been split in the same way.

**Question 17**

Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?

56. Not comment.

## **PART B: HOW WE PROPOSE TO IMPLEMENT OUR REQUIREMENTS**

57. We have no comments to make in respect of questions 18 to 28 contained in Part B of the consultation.

# Hargreaves Lansdown



# **PSR CP22-4: AUTHORISED PUSH PAYMENT (APP) SCAMS – REQUIRING REIMBURSEMENT**

## Consultation response

25 November 2022

## Introduction

This response is made on behalf of Hargreaves Lansdown (HL), the UK's largest direct-to-investor savings and investment service. We support more than 1.75 million clients<sup>1</sup>, who trust us with £122.7 billion<sup>2</sup>.

Our purpose is to empower people to save and invest with confidence<sup>3</sup>. We want to provide a lifelong, secure home for people's money that offers great value, an incredible service and makes their financial life easy.

We offer five core services:

- A financial platform to enable investors to transact and manage their wealth and securities. This business is referred to as HL Asset Management.
- An asset management service of HL funds – this business is referred to as HL Fund Management.
- HL Workplace pension scheme.
- Financial advice delivered via HL advisers.
- In 2018, we also launched [Active Savings](#), an online cash savings platform that lets savers move money easily between partner banks and building societies to help their money work harder without the hassle.

We welcome the opportunity to respond to this Consultation Paper. If you have questions about our responses, please contact 

---

<sup>1</sup> As at 30 September 2022.

<sup>2</sup> Further information is available via our [website](#).

<sup>3</sup> [HL Purpose and Strategy](#).

## Answers to Questions

### 1. Do you have views on the impact of our proposals on consumers?

We want consumers to be more resilient to scams and fraud. These proposals will arguably have a positive impact for consumers, providing reassurance that should they be a victim of an Authorised Push Payment (APP) scam, they are protected. Specific proposals to support consumers in vulnerable circumstances are also welcome, given the heightened risk of such individuals falling victim to scams<sup>4</sup>. As part of a wider package of regulatory and legislative efforts to reduce instances of fraud (including extending Confirmation of Payee requirements<sup>5</sup>; changes under the Online Safety Bill<sup>6</sup>; publication of APP performance data<sup>7</sup>; and improved intelligence sharing<sup>8</sup>), coupled with educational initiatives (e.g., FCA ScamSmart and UK Finance's 'Take 5' initiative), this proposal should support a reduction of the impact of fraud on Consumers.

However, whilst we are supportive of measures to improve the protection afforded to consumers, and whilst we acknowledge the PSR's comments in Box 2, we believe that mandatory reimbursement could lead to increased consumer complacency, potentially reducing the need for consumers to take appropriate responsibility for their decisions – which runs counter to one of the regulatory principles that consumers should take responsibility for their decisions<sup>9</sup>. Although it relates primarily to fields of safety, the Peltzman Effect<sup>10</sup> suggests that increasing protection results in greater risk-taking behaviour; it is possible that mandatory reimbursement could lead to an increase in risk-taking behaviour by consumers when it comes to APP fraud. Whilst we cannot point to academic studies specific to financial behaviours, we nonetheless argue that it is a potential risk. Further, given that explicit fraud warnings to consumers do not appear to deter fraud<sup>11</sup>, it is difficult to foresee how mandatory reimbursement would encourage consumers to exercise higher levels of due caution than they do at present (if payment behaviour patterns align with behaviour adaptations based on perceived levels of risk).

Fraudsters may also exploit these changes. If fraudsters are aware that consumers 'cannot lose' because PSPs are required to reimburse consumers, these proposals could have the unintended effect of increasing instances of fraud (albeit reducing the cost or loss to consumers), which could undermine the PSR's desired outcome of fewer APP scams<sup>12</sup>. For example, fraudsters may be able to reassure potential victims that they will receive their money back if there are issues with delivery of goods (as in the case of APP Purchase Fraud), or otherwise reassure potential victims that they will receive their money back (as for other APP scams). This is also relevant for 'repeat' instances of fraud, where fraudsters may commit fraud multiple times via a single victim, because they are then known to the fraudster as someone through whom APP fraud can be committed.

---

<sup>4</sup> See Paragraph 2.4 (g) of [FG21/1](#).

<sup>5</sup> See [PSR PS22/3](#).

<sup>6</sup> Chapter 5 of the Online Safety Bill places requirements on user-to-user services and search engines with respect to fraudulent content.

<sup>7</sup> See Paragraph 1.12 (1) of [PSR CP21/10](#) for an explanation of Measure 1.

<sup>8</sup> See Paragraph 1.12 (2) of [PSR CP21/10](#) for an explanation of Measure 2.

<sup>9</sup> FSMA Section 3B (1) (d), as referenced on the [FCA's website](#).

<sup>10</sup> Also referred to as the risk compensation effect, this suggests that when safety measures are implemented, people's perception of risk decreases.

<sup>11</sup> Paragraph 405 of the [House of Lords' Fraud Act 2006 & Digital Fraud Committee report](#), 12 November 2022.

<sup>12</sup> Paragraph 2.11 of PSR CP22/4.

That said, we do understand that victims' shouldering of responsibility can lead to 'victim shaming', which results in under-reporting of fraud<sup>13</sup>, and we do absolutely recognise the importance of reducing the impact of APP fraud on victims.

## 2. Do you have views on the impact of our proposals on PSPs?

Whilst it is arguable that an increase in fraud compensation costs will incentivise firms to enhance fraud controls, from a competition perspective, mandating reimbursement could have a disproportionate impact on smaller firms whose anti-fraud controls may not be as strong as larger firms. The dynamic nature of fraud means that fraudsters may seek to move to smaller PSPs where fraud can more easily be perpetrated – we note the PSR's observations in Paragraph 5.22 that non-SD10 PSPs accounted for 20% of Faster Payments transactions in 2021 but received 50% of APP scam payments from SD10 PSPs<sup>14</sup>. Extending COP requirements may reduce this effect<sup>15</sup>, as part of the broader package of APP remedies.

We recognise that Measure 2 should improve intelligence sharing between firms, on a real-time basis; improved intelligence sharing should result in more effective detection, and therefore prevention, of fraudulent activity. However, we would note that any build requirements may impose costs on PSPs, which may be disproportionate for smaller PSPs.

Where payments are delayed due to investigations, this could lead to an increase in complaints from consumers. Firms will need to ensure a consistent and fair approach to dealing with such complaints. The Financial Ombudsman Service should also be involved, again to ensure a consistent approach.

## 3. Do you have views on the scope we propose for our requirements on reimbursement?

We note that the proposals align to the definition in the Financial Services and Markets Bill s.62 (2), and therefore covering any payment over the Faster Payment Scheme (FPS). Given that 97% of APP scams are made via FPS<sup>16</sup>, it is logical to focus on FPS.

We note that all APP frauds would be in scope<sup>17</sup>; given that existing arrangements have been deemed to provide insufficient protection for consumers (i.e., the existing requirements under the CRM code have been determined as providing too low a level of reimbursement and protection<sup>18</sup>), the bar for, or definition of, gross negligence will need to be clarified. For example, what would happen in repeat instances of fraud (e.g., where a victim is repeatedly targeted by multiple fraudsters within a fraud network)? Would ignoring warnings constitute "*gross negligence*"? In this regard, please see our response to Question 4.

For harder-to-detect first party fraud, this could open a new window – specifically, individuals working with other fraudsters and sharing in the proceeds of fraud. For example, a multi-generational scam involving an individual making a payment, claiming APP Fraud

---

<sup>13</sup> This is highlighted throughout the House of Lords' 12 November 2022 Fraud Act 2006 & Digital Fraud Committee report but is particularly clear at Paragraph 361.

<sup>14</sup> Paragraph 5.22, CP22/4.

<sup>15</sup> See footnote 5.

<sup>16</sup> [UK Finance Annual Fraud Report – 2022](#), Page 68.

<sup>17</sup> Paragraph 4.11 of PSR CP22/4.

<sup>18</sup> Paragraph 1.11 of PSR CP22/4.

(and receiving mandatory reimbursement), receiving a payment from the fraudster later as a reward for participating in the fraud.

**4. Do you have comments on our proposals:**

- a. *That there should be a consumer caution exception to mandatory reimbursement.*
- b. *To use gross negligence as the consumer caution exception.*
- c. *Not to provide additional guidance on gross negligence?*

In line with our comments in Question 1 concerning consumer responsibility for decisions, we agree that there should be a consumer caution exception to mandatory reimbursement. We also agree that this should align with the gross negligence definition.

However, we note that gross negligence must be a “*high bar*”, with customers having to have shown a “*very significant degree of carelessness*”. In this regard, we note the House of Lords’ Fraud Act 2006 and Digital Fraud Committee report, which cites evidence that consumers ignore warnings and recognisable anti-fraud campaigns, such as UK Finance’s ‘Take 5’ campaign<sup>19</sup>. If consumers have an awareness of campaigns such as ‘Take 5’ or educational materials provided by their PSP but can ultimately ignore warnings and still proceed with fraudulent transactions, it is arguable that further guidance on what constitutes gross negligence would be required, particularly if current approaches to APP are deemed to be insufficiently effective at reducing APP scams<sup>20</sup>. This is arguably important to achieve consistency across different multiple stakeholders (including PSPs and the Financial Ombudsman Service, amongst others), and to aid investigations within the 48-hour window proposed at Paragraph 5.5.

**5. Do you have comments on our proposal to require reimbursement of vulnerable customers even if they acted with gross negligence?**

As the PSR have acknowledged in Annex 3, vulnerable customers may be at greater risk of becoming victims of fraud. Further clarity may be helpful in this space – for example, would this only apply if a firm was aware of vulnerability before the fact, or also if a consumer notified a vulnerability at the point of requesting reimbursement? Should all customers in vulnerable circumstances be treated the same?

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

We think that consistency of definitions is helpful for firms and recognise that the FCA have issued comprehensive guidance on their expectation for the treatment of vulnerable customers<sup>21</sup>.

**7. Do you have comments on our proposals that:**

- a. *Sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement.*
- b. *any excess should be set at no more than £35.*
- c. *PSPs should be able to exempt vulnerable consumers from any 'excess' they apply.*

We do not disagree that sending PSPs should be allowed to apply an excess in the manner proposed by the PSR, and that PSPs should be able to exempt vulnerable consumers from

---

<sup>19</sup> Paragraphs 402 to 406 of the [House of Lords’ Fraud Act 2006 & Digital Fraud Committee report](#), 12 November 2022.

<sup>20</sup> Paragraph 1.11 of PSR CP22/4.

<sup>21</sup> [FG21/1 – Finalised Guidance for firms on the fair treatment of vulnerable customers](#)

this excess. However, we would observe that optionality could lead to inconsistent treatment of vulnerable consumers by different PSPs (i.e., PSPs may exempt vulnerable consumers). Further clarity on how this optionality would apply in practice would be welcome. Whilst we recognise the PSR's comments that a percentage-based excess would be inappropriate<sup>22</sup>, it is arguable that a fixed excess of £35 may not amount to a sufficient incentive for consumers to exercise due caution with larger payments.

We wonder whether a combination of a fixed and percentage value may be fairer – for example, setting the excess as the lower of £35 or X%. Such an approach could arguably reduce the burden on victims of smaller APP frauds, for whom the small amount may be significant; for example, a £35 excess is 35% of £100, but 3.5% of £1,000.

**8. Do you have comments on our proposals that:**

- a. *Sending PSPs should be allowed to set a minimum claim threshold.*
- b. *Any threshold should be set at no more than £100.*
- c. *PSPs should be able to exempt vulnerable consumers from any threshold they set.*

We agree that sending PSPs should be allowed to set a minimum claim threshold, and that that threshold should be no more than £100. We agree that PSPs should be able to exempt sending PSPs from this threshold but reiterate our comments in Question 7 that the voluntary nature of such an obligation could lead to inconsistent treatment of vulnerable consumers across different PSPs.

**9. Do you have comments on our proposal not to have a maximum threshold?**

We have no comments on this proposal, other than to reiterate the potential impact for smaller PSPs where volumes and values of mandatory reimbursements are significant.

**10. Do you have comments on our proposals that:**

- a. *Sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement?*
- b. *any time-limit should be set at no less than 13 months.*

This is reasonable, bearing in mind the 13-month limit under the Payment Services Regulations 2017<sup>23</sup>.

We would observe that some products into which fraudsters encourage payments could have a maturity period which exceeds the 13-month limit. Consumers in these circumstances could therefore receive different treatment; however, we do also recognise that there must be a 'line drawn' somewhere.

**11. Do you have comments on our proposals that:**

- a. *The sending PSP is responsible for reimbursing the customer.*
- b. *Reimbursement should be ASAP, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?*

Whilst we understand the importance of protecting victims of fraud, 48 hours is a short amount of time to conclude any investigations. Fraud can take a significant amount of time to investigate, particularly where fraud is 'multi-generational' or complex. Whilst we

---

<sup>22</sup> See Footnote 31 of PSR CP22/4.

<sup>23</sup> See Paragraph 8.184 of the [FCA's Payment Services and Electronic Money Approach document](#).

recognise that the intention of these proposals is to protect consumers by requiring reimbursement within 48 hours, with PSPs conducting investigations behind the scenes after a consumer has been reimbursed, we reiterate that this could have a significant impact on the resources of smaller PSPs. Finally, we would encourage the PSR to consider requiring reimbursements within a specified number of business days; this may support smaller PSPs who are not open for business 7 days per week (in this regard, we point to Paragraph 8.292 of the FCA’s approach document<sup>24</sup>).

**12. What standard of evidence for gross negligence of FPF would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Please see our comments on further guidance for gross negligence in Question 4. We have no views on the length of time afforded to PSPs to investigate but suggest that the PSR may wish to consider aligning with complaints timelines in DISP 1.6<sup>25</sup>.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

No comments, other than those raised in Question 2 regarding the impact on smaller PSPs.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

It will be important for terms defined by Pay.UK to be fair, such that there is consistency across PSPs irrespective of size: smaller firms should be just as able to negotiate alternative terms as larger firms.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

The role of indirect participants will vary depending on business model. For example, such firms may only allow withdrawals to nominated accounts, with controls surrounding a change to those nominated accounts. If the requirements are implemented as consulted upon, clarity will be needed to identify who the ‘sending’ PSP is – for example, using Figure 1 below as a hypothetical case, should it be the indirect PSP (PSP 1), who made the first payment at the customer’s request, to an account in their own name? Or should it be the receiving PSP (PSP 2), who is subsequently instructed by the customer to send the payment to the fraudster’s PSP (PSP 3)?

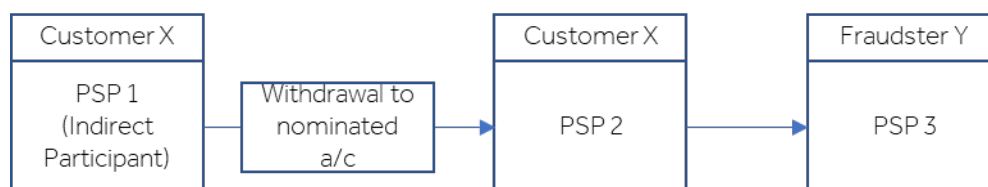


Figure 1: Screenshot

<sup>24</sup> See Paragraph 8.292 of the [FCA’s Payment Services and Electronic Money Approach document](#).

<sup>25</sup> [FCA Handbook – DISP 1.6](#).

Our current interpretation is that if the rules are implemented as proposed, it would be the latter (i.e., PSP 2 would be the 'first' PSP, and therefore responsible for reimbursing the customer). Thus, a customer sending the proceeds of investment sales from a platform which is an indirect PSP to their nominated account, before sending on to a fraudster, would not be in scope for mandatory reimbursement: PSP 2 and PSP 3 would bear accountability for reimbursement, and PSP 1 would bear no accountability.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

We have no specific comments for this question. However, we believe that amounts of repatriation should match the split agreed between firms for reimbursement – thus, if firms agree to depart from a 50:50 split of reimbursement, any repatriation of funds should match the agreed split for reimbursement.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We have no comments for this question.

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

We have no comments for this question.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

We have no comments for this question.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We have no comments for this question.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

We have no comments for this question.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

We have no comments for this question.

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We have no comments for this question.





**24. Do you have views on the best option for short-term enforcement arrangements?**

We have no comments for this question.



**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

If the PSR wishes to proceed as consulted, it is arguable that a direction is the optimum method to apply requirements to indirect participants. Although Pay.UK could amend scheme rules to apply to indirect PSPs, this could take time to achieve<sup>26</sup>, potentially impacting the delivery of APP reimbursement requirements in the short-term.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

We believe that directing PSPs makes more sense, as IAPs will not have a direct relationship with the fraud victim.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

We have no comments for this question.

**28. Do you have any other comments on the proposals in this consultation?**

We have no comments for this question.

---

<sup>26</sup> Paragraph 7.33 of PSR CP22/4.



# Innovate Finance

## PSR Consultation Paper

### 'Authorised push payment scams: Requiring Reimbursement' (CP22/4)

#### Innovate Finance response

#### **About Innovate Finance**

Innovate Finance is the independent industry body that represents and advances the global FinTech community in the UK. Innovate Finance's mission is to accelerate the UK's leading role in the financial services sector by directly supporting the next generation of technology-led innovators.

The UK FinTech sector encompasses businesses from seed-stage start-ups to global financial institutions, illustrating the change that is occurring across the financial services industry. Since its inception following the Global Financial Crisis of 2008, FinTech has been synonymous with delivering transparency, innovation, and inclusivity to financial services. As well as creating new businesses and new jobs, it has fundamentally changed the way in which consumers and businesses are able to access finance.

#### **Introduction and key points**

Innovate Finance welcomes the opportunity to respond to the Payment Systems Regulator's ("PSR") Consultation Paper ("CP22/4") which sets out proposals that will require Payment Service Providers ("PSPs") to provide mandatory reimbursement to consumers who lose money to Authorised Push Payment ("APP") scams. Innovate Finance recognises that APP fraud presents a significant and growing challenge for the payments industry<sup>1</sup>, and that it is important for consumers to be adequately protected in the face of increasingly sophisticated APP scams. Ultimately, consumer trust and safety is paramount if innovation and competition is to flourish in the payments sector.

Our members support the PSR's intended aim of providing a fair level of protection to consumers who fall victim to APP scams, and they welcome the introduction of a consistent

---

<sup>1</sup> UK Finance reported that £583.2 million was lost to APP scams in 2021.

approach to consumer protection across the industry. However, by creating an unfunded and uncapped mandatory reimbursement obligation with an extremely high bar for exceptions, our members are concerned that the liability regime will lead to a number of unintended consequences that will be detrimental to consumers and PSPs. In particular, our members are extremely concerned about the potentially devastating impacts on the FinTech sector and the repercussions for innovation and competition in the payments market, as well as the international competitiveness of the UK.

The PSR's mandatory reimbursement proposals are the first of its kind in the world. Hence, a careful, iterative roll out is necessary in order to ensure the UK remains the most attractive place in the world to start and scale a FinTech business. A balance must be struck so that consumers are protected from losing life-changing sums of money while innovation in digital payments can continue to grow with appropriate incentives being applied to all participants in the digital economy in order to reduce fraud.

In reviewing the consultation paper and producing our response, we have consulted with a range of Innovate Finance members that provide payment services, including neobanks, and others who are indirectly impacted or may fall within the scope of this liability framework in the future.

Innovate Finance would be pleased to discuss this response in more detail with the PSR and/or facilitate discussions directly with our members.

## Consultation Paper questions and responses

### Question 1: Do you have views on the impact of our proposals on consumers?

We outline views on:

- Reimbursement levels and what more can be done to reduce the amount of consumers falling victim to APP scams in the first place; and
- Impact on consumers' user experience as a result of the PSR's proposals.

#### ***Reimbursement levels and what more can be done to tackle APP fraud at source***

The APP scam landscape is complex. Both the PSR and the Lending Standards Board ("LSB") agree that there are eight types of APP scams; each with different characteristics, typologies and refund rates. Our members recognise the significant impact (not only financial) of these APP scams on victims. Our members are supportive of providing a fair level of protection for consumers who, notwithstanding reasonable steps to protect themselves, fall victim to APP scams, and they welcome the introduction of a consistent approach to consumer protection across the payments industry.

We expect that the liability model will lead to a material uptick in reimbursement levels (we unpack the ramifications of this for the FinTech sector in more detail, below). But the PSR's liability framework has remediation rather than prevention at its core, as we argued in our response to CP21/10. So, APP fraud victims will in most cases receive reimbursement; however, our members do not consider that this will actually reduce the amount of people falling victim to APP scams in the first place, and believe that an uncapped, near strict-liability regime is likely to increase APP fraud volumes by creating moral hazard and providing an incentive for first-party fraud.

Collectively, FinTechs and incumbents have invested billions in financial crime systems and strategies in order to tackle all types of fraud at source, but APP scammers are sophisticated and they are exploiting weaknesses outside of PSPs' control to trick consumers. The FinTech and wider banking sector recognises that more can be done to enhance their financial crime controls, systems and strategies; however, in order to truly reduce the number of victims of APP scams, there needs to be a joined-up, public-private sector approach to tackling APP

fraud at source<sup>2</sup>. The recent report from the National Audit Office<sup>3</sup> regarding the Government's progress in combating fraud underlines the need for a joined-up, public-private sector approach to be developed at pace.

Our members urge the PSR to engage with counterparts in the Home Office, Financial Conduct Authority ("FCA"), law enforcement and industry to help shape a future fraud prevention strategy. Our members stand ready to support the PSR in any way they can.

Lastly, we wish to stress the essential role of the Online Safety Bill in the wider context of addressing APP fraud at source. The Bill is intended to introduce a world leading regulatory framework to hold tech and TelCo companies responsible for scams that originate via their platforms<sup>4</sup>. There is no formal accountability or liability today for these firms in enabling fraud conducted over the payment systems. These platforms hold critical data that our members are unable to access to detect and prevent APP fraud at source. With this in mind, we are continuing our advocacy efforts to ensure the Bill is passed as soon as possible. To mitigate the financial impact of the PSR's new liability regime, its implementation should be synchronised with the implementation of the critical controls and obligations created by the Online Safety Bill.

### ***Impact on user experience as a result of the PSR's proposals***

As a result of the PSR's proposals, our members will need to introduce significant friction in the payments journey in order to allow more time to detect and investigate fraud. This will have a knock-on effect in terms of user experience because consumers will likely find it is not as quick or as slick to make payments.

This partially defeats the purpose of the Faster Payments Service ("FPS") – widely regarded as

---

<sup>2</sup> In our response to CP21/10 we cited the Royal United Services Institute for Defence and Security Studies ("RUSI") paper published in January 2021: [https://static.rusi.org/the\\_silent\\_threat\\_web\\_version.pdf](https://static.rusi.org/the_silent_threat_web_version.pdf) Here, RUSI describes the impact of fraud on UK National Security as a silent threat, and calls for a "whole of system, public-private strategy for tackling fraud. This should include: [...] pathways for cross-government collaboration; and a clearer role for the private sector – including the financial, e-commerce and telecommunications sectors – in tackling fraud."

<sup>3</sup> <https://www.nao.org.uk/reports/progress-combatting-fraud/>

<sup>4</sup> We cited in our response to CP21/10 the UK Finance data point that shows more than 70% of all APP scams originate via social media platforms or telecommunications.

a UK success story – which was introduced in 2008 to help enable mobile, internet, telephone and standing order payments to move quickly and securely with real-time transfers between UK bank accounts, 24 hours a day.

There is also a risk that the mandatory reimbursement proposals could incentivise some PSPs to apply increasingly stringent criteria when deciding whether or not to allow a customer, or a class of customers, to obtain payment services, thereby undermining financial inclusion for some consumers. This would be a patently unacceptable outcome, at odds with UK financial services regulators and the Government's efforts to boost financial inclusion.

## **Question 2: Do you have views on the impact of our proposals on PSPs?**

Our members are extremely concerned that the introduction of an unfunded, uncapped liability regime could potentially have a devastating and disproportionate impact on prospective market entrants and existing start-up and scale-up firms in the payments ecosystem.

Below, we outline:

- Issues with the PSR's cost-benefit analysis;
- The impacts that these proposals will have on our members and wider FinTech ecosystem in the UK; and
- An approach to implementation that the PSR may wish to consider, which we believe may go some way to avoid unintended consequences of the proposals for new market entrants and existing start-up and scale-up firms operating in the UK.

### ***Cost-benefit analysis***

The PSR's mandatory reimbursement proposals are the first of its kind in the world. With this in mind, the PSR's cost-benefit analysis is not sufficiently robust in terms of assessing and articulating the impact of mandatory reimbursement proposals for start-up and scale-up PSPs which constitute the vast majority of PSP firms in the UK market. The CRM Code applies to only 10 PSPs, yet there are around 40 Faster Payments Indirect Access Providers and 1500 indirect



access firms<sup>5</sup>. Costs for all firms that are not already CRM Code subscribers extend well beyond new reimbursement burdens and will present a barrier to entry and significant revenue threat to the majority of small- and medium-sized PSPs.

Without providing specific figures or its methodology, the PSR notes that increased costs for PSPs are an intended impact of its proposals, and the PSR considers that the way in which PSPs can stem rising costs is by investing further in financial crime systems and controls.

We challenge this argument. No one disagrees with the principle that having robust and effective financial crime systems and controls should be a precondition for all actors operating within the UK payments sector, and we recognise more can and should be done to enhance financial crime systems, controls and strategies across the financial services sector. However, FinTechs and incumbents investing more time, money and other resources in their financial crime systems, controls and strategies will never address APP scams at source, which means PSPs are likely to see costs increase annually as a result.

The PSR's own argument is undermined by the outcomes from its recent joint TechSprint<sup>6</sup> with the FCA on APP scams. The TechSprint highlighted that PSPs cannot solve the issue at source or in isolation, and one of the most effective ways in which to tackle the fraud at source is to have real-time data sharing that leverages data from across the financial services, tech and TelCo sectors. This real-time data sharing framework, as well as an obligation on social media and tech firms to actively manage fraud risks, should be an important part of any public-private sector approach to tackling financial crime, which we call for as part of our response to Question 1.

### ***Impacts for our members and wider UK FinTech ecosystem***

FinTechs are a positive source of disruption within the payments sector, providing payment services to the underserved or unbanked and solving consumer problems like making it easier to split bills between friends and reducing the cost of spending using your debit card on holiday. Consumers up and down the country benefit from innovation and competition in the sector.

---

<sup>5</sup><https://www.psr.org.uk/publications/policy-statements/access-and-governance-report-on-interbank-payment-systems-january-2022>

<sup>6</sup> <https://www.psr.org.uk/news-updates/events/authorised-push-payment-fraud-techsprint/>

The ramifications of the PSR's proposals for the FinTech ecosystem cannot be underestimated: they pose a material barrier to entry and adversely impact existing start-ups and scale ups' ability to remain economically viable in the UK market.

We outline:

- Costs associated with operational readiness for compliance with the new liability framework and estimated costs of mandatory reimbursement;
- Impact on edge cases that do not neatly fall within the liability framework; and
- Potential supervisory interventions as a result of slowing FPS payments or temporarily freezing consumer accounts to detect and investigate potential fraud.

*Costs associated with operational readiness to ensure compliance with the new liability framework and estimated costs of mandatory reimbursement*

To prepare for the implementation of the PSR's proposals, our members must set aside funds for accruals, new collections and disbursement systems, new data monitoring and alert systems, investigations and dispute staff, and (for some of our members) likely increased capital requirements.

In our response to CP21/10, we noted that mandatory reimbursement costs alone are estimated to be the equivalent of wiping — at a minimum — a tenth of PSPs' revenue, according to data points drawn from our members and the wider FinTech ecosystem. If the PSR chooses to proceed with implementing its proposals without any upper threshold being introduced (please see our response to Question 9), firms will face uncapped liability costs. These costs will only rise exponentially in the event that the liability model is extended from FPS to the Clearing House Automated Payment System ("CHAPS").

While incumbents may be able to absorb the costs associated with mandatory reimbursement, data reporting, and an uptick in Financial Ombudsman Service ("FOS") cases, whether by cross-subsidisation or other means, they are a heavy burden on existing FinTechs and introduce real barriers to prospective market entrants.

Competition is raised as an issue at paragraph 1.22 of CP22/4, which cites respondent firms' concerns that mandatory reimbursement would be expensive to implement and operate as a barrier to entering the market. However, it is not addressed in the response from the PSR. We believe that the current proposals are likely to lead to a substantial withdrawal of PSP firms from the UK market.

*Impact on edge cases that do not neatly fall within the liability framework*

The UK is one of the world's leaders in Open Banking — in January of this year, Open Banking passed the 5 million users<sup>7</sup> mark with more than 7 million successful payments<sup>8</sup> made last month. Innovation within the Open Banking space is a key focus for the Strategic Working Group ("SWG"), which provides the Joint Regulatory Oversight Committee ("JROC") with constructive challenge as it supports the Open Banking Implementation Entity ("OBIE") transition to a future entity focused on 'Open Banking plus'.

Payment Initiation Services ("PIS") are emerging as a competitive, cost-effective alternative to traditional card-based payments for consumers and businesses, and we have highlighted the benefits to SWG in our responses to the payments, data, and ecosystem sprints (see more below in response to Question 3).

The PSR's proposed liability regime for FPS will likely increase costs (such as costs of managing disputes and FOS escalations) for sending and receiving banks. These costs will be passed on to merchants in the form of charges for receiving Faster Payments. This will make Open Banking an unattractive option for merchants because the costs to receive Faster Payments via Open banking will be greater than the cost to receive card payments. Account Servicing Payment Service Providers ("ASPSPs") may even consider introducing charges to consumers for sending or receiving Faster Payments (as is common practice in the EU), which would further disadvantage Open Banking payments.

---

<sup>7</sup> <https://www.openbanking.org.uk/news/open-banking-passes-the-5-million-users-milestone/>

<sup>8</sup> <https://www.openbanking.org.uk/api-performance/>

In addition, the PSR's liability model for FPS will likely exacerbate the problems in relation to de-risking and transaction limits in the Open Banking space. Based on our members' experience, we know that firms offering Open Banking related products and services already struggle with incumbent banks arbitrarily limiting and blocking Open Banking payments. Our members are concerned that the new liability regime for FPS will lead to further limiting and blocking of Open Banking payments by banks and make Open Banking untenable as a payment option (removing a credible alternative to cards).

We recognise that supporting the development of Open Banking is a core part of the PSR's five-year strategy<sup>9</sup>, and we would urge the PSR to consider a phased and iterative roll-out of the liability scheme to PIS, or risk snuffing out emerging business models before the market can reach maturity.

By affording a longer lead time to PIS firms before they are brought within the scope of the liability framework, it will allow industry and the SWG to develop a suitable purchase protection scheme for these payments. Open Banking payments are inherently safe by design<sup>10</sup>, so any proposals should be risk-based and create the correct incentives for all parties involved in the payments chain.

If we are to look at the counterfactual — i.e. the PSR does not regard PIS to be an edge case and it is brought within the scope of the FPS liability framework from the outset — then we predict

---

<sup>9</sup> <https://www.psr.org.uk/media/jw1gjukz/psr-response-to-digital-payments-initiative.pdf>

<sup>10</sup>(1) Every payment uses strong customer authentication ("SCA"). When a customer makes a payment using open banking, they are always sent to their bank's app to strongly authenticate, usually with biometrics.  
(2) No sensitive details are shared with the merchant. There is nothing to intercept, steal or leak that could lead to unauthorised payments, unlike with e.g. card-not-present payments. Instead, Open Banking providers securely communicate with the customer's bank to pass on payment instructions in the background and initiate the payment.  
(3) Payment instructions are pre-populated, removing the possibility of human error when typing payee details (sort code and account number) or customers being tricked into sending money to an account controlled by a fraudster. The beneficiary's name is also presented back to the payer by the PISP in the authentication journey.  
(4) Open banking providers onboard and carry out customer due diligence ("CDD") on merchants before entering into a commercial contract. This is in addition to the checks that Account Servicing Payment Service Providers (ASPSPs) undertake on merchants (which are more rigorous than those conducted on personal accounts) before they are onboarded by the PISP, and further reduces the likelihood that bad actor merchants would use Open Banking for fraud.

that a number of businesses will exit the UK market, which will be to the detriment of consumers and businesses.

#### *Supervisory interventions if firms slow FPS payments and / or temporarily freezes consumer accounts*

There is a potential misalignment of expectations on the part of the PSR and FCA. Based on our members' interactions with their FCA supervisors, they understand that there could be supervisory interventions if a PSP slows FPS payments or temporarily freezes certain consumer accounts in a bid to detect and investigate fraud.

We would urge the PSR and FCA to collaborate and share with industry what 'good looks like' in terms of PSPs' interventions to detect and prevent fraud in this context.

#### ***Suggested approach to implementation that may avoid unintended consequences***

A balance must be struck between protecting consumers from losing life-changing sums of money, incentivising innovation and competition in the payments sector, and introducing the right incentives on all participants in the digital economy to reduce fraud.

Our members recommend:

- An increase to the minimum threshold (from £100 to £250), so PSPs can focus on protecting consumers from losing life-changing sums of money.
- The introduction of an upper threshold cap of no less than £30,000, so that all consumer protection reimbursement for fraud is consistent across payment types. This would provide multiple benefits: resonant with consumers, a proportionate regime for the vast majority of small- and medium-sized PSPs and would not provide an incentive for first-party fraud to be directed at the payment systems. However, the PSR should validate any caps with analysis based on existing CRM Code fraud reporting.
- The PSR should look to apply the FPS liability framework to edge cases such as PISPs in the medium- to long-term and not from the outset, so as to not inadvertently stifle innovation and emerging business models which are the focus of its own five-year strategy as well as the future entity overseeing 'Open Banking plus' in the UK.

- The timing of the entry into force of the PSR's liability model should be aligned with the entry into force of the Online Safety Bill, which will introduce incentives on other players within the digital economy (social media and TelCo firms) to reduce fraud. The PSR should also consider staggering the roll out of its liability regime, focusing first on CMA9, then gradually rolling out across the sector.
- As mentioned in our response to CP21/10, the PSR should collaborate with industry to pilot the data reporting measures and robustly analyse the impacts before mandatory reimbursement requirements come into play. A pilot would provide the regulator and industry time to spot any adverse effects, and pause the data sharing (or consider alternative approaches, such as aggregated data sharing) to remediate the unintended consequences of placing this data in the public domain.
- The PSR should collaborate with relevant counterparts in the FCA, Home Office, law enforcement and other relevant bodies and industry to shape a joined-up, public-private sector approach to tackling fraud in the UK.

While beyond the scope of this paper and the PSR's remit, we will be calling on the Government, as part of its post-Brexit review of legislation and regulation, to focus on payments. Specifically, we wish to see a removal of the 'blocks' in the Payment Services Regulation 2017 that hinder sending and receiving PSPs from stopping payments where they suspect APP (or other) fraud and for authorised payments liability be set out in legislation.

**Question 3: Do you have views on the scope we propose for our requirements on reimbursement?**

The current proposed liability model for Faster Payments poses a material threat to Payment Initiation Service Providers' ("PISPs") business models. We urge the PSR to consider an iterative roll out of the liability model — temporarily excluding PISPs from the scope of liability in the short-term — as this will afford the industry and regulators time to develop a tailored and sustainable purchase protection model, while allowing PIS to continue to grow and scale.

PIS deliver value in a number of ways for UK consumers and businesses — perhaps most importantly, PIS offers businesses, particularly small businesses, a competitive alternative to expensive card payments.

In order to compete with card payments, these providers must offer a reliable service to their merchants, who are relying on them to facilitate payments. The proposed liability model places a significant incentive in the system for account providers in the UK to introduce friction into the payment flow to protect their consumers and reduce the need for reimbursement for even low-value payments. This friction will likely take the form of additional 'pop up' warnings and/or verification steps for consumers when authenticating payments<sup>11</sup>. This additional friction will undermine the user experience and success rates for payments initiated by PISPs. Further, it would also be at odds with the PSR's objective of encouraging account-to-account retail payments.

There are many technical solutions for introducing purchase protection for PIS payments in the event that goods/services are not provided, or as described in an e-commerce environment. There is currently ongoing work in the SWG, feeding into the JROC on Open Banking, to consider how best to create multilateral agreements like those present under the card schemes to govern consumer protections in the event that goods and services are not provided or as described.

Finally, we do not believe that it is necessary or proportionate to extend the liability regime to CHAPS. The consultation notes that less than 0.01% of APP fraud is conducted via Faster Payments. This low rate is expected to drop substantially as consumer payments migrate from CHAPS to FPS in light of the FPS increase from £250,000 to £1,000,000. While CRM Code firms are liable today for APP fraud conducted through CHAPS, liability for a high-value payment would not be proportionate for the size and scale of most non-CRM Code firms.

**Question 4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

---

<sup>11</sup> The OBIE notes in relation to PISP-initiated payments, Confirmation of Payee and Contingent Reimbursement Model pop-up warning messages are of limited utility and the resultant additional friction together with the incremental costs of deployment are not justified.

***There should be a consumer caution exception to mandatory reimbursement***

We consider that a consumer caution exception to mandatory reimbursement should be included. We take the view that including this exception would mitigate the moral hazard of removing any risk to the consumer of proceeding with a potentially fraudulent transaction without taking any precautionary steps.

The consultation paper notes that TSB has not identified evidence of customers exercising less care or caution as a result of its fraud refund guarantee. However, the PSR accepts that it has limited evidence, so no conclusions can be drawn about how the reimbursement policy has changed consumer attitudes to risk. Hence, the PSR is right to conclude that the risk that consumers may exercise less caution if they know that they may be refunded cannot be ruled out.

"Consumer caution" is not clearly defined in the consultation paper, it merely describes that a consumer must exhibit "gross negligence" (paragraph 4.23), which will be set at a "high bar, higher than in the CRM Code".

We call on the PSR to set the standard for "consumer caution" at the same level as that described in R2(1) of the CRM code. This is a standard that distributes responsibility fairly between the consumer and PSP, and ensures consistency for signatories to the Code and their customers. The CRM Code provides four circumstances in which a consumer does not have to be reimbursed which, taken together, should form the basis of the consumer caution exception. These situations are:

- (a) The Customer ignored Effective Warnings, given by a Firm in compliance with SF1(2), by failing to take appropriate action in response to such an Effective Warning given in any of the following:*
- (i) when setting up a new payee;*
  - (ii) when amending an existing payee; and/ or*
  - (iii) immediately before making the payment.*



"Effective Warnings" must be (i) clear and understandable, (ii) delivered at an appropriate time (e.g. when setting up a new payee), (iii) risk-based and tailored to the type of fraud where possible, and (iv) enable the customer to understand the actions they need to take to address the risk. This ensures the customer is made properly aware of the situation, and so any decision to proceed is an informed one and it is fair for the customer to bear the risk.

What constitutes an Effective Warning should be set by reference to the proportion of customers who either do not proceed, or only proceed after making further checks, after receiving a message (or series of messages). This would mean that any series of warnings that a PSP can demonstrate lead to, for example, 99% of customers not proceeding with that transaction without making further checks would constitute an Effective Warning.

*(b) The Customer did not take appropriate actions following a clear negative Confirmation of Payee result. R2(1)(b) can only be relied on where the Firm has fully complied with SF1(3) or SF2(2), and actions would, in the circumstances, have been effective in preventing the APP scam;*

The Confirmation of Payee system must provide the customer with sufficient and adequately clear information, including what their options are, to enable them to make an informed decision as to whether to proceed. If a well-informed customer decides to proceed, it is fair for them to bear the risk of their decision.

*(c) In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that:*

*(i) the payee was the person the Customer was expecting to pay;*

*(ii) the payment was for genuine goods or services; and/or*

*(iii) the person or business with whom they transacted was legitimate.*

This sets out the moral hazard issue that PSPs are concerned about. Where a customer does have reason to think that they are sending their money to the intended recipient, they should bear the risk of their actions. Having a higher bar would require PSPs to reimburse customers

who had acted in an unreasonable manner, which is an unfair distribution of risk as customers will have no incentive to take reasonable care. Not only would this give PSPs an unfairly high level of exposure, but it would likely increase the number of instances of fraud.

*(d) Where the Customer is a Micro-enterprise or Charity, it did not follow its own internal procedures for approval of payments, and those procedures would have been effective in preventing the APP scam.*

Where procedures have not been followed, the risk should fall on those who deviated from the process unless they were unable to follow the process, despite making all reasonable efforts to do so.

In addition to the four exemptions listed above, there should also be two further exemptions:

- The first is an exemption when the customer has been the victim of multiple similar scams and has received education from the PSP. In such a case, the customer has been given multiple warnings and received a detailed explanation of the nature of the APP scam they are falling victim to, meaning that unless they have characteristics of vulnerability, they are exhibiting “gross negligence”.
- The second is an exemption where the customer has lied during their risk-assessment process. A customer who lies is clearly not exhibiting caution as they are attempting to hide their level of risk. As a result, the PSP, through no fault of its own, could not tailor the risk warnings to the level the customer required.

### ***Using gross negligence as the consumer caution exception***

As explained above, we recommend that the CRM code standard set out at R2(1) be used as the consumer caution exception. Should gross negligence be a higher standard than this, it should not be used, for the reasons set out above.

### ***Additional guidance on gross negligence***

Our members are concerned that the lack of additional guidance on “gross negligence” presents a significant problem for both PSPs and customers. The current guidance is extremely vague. It has been described by the FCA as “a very significant degree of carelessness” and by the FOS as

"more than just being careless or negligent" and "an ever-changing state of play". Failing to provide further guidance would be detrimental to all parties concerned — customers and PSPs would be uncertain of where they stand, likely leading to hopeless claims being pursued and good claims not being made. Further, having to go through the courts or FOS imposes time and financial costs on the contesting parties to achieve a ruling that provides the same information as that which the FOS could provide when the liability framework comes into force. We consider that publishing further guidance would avoid these unnecessary negative consequences.

We take the view that more guidance from the regulators would promote certainty and consistency amongst firms. We do not consider that a full definition of gross negligence is required from the regulator, but a list of situations in which a customer should be classified as being grossly negligent, would make the position much clearer for consumers and firms, whilst allowing the regulators to retain the flexibility to adapt their approach to developments in this space.

**Question 5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

More clarity is needed over what constitutes a “vulnerable customer” (see Question 6), and what constitutes “gross negligence” (see Question 4) to answer this definitively.

Should these terms have acceptable definitions and adequate carve outs, we would consider a requirement to reimburse vulnerable customers who acted with gross negligence to be unacceptable.

**Question 6. Do you have comments on our proposal to use the FCA’s definition of vulnerable customer?**

We recommend that the PSR applies the APP fraud specific definition of vulnerability provided by the CRM Code, noting that this does not invalidate the spirit of the wider FCA definition. Alternatively, we urge the PSR to acknowledge that the industry may follow the higher standard CRM Code definition by way of market practice.

The FCA defines vulnerable customers as those who “due to their personal circumstances” are “especially susceptible to harm”. This is a useful guiding principle for firms’ activities as a whole, which is the aim of the definition in the first place. However, this definition creates a one-dimensional, blanket tag that a customer is vulnerable due to their general characteristics rather than how those characteristics interact with the situation at hand. In the context of APP scams, this risks harming both consumers and firms.

By contrast, the definition used by the CRM Code is clearer to our members for it emphasises the circumstances of a potentially vulnerable customer “at the time of becoming victim of an APP scam” and “against that particular APP scam, to the extent of the impact they suffered”. Our members consider that this definition allows for more flexibility in the identification of vulnerable consumers because it implies a case-by-case analysis. It also allows room for customers to be considered vulnerable in some, but perhaps not all, situations.

Innovate Finance agrees that the FCA standard should continue to apply to the industry as a whole, but in the specific case of APP fraud, our members’ experience has led to the opinion that a more specific definition (as used by the CRM Code) is preferable. Our members consider that it will give customers with vulnerable characteristics an increased capacity of self-determination, and ultimately respect and equal opportunity. As the FCA acknowledges in its *Guidance for firms on the fair treatment of vulnerable customers*, consumers may not want the label ‘vulnerable’ applied to them.

While the FCA refers to customers as being vulnerable throughout the Guidance, it also suggests that firms not use this label in their interactions with consumers. In the context of this consultation, Innovate Finance considers that simply applying the FCA’s general definition of vulnerability will create archetypes of vulnerable customers, taking away customers’ ability to define themselves, as well as firms’ ability to accurately analyse each case of APP fraud.

We further consider that the CRM Code definition encompasses the wider FCA definition, but because it is crafted with APP scams in mind, it allows firms to gather more accurate data in relation to specific characteristics of vulnerability in the APP context. In the long term, this will

help create a wider data pool for the FCA definition of vulnerability, while enabling firms to respond to APP scams more accurately.

**Question 7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **Any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

We support the proposal to allow sending PSPs to apply a fixed 'excess' to reimbursement. We also welcome the proposal to allow PSPs the discretion to exempt vulnerable consumers from the 'excess' they apply. Nonetheless, in the context of APP fraud we do not consider that £35 is a meaningful amount.

From a consumer perspective, £35 is a modest amount that is unlikely to persuade consumers to more carefully consider the payments they initiate. In particular where the payment exceeds a nominal sum, consumers may see a maximum deduction of £35 as an expendable risk. We believe that an 'excess' has the potential to deter customers from initiating certain suspicious transactions, but only where the total amount of the 'excess' will be noticeable. We note that customers are used to paying excesses that are proportional to the amount claimed. For example, we are aware that the excess for building insurance cover will generally be higher for high value properties than for low value ones. If the 'excess' is also meant to reflect the cost that PSPs undertake in retrieving refunds for consumers, £35 insufficiently covers those costs.

There is currently no industry standard in relation to when and to what extent the £35 deduction in Regulation 77 of the Payment Services Regulations 2017 ("PSRs 2017") is applied. This is largely left up to market practice, yet no significant market practice has developed, and we are concerned that a similar confusion and added level of complexity would occur in the case of APP fraud.

Consequently, we urge the PSR not to mandate an upper limit for this 'excess' and allow the industry to set a standard.

**Question 8. Do you have comments on our proposal that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable customers from any threshold they set?**

Innovate Finance supports the proposal to allow sending PSPs to set a minimum claim threshold. We also welcome the proposal to allow PSPs the discretion to exempt vulnerable consumers from this minimum claim threshold.

With regards to the minimum threshold being set at no more than £100, we echo our response to Question 7 above. Data points drawn from our membership base and the wider FinTech ecosystem have highlighted that APP scams tend to amount to at least £250. In this context, a £100 threshold is not sufficiently impactful, and we would urge the PSR to consider an uplift of the minimum claim threshold to £250. We would also recommend that this minimum claim threshold amount is reviewed at least every two years in line with inflation and data points from the payments industry on the average APP fraud claim value.

The introduction of an impactful minimum claim threshold is absolutely crucial if the PSR is not minded to introduce a customer caution exemption. The role of customer caution differs across all scam types, and our members acknowledge that customer caution will not necessarily play a role in sophisticated scams involving complex social engineering. However, based on our members' experience, a large proportion of APP fraud relates to low-value purchase scams, the vast majority of which originates and is driven from social media. On the whole, these are edge cases when considering what the CRM code was set up to detect, prevent and protect consumers from. The role of the customer in low-value purchase scams is key; therefore, a clear incentive placed upon consumers to reasonably assess the veracity of the peer or business they are paying is helpful in the prevention of this type of scam. If the PSR does not intend to create a customer caution exemption, the *de minimis* threshold must be significantly robust to promote caution in these scenarios.

**Question 9. Do you have comments on our proposal not to have a maximum threshold?**

We call for the introduction of a maximum threshold — without this, our members potentially face unlimited liability. Our members have suggested the upper threshold should be no less than £30,000.

Unlimited levels of liability pose a significant risk to early stage, venture capitalist funded and pre-profit businesses that do not have the financial resilience to reimburse significant sums, resulting in a significant barrier to entry, the withdrawal of many PSPs from the UK market, and in other cases immediate insolvency that would have ramifications through the payments ecosystem. We believe that an unfunded and uncapped liability scheme is an unrealistic and unreasonable burden for the majority of PSP market participants.

The lack of certainty will also mean firms struggle to calculate and disclose their contingent liabilities as required under UK and international accounting standards. We anticipate that this will pose difficulties for start-up FinTechs wishing to raise capital and go through funding rounds with private investors, as well as scale-up FinTechs who may be considering an Initial Public Offering. Additionally, for new and existing challenger banks, this also likely will require additional Pillar 2 capital requirements.

**Question 10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

***Sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement***

We agree that sending PSPs should be allowed to set a time-limit for mandatory reimbursement. Time-limiting claims allows PSPs to operate with greater levels of financial certainty.

***Time limits should be set at no less than 13 months***

Our members are supportive of a 13-month time limit. We would urge the PSR to make it clear that there should be no retrospective application of the time limit, i.e. claims for reimbursement can only be made from any date on or after the PSR's liability model enters into effect.

Our members consider a 13-month time limit strikes the correct balance between offering appropriate protection for consumers (recognising that some APP scam typologies such as investment and romance scams may take place over an extended period of time) and providing PSPs with certainty.

**Question 11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first-party fraud or gross negligence?**

Innovate Finance agrees with structuring reimbursement in this way.

However, our members are concerned that 48 hours is insufficient time to make preliminary investigations into whether there has been first-party fraud or gross negligence. The need for investigation into the possibility of fraud or gross negligence is acknowledged in the exemption to the 48-hour time limit. However, we consider that the exemption is rendered largely ineffective by the short window within which to conduct such investigations. As such, the proposed time limit would mean PSPs are faced with a choice between not conducting robust investigations, meaning instances of first-party fraud could go undetected, or breaching the 48-hour time limit.

The 48-hour threshold appears to be proposed because it brings APP reimbursement in line with that timeframe used for unauthorised payments. However, given the time required for adequate investigation, usually involving requests for information with third parties and other external processes and discovery requirements, we therefore consider that it makes more sense to bring the PSRs 2017 in line with the CRM Code. Under R3(1), firms should decide whether to reimburse a customer within 15 business days of the APP scam being reported. Additionally, DISP 1.6.2AR gives respondents to EMD and PSD complaints 15 business days to send a final response.



Consequently, we recommend that PSPs are given at least 15 business days to make preliminary investigations before deciding whether there is sufficient evidence to extend the time for investigation further — our members' experience indicates that a full investigation takes 30 to 35 days, on average.

This would give practical effect to paragraph 1.18 and prevent fraud being perpetrated against PSPs by enabling them to investigate reimbursement claims before paying out.

Further, the industry would also welcome guidance from the PSR as to the approach to be taken where individuals refuse to cooperate as part of a PSP's investigation.

**Question 12. What standard of evidence for gross negligence or first-party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

***Appropriate standard for gross negligence or first-party fraud***

The appropriate standard for gross negligence or first-party fraud will depend on the length of time afforded to PSPs to conduct preliminary investigations before being required to reimburse customers. If PSPs are afforded more time to conduct the initial investigation, then a higher standard could be applied.

This further underlines why the 48-hour timeframe for reimbursement is not appropriate. Increasing it would benefit all parties because PSPs would be able to conduct more thorough investigations, meaning there would be more certainty that fraud is not being perpetrated. And many customers will receive their reimbursement sooner because their claims will not reach the higher evidence threshold, meaning they receive their reimbursement after the initial period, rather than after a full 35-day investigation.

***How long should the PSP have to investigate?***

Innovate Finance is of the view that where evidence of gross negligence or first-party fraud is found, the whole process from the receipt of the APP scam claim through to the PSPs final

decision should be 35 days (in line with the CRM Code). Therefore, we call on the PSR to set the time for investigation at 35 days minus the time allowed for a preliminary investigation.

This would still be a fast resolution process. Under DISP 1.6.7, firms have eight weeks to address complaints, and the PSR has 20 working days to review complaints made against it.

**Question 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

Our members understand why the PSR proposed a 50:50 default allocation of reimbursement costs as an initial starting point, but we would urge the PSR to better tailor the allocation of liability and reimbursement costs (please see our response to Question 14).

**Question 14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We outline views on:

- Proposed approaches to create a more tailored allocation criteria; and
- Dispute resolution.

***Tailored allocation criteria to support a departure from a 50:50 default allocation of reimbursement costs***

After the entry into effect of the Online Safety Bill, which should place additional incentives on the tech platforms and TelCo sector to address fraud that originates via their sectors, our members are broadly supportive of an approach being developed and piloted that links liability to the effectiveness of an institution's anti-fraud performance.

Working with industry, a set of key performance indicators could be developed that evidences effectiveness of firms' anti-fraud measures. This approach could be modelled on the approach taken to the revised Payment Services Directive ("PSD2") transaction risk analysis thresholds for exemption. This could be one way to incentivise each institution to evolve its protections, which will be necessary as scammers react and evolve their attacks. If firms defeat XX% of attacks then their liability allocation could progressively fall to zero.

Alternatively, the PSR could look to leverage the data it is collecting as part of its Measure One proposals (publishing APP scam data). The PSR currently plans to make the largest 12 banks in the UK publish their APP scam rates every 6 months starting next year: this could be extended in time to cover all PSPs (much like the roll out of Confirmation of Payee). Based on the published scam data of all PSPs, the PSR could provide a risk score to each PSP on a 1 to 10 scale, based on the amount of APP scams seen as a percentage of total transaction volume. This score would then determine the default allocation between PSPs for the following 6 months, until the next reporting period.

If the PSR is not minded to explore these approaches, our members would reiterate that any tailored allocation criteria would have to be crystal clear and not be open to a high degree of interpretation (which would feed into issues surrounding dispute resolution).

### ***Dispute resolution***

Our members are aligned that — unlike incumbents — they could not afford a model of dispute resolution that is overly cumbersome and involves lengthy bilateral negotiation, mediation, or legal challenge in each and every case in order to secure a departure from the 50:50 default allocation.

Whichever model of dispute resolution is adopted, our members would welcome a process that is automated, so that the process is as cost and time efficient as possible in order to maintain a level playing field between FinTechs and incumbents.

Our members would urge the PSR to convene a technical working group made up of payments industry subject matter experts and legal and other alternative dispute resolution professionals to explore how to operationalise a suitable dispute resolution model that can be introduced in the medium term. We would urge the technical working group to consider the learnings from the FOS alternative dispute resolution regime and the Centre for Effective Dispute Resolution as it develops an appropriate model to apply in the context of FPS liability.

**Question 15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

Our members recognise the complexities inherent in multi-generation scams, which makes it difficult for PSPs caught in this chain to detect and investigate cases of APP fraud. While recognising this is an imperfect solution, our members suggest that liability could fall on the last sending and receiving PSPs in the chain.

This leaves unanswered a number of questions and we suggest that the PSR may wish to convene technical working groups with industry subject matter experts to explore further the issues surrounding multi-generational scams. We would be happy to support the PSR as it explores cases that fall inside and outside the scope of the FPS, including transfers to crypto wallets, for example.

**Question 16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

Please see our response to Question 14. We would welcome the development and piloting of a more tailored approach to allocation of liability; this approach could also lend itself to allocation of repatriated funds.

**Question 17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We have no objection to the proposed scope.

**Question 18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

Our members do not agree that the payment system operator ("PSO"), in the long term, is the appropriate body to undertake the role of making, maintaining, refining, monitoring, and enforcing compliance with, comprehensive scheme rules that address fraud risks in the system.

As mentioned in response to Question 2, we will be calling for the government to undertake a review of payments legislation and regulation as part of its wider post-Brexit review of the UK's statute and regulatory rule books. As part of this, we wish to see the liability framework for FPS

be set out fully in legislation rather than scheme rules with clear roles for the FCA, PSR and Pay.UK.

The role of Pay.UK should not become quasi-regulatory in nature and monitoring and enforcing compliance should sit with the PSPs' supervisory teams at the FCA.

If the PSR is minded to lean on Pay.UK in the short term, we would welcome early sight of a clear plan as to how Pay.UK will recruit and upskill staff to deal with these new responsibilities.

**Question 19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

No response.

**Question 20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

No response.

**Question 21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

Please see our responses to Questions 14 and 16.

**Question 22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

Please see our response to Question 18.

**Question 23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

Please see our response to Question 18. We consider that compliance and monitoring should sit with PSPs' supervisory teams at the FCA.

**Question 24. Do you have views on the best option for short-term enforcement arrangements?**

Please see our response to Question 18.

**Question 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

With regard to indirect clearing firm liability, we consider that the legal obligation rests on each account owning payment services provider (ASPSP) firm. The PSR is proposing for clearing banks to take the liability for their clearing customers. If clearing banks are forced to take on credit risk for their indirect clearing customers, the clearing banks will be required to substantially increase their risk and credit requirements for indirect clearing and this will lead to the loss of access to clearing for many PSPs reducing competition and innovation in UK markets.

In turn, the reduction of PSPs eligible to meet clearing firm risk and credit requirements will have a disproportionate commercial impact on FinTech clearing banks and firms that compete against incumbent clearing firms. One of our members was the first new clearing bank in 250 years, after which four other new clearing banks have obtained access to Faster Payments. The PSR's Access Report in paragraph 4.12 states that *"The new-entrant Indirect Access Providers [IAPs] continued to take on many customers, including smaller PSPs and small money remitters, which historically had the most difficulty gaining access."* As such, new clearing firms service new and innovative PSP business and would likely sustain a higher loss of business than the four incumbent high street clearing banks.

**Question 26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

In the case where the sending firm is acting as an Indirect Access Provider, the payment will be initiated by the Indirect PSP. In this case, the sending firm does not hold the bank/customer relationship and so cannot be held responsible for the Indirect PSP's compliance with reimbursement of the Indirect PSP's customer. We therefore recommend that the PSR issues a Special Direction to indirect PSPs and IAPs to clarify where the legal obligation rests.

**Question 27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

Please see our response to Question 2, which has comments on the cost-benefit analysis.

**Question 28. Do you have any other comments on the proposals in this consultation?**

No response.

[ENDS]

Investec



## **Investec Bank plc response to the Payment Systems Regulator's CP22/4 Authorised push payment (APP) scams: Requiring reimbursement**

### **1. Introduction**

1.1 Investec Bank plc ("IBP") is the UK presence of the Investec group. A specialist bank, in the UK IBP provides private banking and deposit accounts to consumers and capital, risk and advisory services for companies. Investec is publicly traded in London and Johannesburg. It is staffed by 8,200 employees across its core geographies of the UK and South Africa, along with other locations across the globe.

1.2 We welcome the opportunity to respond to the Payment Systems Regulator's CP22/4 Authorised push payment (APP) scams: Requiring reimbursement. Our comments on the proposals in this consultation paper relate to the impact of the proposals on our private banking and savings account clients and on business clients that are microenterprises or charities.

1.3 IBP has worked with the rest of the banking industry on the response that UK Finance has submitted. Our response should therefore be read alongside the industry response.

### **2. Our responses to the PSR's questions**

2.1 We comment by exception for only certain questions the PSR asks in its consultation, either because we want to make additional comments to those the industry has made or because our view diverges from the industry's.

#### **1. Do you have views on the impact of our proposals on consumers?**

2.2 IBP supports efforts to reduce fraud and protect consumers. However, our experience with our clients is that bank efforts are insufficient without further efforts from consumer organisations and public authorities. We ask that whatever the outcome of the PSR's consultation, any changes to regulation are additional to public information campaigns that remind payers to be

vigilant to fraud risks to protect themselves. Whilst we recognise our role in preventing payments and helping consumers when those payments go wrong, there are other organisations whose operations support fraudsters to publicise their scams and to appear legitimate. For example some consumers make payments to fraudsters who advertise on social media services. An effective public policy response to minimise the likelihood of consumers falling victim to fraud needs to include effective interventions in industries other than financial services. We are aware of the work on the Online Safety Bill but this will not address, say, the funding issues the House of Lords Fraud Act 2006 and Digital Fraud Committee cites in its November 2022 report, such as "A lack of financial resources was noted as a barrier to an effective law enforcement response."

## **2. Do you have views on the impact of our proposals on PSPs?**

2.3 We are concerned the costs of the PSR's proposals for mandatory reimbursement of eligible clients' fraud losses will reduce competition in the market for transactional banking services.

2.4 IBP's transactional banking operation is very small compared to the operations of the large high street banks. As a private bank our payment volumes are small but our payment values are high. Our clients are also more likely to make payments to investment services and to make higher value single payments. These proposals will have a significant impact through introducing further friction in the payment journey for high value payments which is typical of High Net Worth clients. Guidance on the steps a client is required to take to qualify for reimbursement should be clearly defined to ensure that banks do not incur an uncapped level of risk in scenarios where a client is very insistent on executing a payment but does not wish to conduct further due diligence checks.

2.5 Our clients will be afforded the protections available under any regulation and we will provide a high level of service when we meet those requirements. However, we think there is a medium or long-term possibility that the growth in account-to-account payments will be met with an increase in fraud that is outside the bank's ability to mitigate, and that the costs of providing transactional banking will increase excessively because of mandatory reimbursement. This could

lead to smaller firms exiting the market or limiting their transactional banking offerings, reducing competition and its associated benefits for consumers and small businesses.

### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

2.6 The PSR's proposal is clear that the requirement will apply to participants of the Faster Payments Service, whether direct or indirect. However, we are unsure about the geographical extent of the proposal. For example a firm operating in the Channel Islands or the Isle of Man could be in scope if it submits payments to the Faster Payments Service even though its regulatory licence is held outside the UK.

2.7 Our view is that mandatory reimbursement should not apply to firms whose regulatory licences are held outside the UK. We would welcome the PSR clarifying that its rules apply only to firms licenced by the Financial Conduct Authority or the Prudential Regulation Authority and the Financial Conduct Authority and the Gibraltar regulators.

### **9. Do you have comments on our proposal not to have a maximum threshold?**

2.8 We support the industry's view that the PSR should set a maximum threshold. This is important because it will help reduce moral hazard that could arise where a payer who knows they will be reimbursed for any funds lost to fraud applies a lower level of diligence to a request for a payment than they would have done if they knew some of the value of that payment would be at risk.

2.9 IBP considers the PSR should set a maximum threshold and that this should be set at an overall case value not individual payment value. Our view is that the value should be set at £85,000.00.

As a private bank with high net worth clients, it might be expected that fraud values would be well above this level because of the nature of payments such consumers make. However, our assessment and the scope of the proposed rule changes support a value threshold of £85,000.00.

2.10 We think this shows consumers are taking care when making high value payments and that introducing, first, a limit and, second, one at this level will prevent the moral hazard that might arise from consumers knowing the entirety of their payment is very likely to be covered by a reimbursement requirement for their bank. In the unlikely event that a fraud occurs in excess of this amount, if a victim is not refunded by the bank then the Financial Ombudsman Service would be able to investigate complaints referred to them up to their maximum award limit (currently set at £375,000.00).

2.11 Such a figure is also likely to be meaningful for consumers. We know from our savings operation that the FSCS limit of £85,000.00 leads to consumers depositing values at or near this figure in different institutions. The presence and absence of FSCS protection is also a differentiator, since some firms have this protection and some do not. Using this figure as the maximum reimbursement for a case of authorised push payment fraud would help consumer understanding because the figure is already in use elsewhere. Indeed it is likely to be the figure that protects the money they hold in the account subject to mandatory reimbursement.

2.12 We note that an uncapped limit would have cost consequences for firms beyond simply reimbursing clients. Insurance costs are likely to increase anyway to reflect the fact of mandatory reimbursement but our view is that the increase is likely to be lower if insurers know the maximum value a firm could have to pay for a single case. Additionally firms will have to retain provisions in expectation of losses. Again having a cap will allow firms to more accurately manage this because the maximum value will be known. This will minimise the opportunity cost to firms and to the economy more widely from firms having to increase fraud provisions for mandatory reimbursement. Lastly we note that without a cap the long-term effect might be that smaller firms consider exiting the market because the costs are too significant, a competition effect we consider would be contrary to the Payment Systems Regulator's statutory objective for competition.

**10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

2.13 We agree the PSR should allow firms to set a time-limit for mandatory reimbursement. However, we think the PSR should mandate that limit to avoid uneven implementation and confusion for victims of fraud about when they can present a claim once they realise they have been defrauded. A uniform limit will remove the possibility of further distress from having to check different firms' limits at a sensitive moment.

2.14 Our view is that the limit should be 13 months. This ensures clarity for eligible clients and it reduces the possibility that firms will compete to offer longer limits, confusing clients and arguably favouring larger firms that are better placed to absorb longer liability periods. We suggest this duration would be supported by data that shows that more than 95% of scams are cited within 13 months of their occurrence date.

**11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

2.15 IBP supports the industry view that 48 hours is too short a duration in which to resolve cases and to reimburse a fraud loss. Gross negligence is very difficult to determine in principle. Having to do so within 48 hours would be an exceptional challenge for firms. Some scams are extremely complex and information firms collect from fraud victims requires detailed scrutiny, including translation in some cases.

2.16 This is not to say that some limit is not appropriate. IBP recognises the period between a client realising they have fallen victim to a fraud and the firm confirming the outcome of its review is stressful. However, given the potential financial costs for the firm of having to reimburse a client for a large payment, it is only reasonable that the firm is permitted longer

than the regulator proposes to determine whether to reimburse.

2.17 We are concerned that a short period in which to make this determination will lead to automatic reimbursement and then recovery later once the full review is completed. This simply prolongs the uncertainty for the victim – funds reimbursed might be recovered later – and will likely hinder their psychological recovery from the scam.

2.18 Our view is that the regulator should require firms to resolve most cases within the existing 15 / 35 day timeline of the CRM Code. A lower threshold could be set for vulnerable clients. This approach will afford time for a thorough investigation and support certainty for victims. An alternative is that the regulator sets different thresholds for different types of fraud or different values of payments but we think this would be inappropriate because the extent of investigation relates to the sophistication of the scam and not the type or value.

2.19 As the industry response says, we recognise that the PSR has chosen the term ‘gross negligence’ to intentionally create a model which will see most victims of APP scams reimbursed, but we suggest that consumer behaviour must form part of the assessment when reviewing a claim. Therefore, we do not agree that gross negligence is the appropriate exemption to reimbursement and instead suggest that a definition of ‘contributory negligence’ may be more appropriate. We consider the PSR should help reduce the time firms need to review cases by providing its own view about what ‘contributory negligence’ looks like. IBP recognises this is in part a decision for the courts but the regulator’s view will be instructive for firms. This will help reduce the time taken to determine contributory negligence and it will support a consistent standard for industry participants.

## **28. Do you have any other comments on the proposals in this consultation?**

2.20 We believe the 50:50 liability proposed by the PSR is the appropriate approach for firms and it should not be left to firms to dispute. We note the PSR has asked Pay.UK to further consider some of the practical implications of implementing this policy but we would welcome the regulator expressing its view of how firms should resolve payments for liability sharing to avoid

smaller firms having to wait for lengthy periods for payments to be made.

2.21 As a smaller firm we would be concerned if all firms did not pay their shares of reimbursement costs following each scam and within a reasonable period. At the extreme some firms could adopt a netting approach where they will pay the net value of reimbursement credits and debits at the end of specific intervals. While doing so would be unlikely to present any financial stability implications for firms waiting for such payments, there would clearly be an opportunity cost to the firm owed and a benefit to the firm retaining the funds.

2.22 We would welcome the PSR saying in any policy statement it publishes following this consultation either that it expects firms to pay their shares of reimbursement to other firms within a reasonable period or that it expects such payments to be resolved within no more than 14 business days of the sending firm submitting its request to the receiving firm.

#### Further information

We will welcome any request from the PSR to discuss further any aspect of this response or how any other aspect of the PSR's proposals could affect our firm. Please contact [IBPFraud@investec.co.uk](mailto:IBPFraud@investec.co.uk) and we will be happy to help.

# ISPAY Limited





18 Springfield Gardens  
Morganstown  
Cardiff  
CF15 8LQ

9<sup>th</sup> November 2022

**ISPAY Limited: response to Payments Systems Regulator Consultation: Authorised Push Payments (APP) Scams: Requiring reimbursement PSR CP22-4 APP**

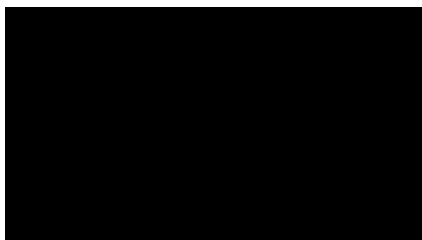
ISPAY Limited is a small management consultancy set up in 2019 and run by [REDACTED].

[REDACTED] has been involved in Payments for over 40 years, during this time he has been Head of Payments at TSB Bank Plc, where he oversaw and managed the 3<sup>rd</sup> party service supplied by Lloyds Bank. He then latterly played a significant part in the team that designed, built and migrated to a new payments platform that allowed TSB to become independent of Lloyds Bank and join the UK payment systems in its own right.

Prior to his role at TSB [REDACTED] worked in the Payments team at Lloyds Bank where he held several senior positions and was a director of the (old) electronic payment schemes, Faster Payments, CHAPS and Bacs. His directorship led to him chairing industry groups like the Faster Payments Rules and Governance group, the Standards working group etc. He also represented Lloyds Bank on, the then, new industry initiatives like Faster Payments and NewCHAPs.

More recently [REDACTED] has been a contracted technical adviser to the Payments Systems Regulator on the New Payments Architecture (ended May 2022).

ISPAY Limited [REDACTED] welcomes the opportunity to comment on this consultation **IPSR CP22-4 APP scams reimbursement** as he sees this as one of the most important areas in need of consumer protection in the Payments systems arena. With the world becoming a lot smaller through technology and criminals becoming more sophisticated even with over 40 years' experience, in the industry, there have been times when [REDACTED] has had to think very deeply as to whether a scam is potentially occurring or not and hence fully supports this work.



Managing Director

### **General view(s):**

As the consultation paper rightly points out there is a responsibility on both the sending and receiving PSP in the case of app scams, however the responsibility must be weighted towards the party with the greater influence of improving the outcomes.

The sending PSP has a duty of care to ensure that the payment is being made to the correct beneficiary, Confirmation of Payee is a step in the right direction. It also has to ensure that the payment instruction contains all the right details/information and run checks on that information before it sends a 'conforming instruction' to the receiving PSP, who will also run checks.

**In my opinion the receiving PSP has a far greater duty of care.** Not only does it have to undertake checks to ensure that the payment meets requirements (money laundering etc.) it also has to apply the funds to an account. The receiving account has to be a key factor in addressing app scams and is the responsibility of the receiving PSP. The PSP must have rigorous account opening procedures. Failure in providing rigorous account opening procedures leads to accounts being opened by criminals and gangs that provide the ability for them to receive and move money, very quickly, well before corrective action can be taken.

Hopefully, the outcomes of this consultation will lead to receiving banks becoming even more rigorous in their account opening procedures to prevent their accounts being used by criminals.

It is for this reason that **I would expect a 75:25 weighting for the receiving bank in covering the costs of any scam.** This would surely incentivise the receiving PSP to ensure that they are not harbouring accounts that may be used in app scams or any other activity that is a result in proceeds from crime.

Below I have provided answers to your specific consultation questions.

#### **1. Do you have views on the impact of our proposals on consumers?**

The proposals are a sensible way forward. Whereas the consumer will be reliant on the sending PSP to obtain refund, as mentioned above, I believe that there is a larger onus on the receiving PSP. There needs to be clear messaging to consumers on their rights in the case of app scams, especially covering the confusing area of 'excess' and 'min threshold'.

The Faster Payments system (3.8) run by Pay.UK will have to ensure that the receiving PSP's are compliant and meet the requirements to aide reimbursement by the sending PSP. What about CHAPS/cheques?

This model will not be too dissimilar to the Bacs Direct Debit Guarantee and subsequent Indemnity Claim model. Here the payer (consumer in the case of app scam) requests a refund from the Payer's PSP (sending bank in app scam), who in turn makes the refund and then claims from the Payees PSP (receiving bank in app scam). Perhaps there is learning from the Bacs model to ensure speedy payment and fewer disputes?

## 2. Do you have views on the impact of our proposals on PSPs?

As already stated, in my opinion the impact on the receiving PSP should be far greater than that of the sending PSP.

The sending PSP is providing a mechanism for money to be sent and whilst they have a duty of care to the sender (Payer) to ensure the instruction is bone fide, often they won't be able to identify if it is a result of an app scam, unless they have recognised a trend or have specific shared information to alert them.

However, the receiving bank maintains an account for the receipt of money, this is where the proceeds of the app scam have to pass through, or sit. Whilst it is difficult to be 100% assured as the standing of the new account holder when opening an account, should this person be a perpetrator of app scams then he/she has been allowed an account, which is a necessary mechanism to perform such an act. This is why, in my opinion, the receiving bank has a far greater duty of care i.e., not to provide the ability for app scammers to move money through by giving them an account in the first place.

I accept that it is not always easy to identify app scammers at the time of account opening, but if the onus is not placed on the receiving PSPs who receive and process the proceeds of crime then account opening procedures will not be tightened and we will continue to provide the ability for app scammers to receive and use funds.

## 3. Do you have views on the scope we propose for our requirements on reimbursement?

You have specifically mentioned Faster Payments Scheme as being in scope (4.11), you also mention CHAPS (4.9). But there are other forms of payment whereby 'authorised payment' could be made e.g., Cheque, on-us. A cheque can be cleared same day now, should this not be in scope, or being given consideration?

## 4. Do you have comments on our proposals:

### • that there should be a consumer caution exception to mandatory Reimbursement

The majority of consumers don't want to be party to an app scam. Not only is there a 'potential' monetary loss but there is also a personal impact i.e. even though there might be mandatory reimbursement the consumer is never absolutely sure they will keep this until the case is fully investigated and settled. Secondly, the consumer often feels foolish and ashamed that they have been duped into a scam and so may, in the first instance, find it hard to claim and/or live with the fact that they have been duped.

Whilst my statement above would lead you to think that I don't support a 'consumer caution exception to mandatory reimbursement', there will no doubt be others who try and claim for an app scam, when a true app scam hasn't actually occurred or they have undertaken a lack of care when transacting and so **I do agree that there has to be some caution.**

Clear consumer and PSP guidelines are imperative, Bacs has honed their guarantee guidelines for years, and yet there are still incorrect claims are made, again there may be learning here.

- **to use gross negligence as the consumer caution exception**

This seems appropriate, consumers need to be aware that this is the measure and what it means to them.

- **not to provide additional guidance on gross negligence?**

Not being prescriptive means that it is left to other parties to interpret, in this case it will be the PSPs who will interpret what qualifies as 'gross negligence'. I agree that a 'case by case' basis needs to be undertaken, but interpretations can often be skewed in favour of the party providing the interpretation.

In view of this I feel that the consumer needs to be made aware what means of recourse is available should they wish to challenge a decision that 'gross negligence' has occurred.

Additionally, cases where 'gross negligence' has been deemed to occur should be recorded, monitored and analysed to check that it is not being skewed in favour of the PSPs.

**5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

This seems to be an appropriate stance.

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

It makes sense not to have conflicting definitions.

**7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to Reimbursement**

The rationale for applying a modest fixed 'excess' to mandatory reimbursement would seem an appropriate course of action.

However, the non-investigation into low value scams that results from this will not help compensate for the personal harm that may have been inflicted by the scam on the consumer both monetary and mentally. For an 'excess' to be applied the communication to the consumer needs to be clear on why an excess has been applied and that, perhaps, the claim will be logged for potential investigation at a later date if a number of similar claims is reached.

Logging the claim will allow industry analysis as to the magnitude of the lowest value claims and whether further investigation should be required.

- **any 'excess' should be set at no more than £35**

Whilst there is rationale for having an excess and this is explained, it is not clear how the actual £35 figure has been arrived at.

- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

I agree with this action.

## 8. Do you have comments on our proposals that:

- **sending PSPs should be allowed to set a minimum claim threshold**

Notwithstanding my previous comments under Q7, where I can understand the potential need for a modest fixed excess. I believe that having a 'minimum claim threshold' alongside an 'fixed excess to reimbursement' will be confusing to the consumer. A consumer is more likely to accept a single ceiling figure for which an investigation will not take place. The reasons for taking this action should be clearly stated and justifiable to the consumer. Therefore, it may be more appropriate to completely ignore the terms 'minimum claim threshold' and 'fixed excess to reimbursement' and implement a single figure below which claims will not be investigated stating clearly why and how this figure has been arrived at.

It would be interesting to understand what TSB currently do for low value claims. Unfortunately, their detailed T&C's stating whether they have an 'excess' or 'minimum claim' have proved difficult to find on the internet.

- **any threshold should be set at no more than £100**

My answer is covered in the responses above.

- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

I agree vulnerable customers should be exempted.

## 9. Do you have comments on our proposal not to have a maximum threshold?

Not having a maximum threshold creates an 'unlimited liability' to the PSP. This will probably have to be incorporated in its balance sheet and might have an adverse effect on its operational capital. I am not an accountant and so this would need to be investigated but my feeling is that it will be better to cap the maximum threshold and that £1m is more than appropriate. Capping should not exclude the PSP from investigating and settling claims larger than £1m, its just that it shouldn't have the mandatory element applied.

## 10. Do you have comments on our proposals that:

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

It would make sense to have the same 13-month time limit as claims for unauthorised payments, it is clearer for consumers when there is conformity.

With this in mind I would expect ALL PSPs to agree to the same time limit. Many consumers are multi-banked and whilst some PSPs may see it as a competitive opportunity to offer a different time limits, it would make it difficult, as an industry, to explain different time limits to a consumer if they were party to an app scam across two different accounts at two different PSPs offering different terms.

- **any time-limit should be set at no less than 13 months?**

As stated above, it would make sense to have the same 13-month time limit that we have for unauthorised payments claims as this will ensure conformity and clarity for consumers.

**11. Do you have comments on our proposals that:**

• **the sending PSP is responsible for reimbursing the consumer**

Yes, the sending PSP should be responsible for reimbursing the consumer. I have mentioned previously some of the issues that may be experienced with this model and the learning that might be achieved from the Bacs Direct Debit Guarantee.

• **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

This is fully supported as a target for the majority of claims! However, complex claims may understandably take longer than 48 hours, as long as the consumer has been advised of this extension (perhaps advised of a next contact date), I see no problem with extending this period.

This does make me wonder whether there should be a mention that if a claim is paid within 48 hours and then subsequently proved that a first party fraud or gross negligence has occurred that the PSP has immediate recourse to the money paid under the claim and could take legal action against the party concerned.

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

I think that we have to accept that not all decisions can we made within the proposed 48 hours. Whilst this should be the target there will be some claims that are more difficult to investigate, especially those where sizeable amounts or where complex processes have been undertaken.

These will require high levels of investigation to ensure that gross negligence or first party fraud has not occurred and each case needs to be judged on its own merits. A PSP will need to build a clear case and provide strong evidence to prove that gross negligence or first party fraud has occurred and this will take time! Each case will have to be judged on its own merits; whatever additional time is required should be conveyed to the consumer with a clear timeline to completion. The PSP should audit their performance against the timelines provided, which should be 'realistic' in length.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

I am accepting of a 50:50 split as I think this will lead to easier sender/receiver PSP acceptance. However, I restate my comments from the 'General views' section in my response that **the split should fall more heavily on the receiving PSP (75:25)** as they should not be harbouring accounts that support criminal activity.

If PSPs had more thorough account opening procedures, then they would reduce the accounts that are used by criminals. They have an obligation to stop their own accounts being used by criminals as this would stop criminal activity at source i.e. nowhere for the money to go!

As for existing accounts that are in use today, I can understand why 'blocks' are not always placed on these accounts but preventing their use and then preventing new accounts being opened prevents criminal activity.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

Departing from the agreed 50:50 split by negotiation, mediation .... is not a good idea in my opinion. This will add another layer of bureaucracy to the claims process.

I suggest that a figure is set and agreed as the default. Of course, on the rare occasion and if there are very strong grounds that the split should have been different to the default then this should be negotiated, but this negotiation should only happen AFTER the receiving PSP has settled their initial share of the costs (50%) i.e. if proven the default was incorrect they will get a refund.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

This is going to be really difficult and will not be a catch-all. I think that this is one for the schemes/Pay.uk rules and governance committee to work out. Historically, Faster Payments has been in a silo, but now under Pay.UK and with the formation of the New Payments Architecture it should have a much wider remit.

However, I can't see them as being able to fully oversee areas such as Crypto Wallets, because unlike bank accounts the Crypto Wallet is not necessarily a product of PSPs (there are specific companies set up as 'wallet providers'). I am aware that some PSPs are now offering Crypto Services (and storage), there may be opportunities to bind those PSPs in through Faster Payments route, but this would not be a catch-all.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

Yes, I agree with this proposal. Obviously, were there to have been an agreement to depart from the 50:50 (see my answer to Q14) the repatriation should be made on that basis.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

I agree with the scope

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

It makes sense for Pay.UK to become the PSO in the long term.

However, as identified, Pay.UK is limited in the areas where its rules currently have jurisdiction (it doesn't cover crypto wallet).

You have talked specifically about Faster Payments and it is not clear in 6.10, when you talk of 'comprehensive scheme rules', whether this is solely 'Comprehensive' Faster Payments rules or whether it includes other schemes at Pay.UK as well.

Obviously, the greater number of schemes and the wider the membership and remit that Pay.UK has; then the wider they will be able to impose rules on their members/users.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

It makes sense to implement a minimum initial set of Faster Payment scheme rules, which can be built upon at a later stage.

I have already highlighted my concerns with implementing any methodology that allows a move away from a pure default cost allocation, I believe that the default allocation should be mandatory and settled as soon as the claim has been settled. Only at this point and if there is a dispute, should the 2 parties negotiate and use further methods to come to an arrangement.

I also think that it would be beneficial if the Faster Payment scheme rules were able to incorporate PiSPs, whilst I have said that the majority of the onus should be on the receiving PSP (preventing criminal accounts), anyone initiating a payment does have obligations and so should be bound to pay their share of the costs.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

Using powers under FSBRA S55 would seem to be the most effective way to get the required rule amendments. However, before doing so there is a need to be clear on whether solely changing the Faster Payments scheme rules will sufficiently capture all the parties that initiate and receive payments linked to app scams e.g. PiSPs might not be included.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

As I have already stated, I would have concerns with anything that offers additional up-front options to the default position. Especially, when they are left to potentially conflicting parties to resolve prior to reimbursement settlement. In my opinion the default position should be imposed and settled immediately, only after settlement should negotiation take place over re-apportionment of the default. This should ensure that there is no adverse impact on the claim due to warring factions.

Implementing to this effect, in the scheme rules, should work and benefit the process.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

As you rightly point out, it will require an effective system to monitor compliance. As I have said previously, there must be some learning from how the DD Guarantee scheme and how parties are monitored under that system as to performance of the KPIs in place.

Ultimately, there needs to be an automated means of monitoring performance not just for Pay.UK but for PSPs so that they can see their performance and set targets for improvement. However, a manual system can and should be implemented at the outset if an automated one cannot be readied for the start date.

One key area of monitoring will be disputes, especially where agreement cannot be reached on the reimbursement allocation. This has to happen whether my suggestion of post default reimbursement allocation happens or whether you allow negotiation pre reimbursement allocation.



**23. Do you have views on the costs and benefits of Pay.UK implementing a realtime compliance monitoring system and when it could be introduced?**

This is covered in the answer above (22.).

**24. Do you have views on the best option for short-term enforcement arrangements?**

Pay.UK has historically lacked power in enforcement of scheme rules. Naming and shaming seems to have been used in the past and this has worked to a degree. Issues can arise when it is a 3<sup>rd</sup> party of the scheme member who is at fault e.g. a corporate submitting direct (indirect participant) or banks with them.

Pay.UK's relationship is with the PSP through the scheme and not the corporate, meaning enforcement of rules becomes the responsibility to the PSP and leans on their relationship with the corporate (3<sup>rd</sup> Party), this can lead to issue that prove difficult to resolve especially if the PSP wishes to maintain a positive business relationship and might not want to enforce a costly change or impose sanction on their customer.

In view of this Pay.UK should have responsibility for enforcement, but for them to be powerful enough to ensure far-reaching compliance i.e. they need to have powers over 3<sup>rd</sup> parties. Perhaps the rules should be extended to include indirect participants, after all they also have impacts on the scheme.

As this is unlikely to be the case, in the short term it is more than likely that the PSR will have a role to play in this area and will require suitable reporting from Pay.UK.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

This is covered above (24.).

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

My view is that direction should be made direct to the indirect PSPs. In my answers above I feel that I have explained why I think there would be a risk placing reliance on an IAP. You have also identified this in 7.34.

Unless Pay.UK is given powers to impose sanction directly on indirect PSPs, then it has to be the PSR who does this and you have to do it direct on the indirect PSP and not through the IAP for the reasons mentioned above.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

I have covered everything in my earlier answers.

**28. Do you have any other comments on the proposals in this consultation?**

No.

# Larkfleet Group

I had a situation about 18 months ago where my company was subject to a fraud and that illustrated a number of things that I think as the Small Business Minister, you should be aware of, regarding changes, that I would suggest should be part of amendments to help businesses that don't hit the small company threshold, where those businesses get some help, but for businesses over the turnover threshold there is nothing. I will illustrate what happened so you can realise the issues that need to be addressed for small, medium, and large companies that meet the EU company definition of small businesses, which we did, based on 1) turnover, 2) asset value, 3) and/or employees. If 2 and 3 are not met, then that is okay as an SME.

1. The fraud happened by a scammer cloning the HSBC bank phone line and masquerading as an HSBC employee. The most remarkable things are that one of my staff actually checked the number and confirmed that it was HSBC, but what was more remarkable to me was that it was the HSBC number phoning. The reason the scammers were able to succeed was due to the fact that they relied upon the HSBC phone line, i.e., the actual line always being delayed and not answered straight away. So, people in a situation where the fraud line is never answered panic and give up waiting on the line. That is what happened in our scenario where one of my guys checked the line, it was HSBC and then when he tried to phone and deal with it, the line was engaged and so he was sure that it was HSBC calling. As part of the system, he then gave information out to one of our accounts, which helped the scam to work. Long story short, we potentially lost an amount of money which was initially £1 million but managed to reduce this to £176,000 by fortunately putting a stop on the last balance transfers just before they went out. It was horrendous but not as bad as it could have been.
2. The summary of the issues that I think may be relevant in trying to get HSBC to then check with the other banks that received the money (there were approximately 30 transactions with a number of banks), all of the mainstream ones claimed confidentiality and frankly couldn't be bothered to follow up the lost money, so after 1 year of chasing, HSBC came back and said sorry, none of the banks will answer, none of the banks will pursue it because of confidentiality!
3. There is no banking ombudsman, nor any FCA help for medium sized companies above a certain level, therefore, there is no help to follow up and query anything and this is only in place for personal and very small companies. I have tried to speak to everyone, but they have no jurisdiction over a certain level. We tried to go through the BBRS (Business Banking Resolution Service) however, they were unable to take on our case due to the level of turnover at the time of the fraud. The following statement is what we were told by the BBRS - **As discussed today, we have to assess the eligibility of your complaint. I did advise you that referring to the financials of your business, it appears that your business far exceeds the upper financial limits of a business that the BBRS can consider a complaint for. As discussed the financials being between £2 million – £10 million for the total annual turnover and between £2 million-7.5 million for the total assets for any complaints made after 1 April 2019.** I have spent a long time getting nowhere with HSBC, as they believe it is

not their issue, and then the other banks just all completely wiping their hands of the matter.

4. My suggestion would be that for companies of a certain level there has to be an independent body at the FCA that can cut through the banks claiming confidentiality because these scammers and fraudsters are getting away with it and will keep doing so. The banking system looks after each other and won't bother to claim or check where the money has gone because if they do, then the whole banking system must do it. So, every single bank Kevin, hides behind the fact that if none of them have to do anything and they all claim confidentiality, people like me give up because there is nowhere to go. There has to be a system so the banks have to follow up and find the missing money whilst losing the scammers down. Also, their 'know your client' regulations should enable them to do so. They should and can pursue them if they did their job properly in the first instance.
5. In my instance I did have insurance, or so I thought, but then when I went to claim from the insurers, they said that the fraud was partly due to a breakdown in HSBC's system because they were cloned and therefore, they would not cover the loss, so they claimed it was due to HSBC's system failure. HSBC have said, well it's not our problem we have been cloned. Therefore, I am trying, as a matter of principle, to pursue HSBC on the basis that their system was cloned, they advertised a number that was not fit for purpose, albeit probably not their fault in this instance because someone had taken over their number. I did ring the number the day after the fraud to find that I eventually got through to HSBC on the same number that the scammers were using and so I could see what had gone on and happened. Again, I was delayed and obviously waited to see how long it took for the line to be answered which was a fair time and if you were in the middle of having all your money taken from your bank, you would not hang on that long. I wanted to check that the number did go through, which then allowed me to conclude that the fraud was down to the banking system fraud line being too busy and no one answering it. Therefore, the scammers are relying upon that as the route of the scam, but I have no idea if there has been any improvement.
6. In this instance, although I am not sure it would be universal, the relationship manager at HSBC didn't know any other number but the fraud number that is on the website and so my team were trying to get hold of that number and couldn't even get any details after there was a suspicion that something was going on because we couldn't get through. Eventually, one of my guys did ring the relationship manager again to get a different number which I have proposed should be there for all corporate customers, so they don't have to go through the main line when it could be a long waiting time. We got the account closed, which fortunately, managed to stop approximately £800,000 of money leaving my account to go into the scammer's accounts. However, unfortunately we couldn't get the approximately £200,000 stopped and so that went through. For your information on a private and confidential basis, the banks that received that money were as follows:
  - Clearbank Ltd

- Nationwide Building Society
- Santander
- Halifax
- Barclays
- Bank of Scotland
- The Royal Bank of Scotland
- TSB

There were approximately 30 transactions that made that value throughout these banks.

These banks all categorically refused to acknowledge anything or do anything to try and find where that money has gone. I am putting the loss on HSBC again, that they need to put pressure on because if those banks, as well as HSBC open bank accounts with the regulatory requirements of 'know your client' all of those banks should have known who opened the account and what and where they are because they should all of had passports and other personal information that would allow you to contact and trace them later. To be honest there are still banks who open without any of that, albeit that is now only a few, and that allows the scammers to open with minimal information and then be able to disappear quickly. I hope that most of the larger banks now are much better. I know from my own experience that if I open a bank account with HSBC, it takes me a couple of months because they need to go through their 'know your client – KYC' information and then that presumably allows them to trace a fraudster if they have done something similar because they should be able to find them. Whether they or any of the other bank's bother, I don't know, but turkeys don't vote for Christmas, albeit this year some of them won't get a chance!

In my experience, the banks must be forced to deal with this and have an independent body and not hide behind the confidentiality and do nothing at all. HSBC are just as bad as all the others because they have all got a protected group whereby if none of them do anything and claim confidentiality people like me will just give up, and in the end I either lose the money or I am insured. In my situation my insurer is blaming HSBC's cloned line because why should they be advertising a phone line that isn't theirs, or they can't regulate. I then have a problem with the insurance company saying, well how are we supposed to deal with a line that we thought was a genuine line, but it has been cloned and taken over by a scammer. We think we are dealing with HSBC, but in fact it isn't HSBC at all. I don't know what can be done about this, because I haven't been able to get HSBC to see how they can interpret their line being used and cloned. That is something that is ongoing.

7. The summary of all of this is that businesses that are scammed should under the banking and FCA regulations have an independent body that examines the claim so that the scammers are followed up, and those banks that don't have systems in place should check the bank account openings. Also, those banks that just open the accounts without doing any proper due diligence should be named and shamed because they are the ones who allow the scammers to get away with it. Those banks that are regulated by the FCA should be accountable for the money and where it

goes, and they shouldn't be able to just claim immunity by all working together to stop and not check where the money has gone. If they were made to do that or had an independent body they wouldn't be able to claim that they can't do it because even the scammer has confidentiality and therefore, it is sorry, we can't do anything. They all have teamed up to give the same answer so people like me just get nowhere and it is illustrated that this is a massive issue and needs to be dealt with urgently, because this must be happening all round the country.

This is completely unfair and unreasonable, and the banks should not be able to get away with it, they should be made to open accounts properly, they should be made to follow up on where the money has gone, and they should be sent to the fraud squad to pursue these people to stop them doing it again. By allowing them not to be pursued and letting them keep the money is almost encouraging them to do it again, it just seems farcical and unreasonable. There is no system for the banks to be accountable or to follow up, they are getting away with it and people just don't know what to do like me. I am the kind of guy that is not prepared to accept that so I am carrying on with HSBC and I am trying to see if I can get the FCA to investigate it to see whether they can change the rules to protect businesses above the threshold which are multiple. Those where the insurance companies will not pay out, even if there is a fraud when they blame the banks internal system, which again, we can't do anything about because they have been scammed as well. You can see the nightmare scenario that goes on and which needs dealing with.

8. I thought as a fair bank trading guy and a Small Business Minister you may well be interested in looking at how this can be dealt with because I suspect it is a massive issue and I have just highlighted the depth of the problem. I can't be the only person it must be rife. I have got nowhere with HSBC, and one of the areas that probably most companies don't realise is that you need your bank on your side, and complaining is not great! Therefore, you dare not start a situation like this because the banks will probably then take it out on you, not matter what they say, and you know that as well as me.

I am in a fortunate position where I have sold my main housing business and I have launched Phoenix which is my sustainability business looking at green businesses, green agendas and low carbon technologies so I don't need to worry about HSBC and what they might do me, as I don't need them as much. I am therefore prepared to go out on a limb, one to try and see if I can get my £178,000 back but secondly to try and help other people who can't take the same stance. I could do with some help in trying to get the FCA to investigate and see whether they would put something in place as an independent body for businesses above a certain threshold, for those banks that have transferred this money to follow up, and make sure that their systems are in place to find these scammers and bring them to justice, so they can't keep doing this. The system now just allows them to re-do it and there is no accountability whatsoever, that has to be wrong!

Anyway I hope my ramblings have not been too complicated but I know that you will look into it, and I know that you will try and see that fairness is done. I am not looking to name

and shame any banks; I am not looking to do anything other than make sure that their systems are in place to catch these people. They have an obligation to catch them, and they don't hide behind the fact that all of them get together and all agree confidentiality knowing that the FCA has no policy for businesses above that threshold and they know that the FCA won't do anything. The FCA should also have legislation or a mechanism for mediation or arbitration that can stop the banks hiding behind confidentiality. I know that you can probably do that, but it may be that you need to involve larger businesses because they will be bound by the same issues, because above that certain level there is no recourse, in my experience, to go anywhere and do anything and the FCA just have no interest as they have no policy or mandate on it, so I will hopefully get some feedback from you.

If you want me to help in any way, because all I want is fairness and justice, then please do get in touch. If I can get my £178,000 back then that will be great, but also if I can stop this happening again for other businesses who probably are not as able to influence and do something.

Also, under the definition of SME the criteria regarding assets, turnover and employees do make largish companies, like I was, so I would suggest that a lot of UK small businesses fall under the companies act definition.

# Law Society of Scotland





Law Society  
of Scotland

# Consultation Response

CP22/4: Authorised push payment (APP) scams:  
Requiring reimbursement.

November 2022



## Introduction

---

The Law Society of Scotland is the professional body for over 12,000 Scottish solicitors. With our overarching objective of leading legal excellence, we strive to excel and to be a world-class professional body, understanding and serving the needs of our members and the public. We set and uphold standards to ensure the provision of excellent legal services and ensure the public can have confidence in Scotland's solicitor profession.

We have a statutory duty to work in the public interest, a duty which we are strongly committed to achieving through our work to promote a strong, varied, and effective solicitor profession working in the interests of the public and protecting and promoting the rule of law. We seek to influence the creation of a fairer and more just society through our active engagement with the Scottish and United Kingdom Governments, Parliaments, wider stakeholders, and our membership.

Our Consumer Law and Mental Health and Disability Law sub-committees welcome the opportunity to respond to the consultation from the Payment Systems Regulator – CP22/4: Authorised push payment (APP) scams: Requiring reimbursement<sup>1</sup>.

We have the following comments to put forward for consideration:

## Consultation questions

---

### **Question 1. Do you have views on the impact of our proposals on consumers?**

We support the proposals, and we consider that authorised push payment scams are a significant and a very serious issue for consumers, as the financial losses can be significant and high in value, and there is often no redress or remit for protecting consumers from high value scams. We support the proposals.

---

<sup>1</sup> [CP22/4: Authorised push payment \(APP\) scams: Requiring reimbursement | Payment Systems Regulator \(psr.org.uk\)](https://www.psr.org.uk/consultation/cp224)

## **Question 2. Do you have views on the impact of our proposals on PSPs?**

We believe this will have a significant impact on financial firms, as the proposals may incentivise PSPs to improve their procedures and we support the 50/50 split repatriated funds between the sending and the receiving PSP.

## **Question 3. Do you have views on the scope we propose for our requirements on reimbursement?**

We are happy with the current scope of the proposals on reimbursement subject to the event where consumers are experiencing an accumulation of scams. However, in some cases, the £100 limit may not be high enough where consumer(s) are experiencing a high volume and accumulation of scams.

## **Question 4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**

We are comfortable with this.

- **to use gross negligence as the consumer caution exception**

We are comfortable with this.

- **not to provide additional guidance on gross negligence?**

We believe that additional guidance should be provided.

### **Question 5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We think this is reasonable.

We also consider that the proposals fail to recognise that where a vulnerable person lacks capacity in relation to the transaction leading to the loss, in Scots Law the transaction was a nullity, and the position must be restored. This is a basic concept of Scots Law, but not the law of England and Wales. We believe that consultation and the proposals do not address the situation where a vulnerable person may have a guardian with authority in relation to financial matters who had not authorised the transaction. The focus of the consultation is on vulnerability arising from personal circumstances, which implies external circumstances, however we consider that no account appears to have been taken of 'internal factors' such as impaired capacity.

### **Question 6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

We note that the FCA's definition of a vulnerable consumer<sup>2</sup> allows for a consistent approach, however we are concerned that the FCA's definition of a vulnerable consumer is too vague. We believe that additional clarity maybe required, which must be consumer friendly and workable.

### **Question 7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**

This seems reasonable and practical.

- **any 'excess' should be set at no more than £35**

This seems reasonable and practical.

---

<sup>2</sup> [FG21/1: Guidance for firms on the fair treatment of vulnerable customers \(fca.org.uk\)](https://www.fca.org.uk/guidance/fg21-1)

- **PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?**

This seems reasonable and practical.

#### **Question 8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**

We consider that the proposals in point i and ii are at odds with each other.

- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

We support exempting vulnerable consumers, however we are concerned that it is voluntary. If PSPs do this on a case-by-case basis, we think it will be difficult to know whether an exemption should be legitimately applied. This will be particularly difficult if a vulnerable person is having to advocate for their cause. We consider that perhaps PSPs should be required to publish a policy on the application of such exemptions?

#### **Question 9. Do you have comments on our proposal not to have a maximum threshold?**

We have no comment to make.

**Question 10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

We think this seems reasonable and is consistent with the PSR's.

- **any time-limit should be set at no less than 13 months?**

We think this seems reasonable and is consistent with the PSR's.

**Question 11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**

We think this seems reasonable and is consistent with the PSR's.

- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We think this seems reasonable and is consistent with the PSR's.

**Question 12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

We cannot really comment on this however we feel that the balance of probability and reasonable grounds are factors that should be considered.

**Question 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

We support this.

**Question 14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We think this seems reasonable.

**Question 15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

We have no comment to make and consider that this is a matter for PSPs to comment on.

**Question 16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

We have no comment to make.

**Question 17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We have no comment to make.

**Question 18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

We support this and it seems reasonable.

**Question 19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

We have no comment to make.

**Question 20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We have no comment to make.

**Question 21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

We have no comment to make.

**Question 22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

We believe this seems reasonable and we consider that it is important to ensure that Pay.UK can set appropriate incentives for compliance with the compliance monitoring scheme (e.g. encouraging self-reporting) and sanctions for non-compliance with the monitoring scheme (e.g. financial penalties for failure to provide, or late provision of information).

**Question 23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We have no comment to make.

**Question 24. Do you have views on the best option for short-term enforcement arrangements?**

We have no comment to make.



**Question 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

We have no comment to make.

**Question 26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

We have no comment to make.

**Question 27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

We have no comment to make.

**Question 28. Do you have any other comments on the proposals in this consultation?**

We consider that paragraph 4.13 does not address the situation where a consumer is a victim of doorstep crime/ bogus callers. Consumers can often be misled into paying substantial sums of money to a supplier/ trader who appears to be genuine and legitimate for building works, for example. However often the supplier/trader fails to undertake any work(s), or the work is defective and incomplete. In such circumstances, consumer(s) are often dissatisfied in with the supplier/ trader, as it is unlikely that the trader or supplier will return to complete the service or supply the goods. The supplier or trader appears to be genuine through their appearance, liveried van, flyers, business address etc. however the trader's business address is false, and the trader is not based within the locality.

Whilst the dispute has a civil element to it, there are often criminal offences under consumer protection legislation. We believe that the scope of the proposals could be extended to cover doorstep crime/ bogus callers, where the consumer has paid money by bank transfer at the inducement and request of an illegitimate supplier and/or trader, as consumers are often pressurised into paying monies for goods and/or services.

**For further information, please contact:**

[REDACTED]  
Policy Team  
Law Society of Scotland

[REDACTED]  
[REDACTED]

# Leeds Building Society

**Leeds Building Society response to PSR consultation paper (CP22/4), Authorised Push Payments scams: Requiring Reimbursement, September 2022.**

We're overall supportive of industry improving approach, technology but current proposals have a political bias to implementing a no consumer risk approach which will have unintended negative wrong way risk consequences which need to be carefully thought through so there is consistency across industries and broader economic alignment to fight financial crime etc

*This response doesn't contain any material which we'd call out as commercially confidential or sensitive.*

**Question 1: Do you have views on the impact of our proposals on consumers?**

- Potential for impact on financial inclusion – some PSP's may assess consumers as too high risk to have access to retail banking products with full payment services.
- Mandatory reimbursement may lead to increased moral hazard with consumer comfort around payments increased.
- There is an increased risk of friendly fraud / first party fraud – the actual reimbursement mechanism being mandatory may create its own fraud risks (i.e. abuse).
- PSPs will have to introduce additional friction into payment journeys, we anticipate this will impact a lot of consumers, may increase the volume of Banking Protocol invocations and be littered with unintended consequences such as lost opportunities along with an increase in customer dissatisfaction.
- APP fraud has cost the industry an average of £500m annually since 2020, these losses may increase as a result of mandatory reimbursement and the anticipated increase in moral hazard of individuals. This will impact portfolio pricing and result in reduced consumer value in product offering across the industry to allow PSPs to cover costs. Given the current economic climate firms need to be encouraged to pass value back to consumers. Increasing operating costs (especially where firms cannot reasonably be expected to prevent all fraud/scams) will have detrimental impact on all consumers.

**Question 2: Do you have views on the impact of our proposals on PSPs?**

- Potential competition issues specifically relating to the Direct / Indirect model and the impact this may have.
- The outlined proposals will take significant investment to implement which WILL NOT be offset by a reduction in losses for firms with lower risk product portfolios (as it will be with the tier 1's).
- APP fraud has cost the industry an average of £500m annually since 2020, these losses will increase as a result of mandatory reimbursement and the anticipated increase in moral hazard of individuals. Shifting these operational losses almost entirely to PSPs will result in burden that some smaller firms are unable to bear, and may result in reduced enterprise across the industry – ultimately stifling innovation and competition.

- This policy will introduce additional friction into payment journeys in efforts to slow or stop payments, directly counter to the objectives of the scheme/regulators to reduce friction in payment journeys. PSPs may fear potential repercussions without clearer guidance.

**Question 3: Do you have views on the scope we propose for our requirements on reimbursement?**

- Places no onus or incentives on enabler services (i.e. Social Media) which sit outside of the industry for their part in consumer detriment.
- The scope doesn't consider 'No-Blame' cases. PSPs will be held liable for scams which could not reasonably be expected to be prevented by the PSPs involved.
- The scope does not account for the inevitable shift of scam payments from FPS to alternative payment methods, i.e. we've seen victims request both cash and cheque withdrawals. The goal of the policy is to reduce fraud and scams not to transfer the risk to other channels or payment methods.

**Question 4: Do you have comments on our proposals:**

- that there should be a consumer caution exception to mandatory reimbursement
- to use gross negligence as the consumer caution exception
- not to provide additional guidance on gross negligence?
- Gross negligence must be clearly defined to ensure consistent application across the industry. Reliance on the FCA definition is unhelpful as is already subject to different interpretations and application across the sector.

**Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

- Customer vulnerability must have some clearly defined parameters (to ensure that claims of vulnerability are not abused in order to secure reimbursement) to ensure that assessments, if multiple firms are involved, are consistent. By definition, if victims of scams were vulnerable at a point in time, this could lead to automatic reimbursement and deter firms from carrying out full investigations – leading to poor practice and risk management.

**Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

- Customer vulnerability must have some clearly defined parameters to ensure that claims of vulnerability are not abused in order to secure reimbursement and assessments, if multiple firms are involved, are consistent. By definition, victims of scams were vulnerable at a point

in time; this could lead to automatic reimbursement and deter firms from carrying out full investigations – leading to poor practice and risk management.

**Question 7: Do you have comments on our proposals that:**

- sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement
- any ‘excess’ should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?
  - Any potential excess should be fixed, mandatory and consistent across all PSPs, or this could lead to challenges when sending and receiving firms are accounting liability split based on appetite; unless the remitting firm is always intended to benefit from the excess.
  - Our view is that £35 excess will do little to manage moral hazard on the part of individuals.
  - If excess is to be applied, the Society’s agrees it should not be applied to vulnerable customers (subject to clear definition on vulnerability).

**Question 8: Do you have comments on our proposals that:**

- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?
  - Any potential minimum threshold should be fixed, mandatory and consistent across all PSPs, or this could lead to challenges when sending and receiving firms are accounting liability split based on appetite.
  - Our view is that £100 as a minimum threshold will do little to manage moral hazard on the part of individuals.
  - There is a risk that APPs under the minimum threshold could go unreported, resulting in reduced visibility and an inability to measure the true scale of the problem.
  - If minimum thresholds are to be applied, the Society’s agrees it should not be applied to vulnerable customers (subject to clear definition on vulnerability).

**Question 9: Do you have comments on our proposal not to have a maximum threshold?**

- A maximum threshold would help to minimise the impact of and protect against any potential abuse of the policy.
- A maximum threshold could serve as a more effective means to manage any moral hazard risks.

**Question 10: Do you have comments on our proposals that:**

- sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
- any time-limit should be set at no less than 13 months?
  - The Society agrees with a set time limit and that 13 months seems proportionate.
  - Any time limits should be fixed, mandatory and consistent across all PSPs, any sending PSP that were to operate outside of the 13 month window (i.e. greater than) would assumingly accept 100% liability as the receiving PSP may only operate to the 13 month time limit.

**Question 11: Do you have comments on our proposals that:**

- the sending PSP is responsible for reimbursing the consumer
- reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?
  - 48hrs to reimburse from customer claim is operationally challenging when trying to effectively establish any risk/concern of first party fraud or gross negligence. Exceptions must be placed where the victim is unable or unwilling to fully cooperate with the investigation. In addition complexity of case must provide allowance for additional time to properly investigate acquired evidence and potentially liaise with multiple parties. Failure to carry out full investigations will lead to abuse of the policy/scheme and first party fraud.
  - Setting aside 'complex vs bad investment' cases the Society considers 5 working days a more proportionate (and realistic) timeline in order to complete a full investigation prior to refunding a claim. These may not be as easy to prove / disprove unlike traditional frauds.
  - Time limits should be quoted in business days rather than hours to allow for the different operating hours of PSPs and to cover Bank Holidays.

**Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

- Gross negligence is a conscious and voluntary disregard of the need to use reasonable care and diligence before carrying out an action, in these instances a transaction. Scenarios that could require more time to investigate may include;
  - Where the promise of goods/service/return on investment are significantly greater or lower than market average for those goods/services/investments.
  - Where the individual has demonstrably and/or wilfully ignored warnings alerting them to the risks directly relevant to the scenario faced.
  - Where the means of communication are atypically for the associated goods/services/situation – i.e. unsolicited social media direct messages for large investments opportunities.
  - Where it becomes apparent that little to no care/due diligence has been carried out by the victim in scenarios of increased complexity and/or are considered atypical.
- The Society considers 35 days a more proportionate timeline where concerns of first party fraud or gross negligence exist.

**Question 13:** Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

- 50:50 split puts increased operational burden on both sending and receiving PSPs when managing recovery & disputes.
- 50:50 split shifts significant costs to the receiving firm that have inherently less opportunity to detect and prevent the risk, especially in cases where mules are being utilised. An alternate split in favour of the receiving firm should still provide appropriate incentive.

**Question 14:** Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?

- The Society does not have a strong view on this proposal, however notes that any such criteria must be proportionate to the differing risk profiles of varying PSP's. It would not be reasonable to expect low risk providers to meet the same standard of firms with larger payments footprints.

**Question 15:** Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?

- All firms in the chain should be incentivised to recover funds and manage the associated risks, however dispute resolution and calculation of liability could be greatly extended dependent on the number of PSP's in the chain. This comes with increased operational burden through the chain and some PSP's may wish not to pursue values outside of their own appetite.

**Question 16:** Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?

- Repatriated funds should be reallocated to receiving PSP up to the value of their liability, given the onus and cost is upon that firm to recover. Any funds recovered above the receiving PSPs liability should be returned to the sending PSP – this will best incentivise recovery of funds against each firm's accountability and appetites.

**Question 17:** Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?

- **Agreed**



**Question 18:** Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?

- Pay.UK has limited rulemaking and enforcement powers over the direct participants' relationships with consumers, it has none over the indirect participants, essentially creating a two-tier approach within the PSR proposal. The PSR would be better placed with existing enforcement powers across participants.

**Question 19:** Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?

- The Society does not have a strong view on this proposal, however notes that any such rules must be proportionate to the differing risk profiles of varying PSP's.

**Question 20:** Do you have views on how we should exercise our powers under FSBRA to implement our requirements?

- The Society does not hold a view on this proposal

**Question 21:** Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?

- The criteria, whilst fair, doesn't offer any practical guidance on how this will be managed and leaves this open to PSP's/PSO to determine.
- Consideration for all PSP's on obtaining or securing dispute resolution specialists - this could be costly and vary widely across all PSP's and smaller firms may struggle to cover costs alongside increased reimbursement costs, increased prevention and operational costs to meet requirements.

**Question 22:** Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?

- It would be important to ensure that Pay.UK has the relevant capacity and capability to conduct the administration and enforcement of the reimbursement rule as outlined by the PSR.

**Question 23:** Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?

- It would be important to ensure that Pay.UK has the relevant capacity and capability to conduct the administration and enforcement of the reimbursement rule as outlined by the PSR.

**Question 24:** Do you have views on the best option for short-term enforcement arrangements?

- Pay.UK has limited rulemaking and enforcement powers over the direct participants' relationships with consumers, It has none over the indirect participants, essentially creating a two-tier approach within the PSR proposal.

**Question 25:** Do you have views on the best way to apply the rules on reimbursement to indirect participants?

- Agreed

**Question 26:** If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?

- See response to question 18

**Question 27:** Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?

- This doesn't consider the wider impact on consumers who do not fall victim to APP scams; APP fraud has cost the industry an average of £500m annually since 2020, these losses may increase as a result of mandatory reimbursement and the anticipated increase in moral hazard of individuals. Shifting these operational losses almost entirely to PSPs will result in burden that some smaller firms are unable to bear, and may result in reduced enterprise across the industry – ultimately stifling innovation and competition. Additionally, this will impact portfolio pricing and result in reduced consumer value in product offering across the industry to allow PSPs to cover costs. Given the current economic climate firms need to be encouraged to pass value back to consumers, increasing operating costs (especially where firms cannot reasonably be expected to prevent all fraud/scams) will have detrimental impact on all consumers.

**Question 28:** Do you have any other comments on the proposals in this consultation?

# Lending Standards Board

PSR APP Scams Team  
Payment Systems Regulator  
By Email

Lending Standards Board  
Salisbury House  
29 Finsbury Circus  
London, EC2M 5QQ

23 November 2022

Dear PSR APP Scams Team,

**Our response to the PSR consultation on Authorised Push Payment (APP) scams: Requiring Reimbursement (CP22/4)**

We welcome the opportunity to respond to the PSR's latest consultation on Authorised Push Payment (APP) scams. We are responding as the organisation responsible for the governance and oversight of the Contingent Reimbursement Model Code for Authorised Push Payment Scams (the CRM Code).

**About the Lending Standards Board**

The Lending Standards Board (LSB) is the primary self-regulatory body for the banking and lending industry, driving fair customer outcomes within financial services through independent oversight. Our [registered firms](#) comprise the major UK banks and lenders, credit card providers, debt collection agencies and debt purchase firms.

We work with our registered firms to achieve fair customer outcomes through our oversight of:

- The Standards of Lending Practice for personal customers
- The Standards of Lending Practice for business customers
- The Standards of Lending Practice for business customers – Asset Finance
- The Access to Banking Standard
- The CRM Code

Adherence to our Standards of Lending Practice and the other codes of practice which sit within our remit is a clear indication that a registered firm is committed to best practice in the treatment of its personal and business customers.

Our Standards and Codes sit alongside statutory regulation and help ensure fair customer outcomes by helping to raise industry standards and by setting standards where there is no existing statutory regulation. The Standards of Lending Practice for business customers are [recognised](#) by the FCA, providing firms and their customers with confidence that the firms applying the Standards are acting in a manner that the FCA deem a proper standard of market conduct.

## The CRM Code

In relation to the CRM Code, the LSB's role is to: monitor signatory firms' implementation and ongoing adherence to the Code; ensure its effectiveness; and maintain and refine it, as required.

Since taking on responsibility for the governance and oversight of the CRM Code in 2019, we have undertaken a significant amount of work across our compliance, policy and insight teams. We have undertaken four themed reviews looking at firms' adherence to the requirements of the Code, the findings from our most recent review were published in [September](#) this year.

We have also taken steps to improve the CRM Code. We have introduced new governance and oversight provisions into the Code, activated requirements for signatories to implement Confirmation of Payee, strengthened the requirements around communicating with customers, and updated the practitioner guide which accompanies the Code to include further examples of good practice. We have undertaken further work to develop provisions which more clearly draw out responsibilities for receiving firms under the Code. Further information on this work will be published in due course.

We also provide training and insight for firms signed up to the Code to ensure they are continuing to improve the way they are supporting victims of APP scams. For instance, we have recently commissioned Britain Thinks to undertake a piece of research looking at effective warnings, the findings from which will be published in due course.

As part of the [2020 CRM Code review](#), we collected data from Code signatories to inform our understanding of the impact of the Code in its first year. This showed that, during the first half of 2019, customers who had reported APP scams were getting back 19% of funds lost. This figure rose to 41% during the first year of the LSB's oversight. The latest [data from UK Finance](#) shows that CRM Code signatories are returning 60% of the funds to customers who have fallen victim to APP scams. The CRM Code has, therefore, had a significant positive impact for consumers in the three years it has been in place. The introduction of APP scam prevention, assessment, and reimbursement processes by the firms signed up to the CRM Code has represented a significant change for the industry and a step change in customer protections. It has improved the prevention and detection of APP scams. It has seen the support offered to victims of APP scams improve significantly and has seen more customers reimbursed where they have lost money. We hope the information in our response will support the regulator to develop a solution that builds on the success on the CRM Code.

## Our response

As the body responsible for the governance and oversight of the CRM Code, we recognise the enormity of the task facing the PSR in taking forward APP scam measures in line with the requirements that are set to be introduced through the Financial Services and Markets Bill.

We understand the approach the PSR has chosen to take in relation to APP scams and recognise that the position of the regulator is that levels of reimbursement need to be higher and more consistent across industry. Our response to the questions and proposals set out by the regulator have been informed by our experience and our knowledge of APP scams gained through our oversight of the CRM Code.

**A new independent standards framework that builds on the success of the CRM Code**

The LSB strongly believes that the improved customer outcomes and protections achieved through the CRM Code should be maintained and built upon in a new or recast industry code. To that extent, alongside any regulatory framework on reimbursement, there should remain an independently overseen standards framework for firms which captures and builds on the conduct elements of the CRM Code. This framework would complement a mandatory reimbursement rule, would allow existing CRM Code firms to commit to maintaining a focus on good customer outcomes, and would allow a wider base of firms to sign up and benefit from the good practice developed under the CRM Code.

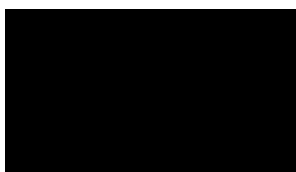
This approach would ensure that firms would be supported in their efforts to meet the high industry standards that many firms have already committed to under the CRM Code, once the PSR has introduced new requirements focused on the reimbursement of APP scam victims.

This framework would maintain the independent oversight provided by the LSB, would help give confidence to customers and key stakeholders that firms are committed to good outcomes for customers, and would support firms in applying consistent protections to victims of APP scams across Faster Payments, CHAPS, and 'on us' transactions.

We would welcome further conversations with the PSR and Pay.UK to work out how this standards framework could best support the regulator's proposals on reimbursement. We would also welcome discussion on how the regulator can best support the LSB in delivering a set of standards that will ensure that as many firms as possible are committed to preventing APP scams from happening in the first place and to treating victims of APP scams fairly.

In the meantime, we welcome the clarity from the PSR of its expectation, which we share, that existing signatories to the CRM Code should continue adhering to the requirements of the Code as the regulator's proposals are finalised and implemented.

Yours sincerely,



Chief Executive

## **LSB's response to PSR's consultation on Authorised Push Payment (APP) scams: Requiring Reimbursement (CP22/4)**

The Lending Standards Board (LSB) is the primary self-regulatory body for the banking and lending industry, driving fair customer outcomes within financial services through independent oversight. Our [registered firms](#) comprise the major UK banks and lenders, credit card providers, debt collection agencies and debt purchase firms. Adherence to our Standards of Lending Practice and the other codes of practice which sit within our remit is a clear indication that a registered firm is committed to best practice in the treatment of its personal and business customers.

The LSB is responsible for the governance and oversight of the Contingent Reimbursement Model Code for Authorised Push Payment Scams (the CRM Code). Our role is to: monitor signatory firms' adherence to the Code; ensure its effectiveness; and maintain and refine it, as required.

We recognise the enormity of the task facing the PSR in taking forward measures to further secure an appropriate and effective consumer protection framework to detect and prevent APP scams. The PSR is a key stakeholder for the LSB, and we welcome the opportunity to input into the consultation process. Our response has been informed by the knowledge and understanding of APP scams we have gained via our role as the oversight body for the CRM Code.

### **Question 1. Do you have views on the impact of our proposals on consumers?**

The LSB understands the intention behind the PSR's proposals and recognises that the position of the regulator is that levels of reimbursement need to be higher and more consistent across industry. The CRM Code itself is drafted on the basis that where a customer falls victim to an APP scam, they should be reimbursed unless the firm can demonstrate that one or more of the exceptions allowed for under the Code applies. However, we believe it is important to note that, while the CRM Code is built on a contingent rather than mandatory reimbursement model, it has had a significant positive impact for consumers since becoming effective in May 2019.

#### **Reimbursement**

As part of the [2020 CRM Code review](#), we collected data from Code signatories to inform our understanding of the impact of the Code in its first year. This showed that, during the first half of 2019, customers who had reported APP scams were getting back 19% of funds lost. This figure rose to 41% during the first year of the LSB's oversight. The latest [data from UK Finance](#) shows that CRM Code signatories are returning 60% of the funds to customers who have fallen victim to APP scams. As CRM Code signatory firms provide protections to most customers using Faster Payments in the UK, this suggests that CRM Code signatories are significantly more likely to be reimbursing their customers where they do fall victim to a scam.

While this level of reimbursement may not be perceived as sufficient by the regulator, it represents a significant positive change by the firms signed up to the CRM Code. It also reflects the fact that the CRM Code is based on a contingent model introduced by a working group formed by the PSR and comprising industry and consumer experts. The Code does, therefore, allow for it to be the case that customers, excluding those who are considered vulnerable to

a scam, may not be reimbursed where the firm assesses that the exceptions to reimbursement set out in the Code apply.

The PSR's proposal focuses strongly on a mandatory reimbursement requirement with the only exceptions being where the customer has acted with gross negligence or there is evidence of first party fraud. As this is expected to be a higher bar for declining reimbursement than that allowed for under the CRM Code, it should lead to an increase in overall reimbursement levels given that fewer exceptions would be allowed under the PSR's proposals.

### **Prevention and the fair treatment of customers**

We have concerns about the impact of shifting to a consumer protection model that is based solely on a reimbursement requirement for Faster Payment Scheme (FPS) rules.

The Code placed a very clear focus on the prevention of APP scams which is a key protection in preventing consumer harm. The impact of the CRM Code, therefore, has not just been higher levels of reimbursement than seen pre-2019. Much of what has been achieved has been improvements in fraud prevention measures, as the Code has introduced new industry leading standards on the detection and prevention of APP scams, including requiring firms to; introduce risk based and impactful effective warnings; monitor and share information about APP scams; and, to focus on the fair treatment of customers who have fallen victim to scams. The Code requires firms to identify and support customers that may be vulnerable to APP scams, to take reasonable steps to raise awareness and educate customers about APP scams, and to offer appropriate aftercare.

The PSR has a statutory objective to ensure that payment systems are operated and developed in a way that considers and promotes the interests of all the businesses and consumers that use them.

We are concerned that the regulator has not fully recognised the significance of the change in firms' approaches to preventing APP scams and to supporting customers when they fall victim to scams brought about as a result of the implementation of the CRM Code. It is our view that the regulator has not clearly set out how it intends to ensure that the interests of consumers are protected and that a focus on customer outcomes will be maintained. While increased reimbursement levels may incentivise firms to prevent APP scams, there is a risk that a focus on prevention will now be primarily linked to cost minimisation for some firms. Unless the PSR's proposals clearly support firms to maintain standards on prevention and the treatment and support of customers, we are concerned that there will be a decreased focus on good customer outcomes and there is a risk of poorer treatment of customers.

We maintain that it is imperative that firms continue to provide education to consumers around APP scams as part of the wider prevention piece, irrespective of reimbursement being provided or not. The introduction of mandatory reimbursement, especially if it is based on new FPS rules as set out in the consultation, may lead to complacency in the education and support provided to consumers. Given the continued evolution of APP scams, a focus on consumer education is vital to support firms' wider prevention work.



The LSB firmly believes there would be a benefit to maintaining a revised version of the CRM Code which retains focus on good practice on the prevention and fair treatment of customers within the payments journey. This could ensure that firms continue to demonstrate their commitment to good customer outcomes and there continues to be oversight of these commitments by the LSB. We would welcome further discussions with the regulator on how such a code could operate alongside the PSR's proposals.

### **Scope of claims protected**

The CRM Code protects customers making Faster Payments, CHAPS payments, and intra-bank or 'on us' payments of any value where their firm is signed up to the Code. While we strongly welcome a proposal that requires a greater number of firms to reimburse their customers, we have concerns that the PSR's proposals do not extend to CHAPS and 'on us' payments. While we acknowledge discussions are ongoing with the Bank of England regarding CHAPS protections, and the consultation proposals expect firms to treat APP scams executed via 'on us' payments in the same way as Faster Payments, the proposals do not make it mandatory for firms to do so. Our concerns are that, without clarity, there will be a lack of consistency in approach across firms in relation to how APP scams are handled. In response to the PSR's previous consultation, we had indicated that we would have been supportive of an approach that would require more firms to commit to the CRM Code as it would have maintained consistent protections across payment types. This approach would also have retained a focus on prevention and customer treatment.

We would welcome discussions with the regulator on how the LSB can effectively maintain a Code, and accompanying oversight framework, that covers 'on us' and CHAPS payments. Such discussions would also cover how a Code could operate alongside an FPS reimbursement rule; and ensure there is consistency of protection across payment types.

### **A risk of poor outcomes for some customers**

We would welcome further information on the rationale for adopting an approach which allows firms to set a threshold of up to £100 and an 'excess' of up to £35. While these proposals may align with protections that exist for other payment methods, there does not appear to be any evidence to suggest that this approach will improve outcomes for customers. We are concerned that the impact of allowing for a threshold or excess to be set has not been fully considered on, for example, lower income customers. This is a point which is explored further below.

Some customers making low value payments who may be entitled to be reimbursed under the Code, will no longer have protections under the current proposals and all customers risk losing £35 on each payment. Our view is that any thresholds or excesses set by the regulator should be clearly evidence based and increase, rather than decrease, customer protections. Under the current proposal, firms will have the option whether or not to set a minimum £100 threshold. This approach may mean that inconsistencies remain in consumer protection as a customer will experience different outcomes depending on their payment services provider. It also means that cases that could currently be assessed under the Code would, depending on whether a firm adopts the minimum threshold, be excluded.

Similarly, we are concerned that inconsistencies in fraud prevention measures across firms may arise without appropriate focus on this key area of consumer protection. It is vital that prevention is not seen as an ‘optional extra’ by firms. There is a risk that those with a low occurrence of APP scams amongst their customer base may decide not to invest in prevention and detection measures. Firms may decide that it would be more cost effective to reimburse where scams do occur, rather than incur expense undertaking work to enhance their fraud controls when their APP scam risk is low. This approach could have a number of unintended consequences and lead to poor customer outcomes. While the PSR’s proposals mean a customer would be reimbursed in this scenario, they will have still experienced the harm of being scammed. It could also result in criminals targeting firms with weaker fraud prevention controls in place which further increases the potential for customer harm.

We remain concerned that there has not been sufficient consideration given to the potential for some customers, considered to be more at risk of falling victim to APP scams, facing barriers to accessing or using Faster Payments in the longer term. The consultation identifies the potential for older consumers to be impacted by its measures, but younger people are increasingly using social media as their primary medium for communication and sources of information, a medium which is increasingly being exploited by criminals. While it is right that customers take care when making payments, we are concerned that a primary focus on reimbursement rather than prevention may result in some firms, in a drive to reduce the costs associated with mandatory reimbursement, finding some cohorts of customers to be grossly negligent or introducing barriers that make it harder for some customers to access certain payment services.

Consumers are not a homogenous group, and there will be a variety of reasons why individuals fall victim to scams. It is important to consider whether their understanding and familiarity with engaging with particular communication channels has impacted on their assessment of any risks associated with the payment itself. This approach applies across both younger and older consumers. We would encourage the PSR to ensure that its proposals do not inadvertently create barriers to accessing or using the Faster Payments system simply because a particular demographic of consumers may be perceived to have a higher tolerance for risk or to be more likely to fall victim to particular types of scams. This type of information should be fed into prevention measures and used to inform whether monitoring, warnings and interventions in the customer journey require further tailoring or enhancing.

**Question 2. Do you have views on the impact of our proposals on PSPs?**

Firms that have signed up to the CRM Code have taken significant steps to change their approach to preventing APP scams, the assessment of cases and information and support provided to customers. They have also taken on significantly increased liability for the costs associated with reimbursing victims of scams, even where other industries have an important role to play in preventing this criminal activity.

We are pleased that the PSR’s proposals will extend to all Payment Service Providers (PSPs) to capture firms who could sign up to the CRM Code, but which have chosen to remain outside of the LSB’s oversight. It is our view that these firms have missed the opportunity to get ‘ahead of the curve’ in terms of developing effective prevention measures, particularly when operating in the capacity as a receiving firm. The consultation document highlights that

criminals target PSPs with the weakest controls, many receiving firms are not signatories to the Code and that there is significant scope for many PSPs to improve their performance in reducing APP scams.

The PSR envisages significantly higher levels of reimbursement across all Faster Payments, and CHAPS and 'on us' payments. This will inevitably increase the cost of reimbursing victims of APP scams for firms, so firms will have to set aside higher levels of funds to reimburse their customers. That said, we understand the PSR's position is that this approach incentivises both sending and receiving firms to do more to prevent customers from falling victim to APP scams.

However, while the reimbursement rule proposed will ensure all firms are required to reimburse customers, the outcome of our oversight activity has demonstrated that firms have found it challenging to put in place effective processes to ensure prevention measures, assessment procedures, and customer support are implemented to a consistent standard. As a result of our oversight and policy work, we have seen improvements in approaches across firms over the course of the past three years and it is vital that focus is not lost on these key areas of consumer protection.

We have concerns that without oversight of the conduct side of this process, the new proposals will pose challenges for firms which are not currently signed up to the CRM Code, in being able to implement appropriate customer outcomes-focused procedures alongside the reimbursement requirements. This may result in continuing inconsistencies in customer treatment. We strongly believe that there is a clear role for a recast, conduct-focused Code or set of Standards which could be designated within scheme rules, supported by independent oversight by the LSB, which would ensure there is greater consistency within the prevention space. We would welcome further engagement with the PSR on this point.

**Question 3. Do you have views on the scope we propose for our requirements on reimbursement?**

While we recognise that the current version of the Financial Services and Markets Bill (the Bill) will require the PSR to introduce reimbursement requirements for FPS payments if 'the payment order was executed subsequent to fraud or dishonesty' (Part 6, s.62(2)(a)), the Bill will also require the PSR to 'impose a relevant requirement, in whatever way and to whatever extent it considers appropriate, for reimbursement to be made in qualifying cases of payment orders' (Part 6 s.62(5)).

We, therefore, believe it is the responsibility of the regulator to set out clearly the parameters of the reimbursement requirements.

In particular, we believe that more clarity is required on the different types of scenarios that may fall under the APP scam reimbursement proposals. The CRM Code, for instance, already sets out that it does not apply to unauthorised payments or to private civil disputes (e.g., disputes between a customer and a supplier). (See DS2(2)).

We believe that more guidance is required from the PSR on the exact type of scenarios and payments that will fall into the mandatory reimbursement rules. This is particularly relevant for:

- Multi-generation scams: These are discussed later in the PSR’s proposal but there will need to be certainty over how these cases should be investigated and managed. The proposals discuss splitting the allocation of reimbursement between firms but do not extend to how customers should proceed with their claim. For example, which payment should be assessed as the scam? Should it be the initial movement of funds by a customer, or the payment made to an account controlled by the scammer? This may be particularly challenging for payments that move across payment types, or which include transfers of crypto assets.
- Open banking: scams involving Open Banking payments are currently within the scope of the Code. Given the different payment journey which applies here, clarity is required from the regulator in terms of its expectations of how cases involving Open Banking payments should be assessed. In addition, it would be helpful for the PSR to be clearer that Payment Initiation Service Providers (PISPs) are captured by proposals and how the reimbursement rules would apply to these firms. While PISPs have a range of business models and the approach taken should be proportionate, it is important that they are brought clearly within scope of the PSR’s proposals to ensure there are consistent protections for customers.
- Investment scams: It is not always clear where, at the point of execution, fraud or dishonesty has occurred in the case of investment scams. Firms may struggle to distinguish legitimate investments that later failed and have not provided a return for the customer, investments that were legitimate but later begin operating fraudulently, pyramid or Ponzi schemes, or scams where no investment fund ever existed.
- Civil disputes: It is not always clear where to draw a line between a dispute and a scam. It is not right that banks should be liable for disputes that can be resolved between a customer and a legitimate supplier of goods and services, but it can be challenging for firms to determine where the payment in question has been requested fraudulently.

We agree with the PSR that no ‘types’ of APP scams, such as purchase scams or investment scams, should be excluded from the protections. This is because protections should apply consistently for customers authorising push payments as the impact of a scam can be significant for a customer irrespective of the value lost or the type of scam. However, we are concerned that allowing for a minimum £100 threshold to be set is removing protections currently in place for consumers in relation to purchase scams, as these generally are of a low value.

**Question 4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

One of the existing challenges in implementing the CRM Code has been working towards a more consistent approach to firms’ understanding as to when it is appropriate to apply the exceptions to reimbursement allowed for under the Code. However, some variation in

reimbursement levels does reflect the fact that firms have different approaches to prevention and detection of scams, and have different risk appetites and risk-based warnings, etc.

The gross negligence exception currently exists under the CRM Code, however, as far as we are aware, it has not been used as a standard means for declining to reimburse a customer and we are not aware of the Financial Ombudsman Service (FOS) making rulings on cases where gross negligence may apply.

The consultation states that the CRM Code has not delivered the levels of reimbursement the PSR would like to have seen. Across current signatories applying the Code, 60% of funds are being returned to victims of scams through reimbursement or repatriation. It is our view that if the PSR wishes to achieve more consistency in customer outcomes and higher levels of reimbursement, it is essential that further guidance is provided on both the definition of gross negligence, beyond that referred to in the consultation paper, and on the level of reimbursement that it will expect to see if firms seek to rely on this exception.

Faster Payments are not like other payment methods, as funds are transferred almost instantly from a customer's account to another account, at which point the recipient can fully utilise those funds. While the LSB recognises the PSR's desire to improve protections for customers making Faster Payments, and gross negligence is already an exception within unauthorised payments, the protections in place for other payment types, such as credit cards, mean that customers are likely to utilise different payment methods in different ways. As such, what actions might be considered grossly negligent, and the degree of consumer caution exercised, may vary between payment types.

As part of mandatory reimbursement, we believe it is important for the PSR to provide clear guidance on the application of gross negligence if this is to be a 'consumer caution exception'. We would encourage the regulator to demonstrate, potentially by drawing on stakeholder input, FOS outcomes, and other relevant information, what it would expect to inform a consistent approach to assessing gross negligence.

Without additional guidance, firms may continue to apply approaches similar to those adopted under the CRM Code, which will not necessarily deliver on the regulator's stated objective. Given that the principle of gross negligence is being incorporated into regulatory requirements set by the PSR, we do not think it is appropriate for responsibility for setting guidance to be passed to FOS. This approach requires customers to have been through the complaints process both at firm and FOS level which is a much longer process than assessing the case at firm level.

While further guidance is needed, we would encourage the regulator to avoid setting anything that might be interpreted as a standard of care for customers. Our experience shows that firms – especially those without the experience of the CRM Code - may find it operationally easier to take a 'tick-box' approach to assessing cases, rather than seeking to understand the customer's circumstances and whether the customer may have been vulnerable to the scam they experienced. What is considered grossly negligent may vary considerably by case, due to the varying circumstances involved and evolving techniques used by fraudsters.

**Question 5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

Vulnerability is wide reaching and can depend on a customer's circumstances. It is important that the PSR's approach places a focus on preventing vulnerable customers falling victim to scams in the first place, rather than focussing solely on reimbursement.

We would agree with the approach that vulnerable customers should be exempt from the gross negligence exemption to ensure there remains a consistency of protection with existing requirements under the Code.

**Question 6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

While we agree that the FCA's guidance on the assessment of vulnerable customers is a good benchmark to work from to ensure there is a consistent understanding across firms, we have concerns that the current proposal may encourage an approach that could result in a decrease in protections for customers who are victims of APP scams.

Moving to the FCA's definition may provide a consistent definition of a vulnerable customer, however the FCA's accompanying guidance is generally financial services specific, with a few references to scams included. Where reference is made, this is typically in relation to the impact on the customer in terms of themes, such as misleading promotions or financial difficulty, rather than a wider consideration of the customer's circumstances at the point the scam occurred. In addition, the FCA's guidance cross references to the CRM Code and states that firms should take the relevant provisions of the Code into account when considering vulnerability in the context of APP scams. Through our oversight work, we have identified that firms face challenges in identifying vulnerable customers within the context of APP scams, therefore moving to the FCA definition without any supporting guidance and a more detailed assessment of the implications of doing so, could lead to further inconsistencies.

We agree that vulnerable customers may be more at risk of, or susceptible to, social engineering. However, the degree to which social engineering takes place within the context of APP scams and how effective it can be on customers who would not consider themselves to be vulnerable, should not be underestimated. We are concerned that a focus on vulnerable customers, rather than whether the customer was vulnerable to the scam itself, has not been fully explored. Should the PSR wish to apply the FCA definition of vulnerability, we believe that further consideration is required on whether, in the context of APP scams, it is relevant only to an existing vulnerability or whether the customer has to have declared a vulnerability, even if not relevant to the scam. The fact that a customer has previously been identified as being vulnerable may not necessarily increase the likelihood of, or result in them falling victim to an APP scam. For example, if a customer has a physical health condition, this may not necessarily make the customer vulnerable to the particular circumstances of the scam. However, the Code is clear that where there is evidence to suggest that it would not have been reasonable to expect the customer to have protected themselves from falling victim to the particular APP scam, firms should reimburse the customer.

The current definition of a vulnerable customer in the Code does not rely on the firm's action or inaction, or for the customer to have previously declared a vulnerability. It is based on the assessment of the customer's circumstances, the particular circumstances of the scam, and whether there was something within the specifics of the scam that meant the customer was unable to protect themselves i.e., they were more vulnerable to the scam. In moving to the FCA definition, we would encourage the PSR to consider whether this could have any unintended consequences, as it removes focus from the specifics of the scam. Under the FCA definition, it could be argued that the harm has been caused by the firm failing to identify the payment as a scam (i.e., it has not taken appropriate care to prevent the customer proceeding with the payment). This approach could result in all customers who fall victim to a scam being considered vulnerable. While being scammed can result in some customers becoming vulnerable, there is a need to ensure that this does not become a blanket term and there is a continued focus on the circumstances that surrounded the scam itself.

**Question 7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

Our view is that any thresholds or excess set by the regulator should be clearly evidence based and increase, rather than decrease, customer protections. It is stated that the excess applicable is the same that is allowed in respect of unauthorised payment transactions which may be appropriate in this context. Where a customer has been the victim of a scam and the decision has been made to reimburse the payment(s) involved, we are not convinced that there is a reason to reduce the amount that should be returned to the customer – it could arguably be perceived as a punishment for falling victim to a scam. Given the nature of APP scams, and that these can often involve social engineering, we are not convinced that a £35 excess would instil the necessary consumer caution but instead incurs additional loss for the customer.

The consultation document states that, for the lowest value claims, firms may not be required to fully investigate the scam and that there is a risk that civil disputes are inappropriately reimbursed when there are other mechanisms to resolve them. We believe there is another risk to this approach in that scams are incorrectly dismissed as being civil disputes. Over time, fraudsters' techniques may evolve so that smaller, lower value payments are targeted as these are less likely to be identified by firms or investigated. Therefore, there is a need to continue to consider the circumstances which sit around the payment and to avoid grouping smaller value payments as more likely to be civil disputes.



**Question 8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

We believe that no scam types or values should be excluded for customers as any amount of financial loss could cause significant harm. While the lowest value scams can be harder for firms to detect, £100 can be a significant sum of money for some customers to lose, especially in light of the current cost of living increases which will continue for some time to come. The £100 threshold proposal appears to be a de facto means of excluding lower value purchase scams. Allowing for a threshold to be applied may lead to further inconsistencies in outcomes as some firms may apply it and others may not, which could create confusion for customers as to which payments are/are not protected. It may, in some cases, also deter some customers from reporting a scam.

Furthermore, we are aware that under the Code, many firms will automatically reimburse lower value claims. This proposal could result in customers not being reimbursed where they would have been under the CRM Code and therefore decrease existing protections.

As this approach may also mean that cases which fall under the threshold are not fully investigated, there is the potential for criminals to take advantage of this by focusing on low value, high volume payments to avoid detection.

**Question 9. Do you have comments on our proposal not to have a maximum threshold?**

The CRM Code does not include any thresholds for claims. We agree that it is right there is not a maximum threshold set by the PSR under its new proposals.

**Question 10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

While we understand there may be a benefit for firms to set a time limit for claims for mandatory reimbursement, we would encourage the PSR to consider that, unlike with unauthorised payments, customers will know about the payment. Therefore, they are only likely to make a claim once they become aware they have been scammed rather than at the point the payment is made. The PSR may wish to consider whether the time limit should apply from when the customer might reasonably have realised, they have been a victim of an APP scam.

In some cases, such as investment scams or romance scams, payments and the relationship between the customer and the scammer can last for a sustained period of time. In investment scams, for example, a customer may not realise that they have fallen victim to a scam for a number of months. A customer may have transferred funds in good faith, expecting a return within 18 months, only to realise the investment was a scam after the 18-month period has surpassed. If a time limit is set, this should apply from when the customer might reasonably



have realised they have been a victim of an APP scam. In order to avoid any customer confusion, it is our view that there should be a consistent time frame adopted across PSPs.

**Question 11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We agree that the firm holding the customer relationship, the sending firm, should be responsible for reimbursement.

We believe the current approach under the CRM code of 15 business days to assess reimbursement is one that allows firms an appropriate opportunity to review cases, particularly those of a complex nature. However, we are also aware that firms have a number of cases which exceed this time period. This can be due to the complexity of the case, challenges with obtaining information from the receiving firm or being able to engage further with the customer where additional information may be required.

The 48-hour period proposed will be challenging and may result in customers feeling pressurised to provide the necessary information quickly or not being given time to fully process what has happened. Given the volume of cases that firms deal with, and that many of them are complex, a 48-hour turnaround period is likely to be too short a timeframe to allow for the necessary assessment of the customer's case and engagement with the receiving firm to take place.

We agree that firms should reimburse customers as soon as possible once a decision to reimburse has been reached, which could be within 24 or 48 hours, however, it is important that customers are not made to feel pressured or that firms are not provided with an appropriate amount of time to assess a case effectively. The Code sets clear requirements in terms of timelines for assessing cases. While there are challenges in being able to meet these timescales in some cases, it is our view that it would be sensible for these to remain in place. This would also align with the approach currently in place for non-signatory firms who are signed up to the Best Practice Standards (BPS).

**Question 12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The timelines for assessing cases currently set out in the CRM Code, and which we have suggested should apply in place of the proposed 48-hour turnaround, should allow for sufficient time for firms to investigate where it is believed that the first party fraud or gross negligence exceptions may apply.

APP scam cases can vary widely in terms of the circumstances and what the customer believed was happening, even where the type of scam is the same. We would encourage the PSR to avoid adopting an approach which could lead to a 'tick box' method being followed by firms as to whether or not a customer was grossly negligent. This could inadvertently be used as a means of setting a standard of care for customers when it comes to assessing cases.

In order to support firms' understanding of what comprises gross negligence, it would first be helpful for the PSR to set out its view on how and when this exception to reimbursement would apply. This could allow for further discussions with key stakeholders to support the development of any supporting industry guidance on how to evidence gross negligence.

**Question 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

It is our view that a change in the allocation of costs currently set out under the Code would be required to drive a reduction in the success and impact of APP scams. Our work has suggested that CRM Code receiving firms may be more likely to accept an allocation of reimbursement costs than non-signatory firms. However, even under the CRM Code, a very low proportion of reimbursement costs are met by receiving firms.

We therefore agree with the principle of splitting reimbursement costs more equally between sending and receiving firms. This ensures that there is a fair allocation of costs between the two firms and creates a greater incentive for firms to invest in, and further develop, prevention and detection measures.

We undertook some preliminary work in the Summer which considered where changes could be made to the allocation principles of the Code to ensure that receiving firms are allocated a higher portion of the costs of reimbursement. However, this was paused in light of the PSR's consultation which we understood would address the allocations piece. In reviewing the existing allocation principles, our view was that this will:

- Ensure that there is a clear recognition of the role firms play in providing accounts and payments services that can be used by criminals to facilitate APP scams.
- Ensure that there are appropriate incentives for firms to prevent the accounts and payments services they offer being used to facilitate APP scams.
- Encourage firms to further improve repatriation efforts to prevent the number of successful APP scams and reduce the impact on customers.

We are therefore supportive of measures which seek to ensure there is a more equal distribution of costs between the two firms.

**Question 14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

As the PSR is aware, the Code allows for a wider range of allocation outcomes based on whether a firm met the required standards for firms in relation to a case. While the Code allows for a formal dispute mechanism, we are not aware that it has ever been used and where disputes have arisen, firms have resolved these informally.

The proposal for a default allocation of costs may create some friction where one firm believes it has done more than the other to try and prevent the scam taking place. While there could be a benefit to exploring whether there is an appetite for a mechanism for firms to depart from the default allocation of costs, the introduction of dispute resolution arrangements into

the FPS scheme rules is one that will need to be confirmed ahead of reimbursement becoming mandatory for firms.

Establishing a dispute mechanism will have costs and resource implications and consideration should be given to the volume and types of cases that may be disputed. The current process under the CRM Code relies on the services of the Centre for Effective Dispute Resolution (CEDR), an independent body with expertise in dispute resolution.

We welcome the PSR's recognition that the CRM Code sets standards for firms and its expectation that any criteria for allocation and associated dispute resolution arrangements built and designated in scheme rules should build on these. The Code sets clear standards for firms in terms of the prevention and detection of APP scams. Should the PSR decide to implement an approach which allows for firms to depart from the default allocation principle, we believe there would be merit in further discussions as to the role a recast conduct focused Code could play alongside the role of a Faster Payments reimbursement rule.

This Code, supported by independent oversight by the LSB, could support good practice in prevention, detection, and treatment of customers and could be taken into account by CEDR or other body, as part of any dispute resolution process and could also be taken into consideration by FOS, in the same way it is now, when resolving complaints.

We are open to maintaining such an industry code, recognised by the regulator as representing good practice and focused on good customer outcomes. However, there would have to be sufficient interest from industry to sign up to a good practice code overseen by the LSB.

**Question 15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

**Question 16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

**Question 17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

Multi-generation scams can involve complex payment journeys with more than one customer, with different amounts being moved via a number of payments, and different payment methods. They may also involve the use of crypto assets.

The PSR's proposals discuss splitting the allocation of reimbursement between firms, but it does not extend to how customers should proceed with their claim, which we believe should be addressed. The challenge with multi-generation scams is that it can be unclear as to which: customer the protection applies to; payment the protections should apply to; customer is the victim, and who authorised the payment to the scammer.

In developing a solution as to how to assess and allocate the costs associated with reimbursement of multi-generation scams, we would encourage the PSR to set out a view as to whether scams are assessed and reimbursed on the basis of the individual payment or whether they are assessed based on the customer's financial loss.

Where other payment protections apply, they generally apply to the payment where the loss occurs. Consider the following two scenarios:

- Customer 'A' gives customer 'B' £100 in cash, with a view to customer 'B' transferring this money to customer 'C' to purchase an item they are selling online. The item later transpires to be fake and customer 'A' has now lost £100 but no direct recourse with their bank as they provided customer 'B' with cash. Would customer 'B' be eligible to claim in this instance for example?
- Customer 'A' transfers £5,000 to customer 'B' with a view to customer 'B' making a £5,000 payment to customer 'C' to purchase an item they are selling online. The item later transpires to be fake and customer 'A' has now lost £5,000.

If customer 'B' has made the payment by credit card, customer 'B' may have a Section 75 protection for the purchase. If the payment is made via FPS, would it be the responsibility of customer 'B' to claim for the payment made to an account controlled by a scammer or should customer 'A' report and make a claim for reimbursement?

For consistency, the PSR may need to consider clarifying whether the payment or the customer are protected. If it is the payment, the issue of assessing multi-generation payments becomes simpler and a 50:50 allocation would still see the receiving bank take 50% liability for the scam. However, the original victim of the scam will have to rely on customer 'B' to make the claim, even though they have not lost funds.

**Question 18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

The PSR's five-year strategy sets out that it wishes to give Pay.UK a stronger role to lead the development of protections for payment system users. The vision is for Pay.UK, as payment system operator (PSO), to run Faster Payments so that consumers are protected, and fraud is prevented from entering the system.

We understand the PSR's view that it makes sense for one organisation to have overall responsibility to ensure there are appropriate protections within Faster Payments. However, it appears that much of the success of the proposals outlined in the consultation paper depends on whether Pay.UK is able to give effect to the PSR's proposals in the short term. It is our view that this is a significant undertaking, and we would question whether there should be a clearly phased approach to this work to allow Pay.UK time to develop a solution that is workable and includes any required governance and oversight frameworks, and associated resources. It appears from the consultation that there remain a number of areas which need to be addressed before Pay.UK can give effect to the PSR's vision and take on an expanded role.

While CRM Code signatories will be familiar with the LSB's expectations in terms of the application of the Code and its requirements, there is a much wider pool of firms which will not be familiar. These firms may not have the required systems, policies, procedures and processes in place to address the PSR's proposals and may require additional oversight in order to reach the required standard. This will be key if the PSR decides to allow for firms to depart from the default reimbursement allocation. Some firms will be more advanced in their

prevention and detection measures which means there will continue to be inconsistencies in areas which are key to preventing fraud from entering the system.

We are committed to working with the PSR and Pay.UK and would welcome further discussions on the role that the LSB can play in the short to medium term which would support the PSR's vision, and Pay.UK, as it undertakes its work to address the PSR's proposals.

**Question 19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

The minimum initial set of rules proposed by the PSR are focused primarily on reimbursement. Much of the improvements seen since 2019, including the development of good practice in relation to scam prevention and the treatment of customers, are not covered by the proposals. Furthermore, the LSB's thematic reviews and ongoing monitoring of firms' conduct have allowed us to identify key issues and drive improved customer outcomes.

We are concerned that the initial set of scheme rules do not include consideration of how the good practice implemented through the CRM Code will be expanded to a wider range of firms, nor does it cover how firms' conduct around the reimbursement process will continue to be overseen. We believe that in order to support the implementation of the initial set of rules, there would be a benefit to retaining the conduct requirements of the Code, accompanied by the LSB's oversight, during the transition phase. This would apply to all FP participants captured by the rule and would support the PSR's work to drive improvements in the prevention of APP scams.

**Question 20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

**No response.**

**Question 21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

The proposal for costs to be shared 50:50 between firms is one that is likely to create some friction where firms are unable to agree on liability for their involvement in a loss. The introduction of dispute resolution arrangements into the FPS scheme rules is one that will need to be defined ahead of reimbursement becoming mandatory for firms.

The CRM Code sets out an existing approach for dispute resolution, using existing industry expertise to settle challenging disputes. The Centre for Effective Dispute Resolution (CEDR) are an independent body with expertise in dispute resolution, providing a ready-made solution for firms to use should they require mitigation in respect of an ongoing dispute. That being said, from our experience of overseeing the Code to date, we have yet to be made aware of any disputes being referred to CEDR.

While we do not doubt the mediation skills of Pay.UK, the introduction of this work may require additional resource and training, which in turn may become an operational burden which would require further consideration. The number of cases which may be taken to dispute resolution is unknown and there would be a benefit in engaging with industry to understand the degree to which there would be appetite for this and anticipated volume.

We do not see why this approach would need to change. It may be, for instance, that the Pay.UK rules recognise that firms may use an independent process to dispute the allocations where firms are signatories to a conduct focused Code that is based on the existing CRM Code requirements.

**Question 22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

We have concerns that the role proposed for Pay.UK is a significant change in the remit and role of Pay.UK and that the nature of the oversight offered by Pay.UK and/or the PSR will be notably different to that offered under the CRM Code.

Since 2019, the LSB has conducted four compliance reviews involving all CRM Code signatory firms. Our independent oversight ensures that firms are not only applying the requirements of the Code correctly but also that its requirements are embedded within policies and processes, and this is underpinned by an appropriate governance framework. Our work has also focused on embedding a customer outcome focused approach to the Code which is focused on prevention as much as it is on reimbursement. We believe there is still a role for a conduct focused Code, overseen by the LSB, and would welcome further discussions on how this could sit alongside Pay.UK's monitoring activity.

**Question 23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We are concerned that the current proposals on monitoring compliance do not reflect the challenges faced by firms in assessing and reimbursing victims of APP scams. Pay.UK providing oversight of the reimbursement element of the process, which is currently managed by signatory firms through the Best Practice Standards, may be beneficial and ensure all PSPs can work together through a single framework.

However, monitoring of data will not ensure firms are treating customers appropriately or allow for independent monitoring or oversight of firms' prevention work. In addition, as the funds reimbursed to customers do not move through Faster Payments rails, it is likely that Pay.UK will have to rely on firms reporting data. The PSR as the regulator should ensure any regulatory requirements, including reporting requirements, are subject to some form of independent or regulatory oversight.

**Question 24. Do you have views on the best option for short-term enforcement arrangements?**

The LSB wishes to ensure that, for those customers already protected by the CRM Code, that there is no decrease in protections. We also wish to ensure that all firms reimbursing customers recognise the importance of having a customer focused approach to assessing APP scam cases, and to communicating with and supporting victims of APP scams.

Identifying where firms are properly assessing cases and supporting their customers can be challenging and has, for CRM Code firms, required significant oversight from the LSB. In the short term, we hope to work with the PSR and other key stakeholders to ensure there remains appropriate standards on the conduct surrounding APP scams. We also wish to ensure that

there is appropriate independent oversight in place to ensure that firms applying those standards are doing what is expected of them.

It is our view that the CRM Code, in its current form, should remain in place (and all firms remain signed up to it) in the short term to ensure that there is no decrease in customer protections whilst the PSR continues its work to develop its proposals. We therefore welcome the PSR's statement in the consultation document which states that in the period before implementation of arrangements for mandatory reimbursement, the regulator expects signatories to continue to adhere to the requirements in place under the CRM Code.

**Question 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

It is our view that in order to ensure there is a consistent approach to the prevention of APP scams that the PSR should direct indirect PSPs or IAPs.

**Question 26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

It is our view that in order to ensure there is a consistent approach to the prevention of APP scams that the PSR should direct indirect PSPs or IAPs. The alternatives set out in the proposals do not allow for the PSR or in turn, Pay.UK, to have direct oversight over this group of participants. It is right that one rule applies across the board and having requirements in different places and sitting with different organisations could create challenges and lead to inconsistencies.

**Question 27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

**No response.**

**Question 28. Do you have any other comments on the proposals in this consultation?**

We would welcome further discussions with the PSR on what we believe could be the future of the LSB's role in respect of APP scams and how we can best support the PSR, and Pay.UK, in the short and longer term.

# Lloyds Banking Group





**LLOYDS BANKING GROUP PLC**  
**CP22/4: Authorised Push Payment (APP)**  
**Scams- Requiring Reimbursement**  
**Consultation Paper**

**Submission Date: 8 December 2022**

*The information contained in this response is provided to the Payment Systems Regulator (PSR) in relation to the recent APP Scams Consultation. This response does not contain confidential information. This response can be published or disclosed to any third party, as we have redacted any confidential information. We have provided a separate confidential version for the PSR's purposes.*

## Executive Summary

The UK's fraud epidemic is an increasingly significant national security issue, and we commend the PSR for their work to date on this complex and distressing matter for UK consumers<sup>1</sup>. Lloyds Banking Group recognises the hugely damaging impact fraud has on our customers and we have invested heavily in protection and reimbursement, but it is important that there is a holistic and consistent approach to customer protection across the industry.

The impact of Authorised Push Payment (APP) scams on consumers is significant. In 2021<sup>2</sup>, UK Finance data shows that losses due to APP scams were £583 million. In total there were 196k cases, 189k of which were on personal accounts. We have invested over £100 million over the last three years in our fraud detection systems to protect our customers, working closely with the PSR and the industry to implement the Contingent Reimbursement Model (CRM) Code. The CRM Code has helped reimburse tens of thousands of victims, and we currently refund the majority of APP scam cases reported to us.

**We are concerned that the PSR's proposals do not place sufficient emphasis on prevention and will continue to expose consumers to significant risk. Focusing on reimbursement, rather than prevention, does nothing to reduce scams**

Mandating reimbursement without Payment Service Providers (PSPs) being fully equipped with the preventative tools needed to identify and stop fraud, risks exacerbating the problem: by failing to protect consumers from initial harm; not preventing funds flowing into the hands of criminals; and not addressing the UK's attractiveness to fraudsters.

We believe the focus should be on enabling and implementing stronger preventative measures to stop APP scams taking place in the first place. While reimbursing losses as a result of fraudulent activity addresses the financial harm suffered, it does not address the emotional distress caused to the consumer and does little to deter such scams taking place.

**We strongly advocate that the PSR pauses the mandating of reimbursement until urgent fraud prevention measures are enabled through legislative and regulatory changes to tackle the UK's fraud epidemic at its root cause**

We encourage the PSR and FCA, along with HM Government (HMG), to urgently convene to first collectively deliver prevention measures. We see the following as immediate priorities:

- i. enable banks to intervene in or slow payments without recourse if fraud is suspected;
- ii. enable data sharing across sectors to identify scammers, detect mules and protect victims;
- iii. bring all fraud-enabling sectors, including social media giants and telecommunications sector, into the solution; and
- iv. increased law enforcement capacity and capabilities to capture and remove criminals.

---

<sup>1</sup>Consumers include customers, micro-enterprises, and charities. These terms are defined regulation 2(1) of the PSRs 2017

<sup>2</sup> [Annual Fraud Report 2022\\_FINAL\\_.pdf \(ukfinance.org.uk\)](#)

These preventative measures should be supported by the development of a coherent and evenly distributed approach to reimbursement for fraud victims across the fraud ecosystem, with a government-led communications campaign to support consumers in understanding their rights to reimbursement and their role in protecting themselves from fraud. Crucially, we believe these steps need to take place as a holistic approach, focusing solely on reimbursement risks being ineffective in tackling the issue.

We understand the PSR is somewhat constrained by the timeline requirements within the **Financial Services and Markets Bill (FSMB)**. **We therefore urge the PSR to support us in advocating for HMG to extend this deadline within the Bill**, in order to allow time for the other legislative and regulatory changes to come into force.

This approach is endorsed by the recommendations within the House of Lords report 'Fighting Fraud: Breaking the Chain'<sup>3</sup>. The Committee that compiled the report arrived at these recommendations after having received over 90 individual submissions to its call for evidence and having also heard oral evidence from over 45 witnesses ranging from academics to victims and law enforcement.

**Preventing fraud is a shared responsibility going beyond just the role of banks, in particular social media, platform providers, and the telecommunications sector though which over 70% of scams are enabled<sup>4</sup>**

We appreciate the efforts being made by the telecommunications sector to help prevent scam calls and texts, however, much more needs to be done, and there are currently no incentives or mandates for these firms to act.

Fraud education, identification and prevention can never happen properly until the wider fraud ecosystem is taking full responsibility, jointly and severally, for this. The ultimate aim is to stop consumers from falling victim to fraud and take away the opportunity from criminals to attempt scams. However, this will always fail if the onus sits too much within one part of the ecosystem over another because no one actor has control over all the other parts.

**The reimbursement model, when implemented, needs to be robust, well publicised and understood by consumers, and addresses all the intricacies of the APP scam landscape**

We have reviewed the PSR's proposals carefully and we set out a number of observations and suggestions. Pausing mandatory reimbursement will also give the PSR additional time to work with the industry and consumer groups to refine the proposals. In particular this would allow the PSR to fully review complex areas such as multi-generational scams and PISP-initiated payments.

**We are pleased to see the proposal for reimbursement requirements to be extended to all PSPs; the roll out of the prevention measures must be universal to give consistency to customers and avoid weaknesses in the system**

---

<sup>3</sup> [Fighting Fraud: Breaking the Chain \(parliament.uk\)](https://www.parliament.uk/business/committees/committees-a-z/commons-select/fraud-and-counterfeit-committee/pages/fighting-fraud-breaking-the-chain/)

<sup>4</sup> [Over two thirds of all APP scams start online - new UK Finance analysis | Insights | UK Finance](#)

We welcome consistency for consumers and believe that consistency in both the rollout of prevention tools, and the reimbursement model will be key to preventing consumer harm and reducing the risk of scams.

Currently, consumers may not always be aware whether or not their chosen PSP has signed up to the Contingent Reimbursement Model (CRM) Code or if they have an alternative similar commitment to refunding APP scam cases. Having different commitments across PSPs has created an inconsistent approach across the industry and causes confusion for customers, who may be unaware of their level of protection. We fully support the proposal to extend reimbursement requirements to all PSPs, at the same time, to help achieve greater consistency.

The rollout of Confirmation of Payee (CoP), which helps many customers validate that their payments are being sent to their intended recipient, saw a migration of fraud to those firms who were not part of the original implementation. We welcome the recent expansion of CoP to a further 400 firms to implement CoP, and PSPs should all be required to implement new prevention tools consistently.

### **Consumers also have a role to play in preventing fraud and the PSR's activity should recognise this**

We agree with the PSR that the need for consumer responsibility remains, alongside the need to take caution when sending payments. Consumers taking a degree of responsibility for their own actions is not a new concept. It exists as a core principle under the Financial Services and Markets Act and is recognised in the FCA's new Consumer Duty.

In order to protect themselves against fraud, consumers need to understand the steps that they can, and should, take. For consistency of outcome we ask the PSR, in collaboration with the industry and consumer groups, to lead on developing clear criteria for a minimum level of caution a consumer should take when making a payment in order to be eligible for reimbursement. As well as consistency of outcome, this would be the foundation of the Government-led information campaign, and ensure consistent messages are conveyed across all firms.

### **A sustainable commercial model is needed for the long-term viability of payments in the UK, as well as to support investment and innovation to benefit consumers and provide choice for businesses**

While Faster Payments is undoubtedly an innovative platform, it was never built to support customer to business transactions and direct commerce, which is increasingly used for today. Further, there is a substantial imbalance between the protections and security offered when compared to the card schemes (e.g. Section 75, disputes, chargebacks).

These protections should be sufficiently developed before the further widening of Faster Payments use cases, such as through Open Banking, to avoid consumer confusion, market fragmentation, and to promote trust in the payment channel which will in turn provide greater choice for businesses.

It is crucial that consumer protections are underpinned by a sustainable economic model – in part funded by merchants, as the credit and debit card networks are today. In the case of consumer to business payments, a commercial fee arrangement in the style of interchange is likely needed alongside associated checks and balances on businesses. It is not sustainable for PSPs to absorb the costs of all consumer protections, and this may create further market distortions. Therefore, a robust framework and infrastructure for consumer protection must be developed at pace for delivery into the New Payments Architecture (NPA) and alongside work by Joint Regulatory Oversight Committee (JROC) on Account-to-Account Retail Transactions (A2ART). We are keen to support the development of such an approach working with regulators, industry and other bodies and look forward to continuing to work together on this.

We would welcome the opportunity to work closely with the PSR and other stakeholders as proposals are developed, to discuss any elements of our response in further detail, and to work with regulators and other industries to prevent fraud in a co-ordinated manner.

<b>Detailed Response to Consultation Paper</b>
--

**Section 3: Outline and Impacts****1. Do you have views on the impact of our proposals on consumers?**

- 1.1 We are pleased to see the proposal for reimbursement requirements to be extended to all PSPs; this will help in ensuring consistency for consumers and a much greater proportion of consumers being reimbursed than today, regardless of who they bank with.
- 1.2 Consumers may not always be aware of whether their chosen PSP has signed up to the currently-in-place Contingent Reimbursement Model Code or if they have a similar commitment to refunding APP scam cases. Having different commitments across PSPs creates an inconsistent approach in the industry and causes confusion for consumers, particularly for those that hold accounts across several PSPs. We welcome the positive change to extend reimbursement to all PSPs.
- 1.3 We recognise the PSR's view that bringing both sending and receiving PSPs under the reimbursement model will incentivise the deployment of more fraud prevention. The Financial Services sector has been investing heavily to protect customers and some PSPs worked closely together to develop and implement the CRM Code which has helped reimburse tens of thousands of victims. We do agree that more can and should be done to prevent fraud as it is preventative measures in the first place that will have the greatest impact on consumers.
- 1.4 However, PSPs are limited in the actions they can take due to current regulation and legislation. As a result, we are concerned that the current proposals alone will not yield the desired outcome of preventing APP fraud and risk leaving the UK attractive to scammers. Regardless of the monetary amount lost and whether customers are able to recoup this, the emotional and psychological impacts of becoming a fraud victim may be hard to recover from, and the Money and Mental Health Policy Institute found that people with mental health problems are three times more likely than the rest of the population to have fallen victim to an online scam, further highlighting the importance of focusing on fraud prevention in the first place<sup>5</sup>.
- 1.5 This risk was also signalled in the *House of Lords* report, 'Fighting Fraud: Breaking the Chain', which strongly emphasised the need for the Government to '*revise its proposals to legislate to allow the PSR to mandate blanket reimbursement of APP fraud conducted via Faster Payments*' and further explore '*the long and short-term risks of this approach*'.
- 1.6 **We, therefore, urge the PSR and the Government to pause these proposals requiring mandatory reimbursement, so as to allow the Home Office to bring forward the National Fraud Strategy and, in parallel, deliver prevention measures through legislative and regulatory changes in several key areas.**

---

<sup>5</sup> <https://www.moneyandmentalhealth.org/online-scams-mental-health/>

- 1.7 We recognise that the Financial Services and Markets Bill applies a tight timescale for the PSR to bring forward measures, but we do not agree that it is appropriate to progress with just this one element before the broader strategy is clearly defined and underway.
- 1.8 Implementing the prevention measures which we discuss in detail below would mean fewer customers experiencing fraud in the first place, prevent money passing into the hands of criminal organisations, and better equip the UK to determine a sustainable and long-term approach to reimbursement. We see the following changes as immediate priority:
- **Enable banks to intervene in or slow payments without recourse if fraud is suspected.** As the PSR will be aware, the Payment Services Regulations 2017 (PSRs 2017) do not give sending PSPs comfort to hold a payment for more than one business day, even when it believes the customer may be being scammed. Changes are needed to Regulation 86 in the PSRs 2017 to specify that PSPs can pause a payment for longer where there is a high risk of fraud. The FCA, which has set an expectation of payments being received within two hours, should also update its guidance to allow sufficient time for robust fraud prevention.
    - It is of key importance that the sending bank is enabled to hold the payment for a sufficient period of time to address any high-risk flags that indicate the customer has fallen victim to an APP scam.
    - Addressing these flags can be difficult within a 24-hour timeframe, as customers may not always respond to calls or e-mails from their bank in 24 hours. Therefore, PSPs must be given a non-time bound ability to delay payments, which should not usually extend over more than a couple of days, to allow sufficient time for robust fraud prevention.
    - Receiving firms should be enabled to pause crediting their customers' accounts where there is suspicion the recipient might be acting as a fraudster, or as a money mule.
    - Changes to the PSRs 2017 could allow sending firms greater flexibility to adopt a risk-based approach to pause and investigate higher risk cases. Pausing would allow further investigation and/or customer contact (which is not always possibly within the 24-hour timeframe) and more closely align with the ability to intervene on suspected fraud payments with money laundering.
    - The House of Lords 'Fighting Fraud: Breaking the Chain' report recommends that certain payments should be paused but not for longer than several hours. While we welcome the intention and principle behind this recommendation, we strongly disagree that several hours will suffice to prevent fraudulent transactions for the reasons explained above. We support a non-time bound ability for PSPs to delay payments, which should not usually extend over more than a couple of days.

- **Enable data sharing across sectors to identify scammers, detect mules and protect victims.** Data sharing between online services, platforms, and banks, without commercialisation, is required to identify and prevent harms. Therefore, relevant provisions in the Economic Crime and Corporate Transparency Bill (ECCTB) and Data Protection and Digital Information Bill need to be delivered. We welcome the adoption of the amendments in the ECCTB to introduce civil liability safeguards.
- **Bring all fraud-enabling sectors into the solution, including sharing liability within the reimbursement model.** Across the Financial Services industry, 70% of scams are enabled through social media giants and telecommunications firms. APP frauds are often successful in part due to weaknesses in controls across the fraud ecosystem including in other sectors i.e. purchase scams happen via online marketplaces; investment frauds start in social media channels or with an internet search engine; mule recruitment takes place via social media and impersonation scams usually begin with a spoof text or telephone call. We strongly believe non-financial services actors must introduce robust preventative and detective tools, including cross sector data sharing. Where these measures fail and the scam takes place, these firms should share the financial liability.
- **Government to convene all stakeholders and clarify central accountability.** We recommend the government appoints a Minister of Economic Crime Prevention to provide coordinated leadership, supported by a specific Scams Lead to energise and champion change. Further, only 1% of law enforcement is focused on tackling fraud which makes up circa 41% of all crime affecting individuals<sup>6</sup>. The Government should give fraud the priority it deserves, with resourcing proportionate to the problem.
- **Agree a sustainable and proportionate, long term reimbursement strategy for consumers.** All actors in the ecosystem should be consulted collectively, with the aim of designing the most sustainable, streamlined and appropriately distributed approach to reimbursement. We recognise that the risk of fraud is frightening for consumers, especially the most vulnerable. So consumers can understand the steps they can take to protect themselves from fraud, a common understanding is needed on the minimum level of caution consumers must take when making payments to protect themselves and be reimbursed following a scam.
- **A government-led public information campaign** on the scale of those seen around road safety, drink driving or 5-a-day, recognising the role we and other firms are playing in educating consumers and raising awareness.

1.9 It is important that when the reimbursement rules are implemented, they are easy for consumers to understand and lead to consistent outcomes, irrespective of who they choose to bank with.

---

<sup>6</sup> [Fighting Fraud: Breaking the Chain \(parliament.uk\)](https://www.parliament.uk)



- 1.10 The ability for PSPs to choose their own limits for elements such as the minimum threshold or claim time limit, will likely lead to a confusing consumer landscape. Therefore, we recommend that each requirement within the reimbursement model should be aligned across the industry with no option for PSPs to depart from this. The agreed, industry-broad reimbursement requirements could then be clearly communicated to consumers through a Government-backed education programme.
- 1.11 We are particularly concerned with the impact of undefined gross negligence as one of the two proposed exceptions to mandatory reimbursement. We believe this will create inconsistent customer treatment as PSPs will vary widely in the way they interpret the definition of gross negligence, creating similar issues as seen in the CRM Code currently, and could lead to outcome disputes between the receiving and sending PSPs. We discuss in detail our proposed solution in Question 4.
- 1.12 It is also important to recognise that without the more robust preventative measures enabled by regulatory and legislative changes, outlined above, PSPs will likely become more risk averse, resulting in unintended consequences for consumers. PSPs may:
- **Close accounts or reduce availability of banking products for customers /groups of customers who have a higher propensity to become mules.** PSPs may withdraw from certain segments, for example, no longer offering student accounts.
  - **Close accounts or restrict functionality for repeat victims.** The consultation notes that PSPs might consider restricting services to certain consumers. While we agree that PSPs should not refuse or deny banking or payment services to consumers more at risk of becoming victims of APP scams, if a customer continuously falls victim to a scam, it may be necessary to restrict their banking facilities to prevent them from further harm.
- 1.13 We note PSPs' obligations in the Equality Act 2010 to treat current and prospective customers equally, however a PSP's action to limit or remove access to some services could be evidenced as "objectively justified".

## 2. Do you have views on the impact of our proposals on PSPs?

- 2.1 As mentioned above, we welcome the benefits for consumers of widening the scope of the reimbursement requirements to all PSPs, while also recognising the challenges this will bring for some PSPs.
- 2.2 We recognise the PSR's view that bringing both sending and receiving PSPs under the reimbursement model will incentivise the deployment of more fraud prevention across the industry. However, PSPs are limited in the actions they can take without the urgent legislative and regulatory changes, as laid out in our response to Question 1, to enable stronger preventative measures.
- 2.3 We welcome the inclusion of indirect participants in the mandatory reimbursement model. It is our strong preference for the PSR to give a specific direction to mandate

all direct and indirect PSPs to comply with the reimbursement proposals and thus ensure consistency across the industry.

- 2.4 We note the significant negative consequences for Indirect Access Providers (IAPs), should the PSR decide not to implement reimbursement requirements via a direction on all PSPs, and instead chooses either of the remaining two implementation options: i) applying the Faster Payments Scheme (FPS) rules on reimbursement to all transactions; and ii) a direction to IAPs to ensure transactions by the indirect PSPs comply with the reimbursement rules in FPS.
- 2.5 Either of these implementation options will place a significant burden on the IAP to monitor and enforce compliance on its indirect customers. This would therefore be an additional consideration for assessing eligibility for providing services to indirect PSPs leading to a more stringent risk appetite and thereby reduce availability of indirect access services with the knock-on effect on competition in the market and ultimately consumer choice.
- 2.6 Furthermore, if an indirect PSP was not able to meet its obligations in the FPS, we do have concerns about the additional financial burden for IAPs. For context, as an IAP, we have circa [REDACTED] agency and non-agency indirect PSP customers. If we were to be held liable for the transactions enabled by our indirect PSP customers, we would need to reconsider the terms and conditions for sponsoring a firm into the FPS to mitigate this new risk.
- 2.7 It is also worth noting that mandatory reimbursement that is not coupled with the prevention measures outlined in response to Question 1, will likely disincentivise merchants from participating in the future A2ART ecosystem. That is because, without better prevention measures which should keep the operational costs lower, PSPs may need to pass on the risks and costs of fraud into the commercial model underpinning A2ART.
- 2.8 Overall, we believe the PSR needs to be mindful of the impact their proposals will have on competition and, ultimately, innovation in Financial Services.
- 2.9 Finally, we would like to emphasise the operational burden and additional costs that the CRM Code signatories would face, should the Code continue to operate in parallel to the reimbursement rules. We strongly feel the Code should be retired once the rules have come into force to avoid duplication, and the type of operational burdens, we have seen with the CoP dual running period of Phases 1 and 2.

## **PART A: The Reimbursement Requirements Proposed**

### **Section 4: Mandatory reimbursement for consumers**

#### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

- 3.1 We welcome the clarification that the PSR consultation is consistent with the definition of payers as defined in the CRM Code:

- *"A consumer is an individual who, in contracts for payment services to which the PSRs 2017 apply, is acting for purposes other than a trade, business or profession.*
- *A micro-enterprise is an enterprise that employs fewer than ten persons and whose annual turnover and/or annual balance sheet total does not exceed €2 million.*
- *A charity is body with annual income of less than £1 million and is a charity as defined in relevant legislation in the UK."*

- 3.2 As previously referenced, we welcome the inclusion of all PSPs including those directly connected PSP participants sending payments over Faster Payments, as well as PSPs indirectly connected via an IAP.
- 3.3 We understand that other payment mechanisms are not in scope for these reimbursement measures. While we are not advocating at this stage that all come in scope, we are concerned scams will migrate to other channels, potentially resulting in inconsistent outcomes for consumers across different payment methods or firms.
- 3.4 We do, however, urge the PSR to include on-us payments within its reimbursement requirements. While we, and other firms, will act on the PSR's recommendation to reimburse this type of payments, we are concerned gaps will remain in the industry, which in turn will create inconsistent customer treatment.
- 3.5 The consultation states that reimbursement rules would apply only to APP scams where the most recent payment was authorised after the regulatory requirements came into force, with no ability to apply the rules retrospectively. We welcome the PSR's clarification, during the UK Finance roundtable session on 21 November that only those payments within the claim that were authorised after the regulatory requirements came into force will be eligible for mandatory reimbursement. In order to provide clarity and set expectations for consumers this should be clearly outlined in the rules, and we ask that the PSR work with HMG to ensure this is included in communications relating to the FSMB.
- 3.6 We agree with the PSR's proposal that no categories of APP scam are excluded from mandatory reimbursement.
- 3.7 Recognising that this is an area which has had significant debate across the industry, we have focused on the need to design a solution that gives clarity and simplicity to both consumers and firms. In coming to our position on not excluding certain categories we gave special consideration to the inclusion of purchase scams and in particular how they can be identified:
- 3.7.1 We are pleased that the PSR has confirmed mandatory reimbursement would not apply to private civil disputes. However in practice, with the information available to us, it can be difficult to distinguish between the two.

- 3.7.2 It can also be difficult to distinguish between purchase scams and other scam types, for example the fraudulent purchase of gold for investment purposes could be classed as an investment scam or a purchase scam.
- 3.8 Balancing these considerations, we agree that purchase scams should be in scope, however, **this must be supported by an appropriate minimum claim threshold, and an agreed definition of minimum customer caution**, on which we have provided more detail in our response to Question 4.
- 3.9 We would like to highlight that around over 80% of purchase scams are enabled through social media marketplaces and social media-displayed adverts. This reinforces our view that online platforms and online services must take preventative action and, where that failed, share the liability.
- 3.10 We cannot support multi-generational scams being within the scope of the reimbursement model until they, and the role of all PSPs within the chain, are clearly defined. More information on this is contained in our response to Question 15.
- 3.11 We support the need to bring PISP-initiated payments into scope, particularly as evidence-based analysis of Open Banking transactions shows a three-times higher risk of fraud than other digital channel Faster Payments.
- 3.12 As the PSR recognised in the roundtable hosted by UK Finance, the consultation does not give detailed consideration to the inclusion of PISP-initiated payments. While the consultation is clear that PISP-initiated payments are in-scope, it is unclear whether the PSR intends PISPs to be liable for the reimbursement. We would therefore welcome more clarity from the PSR on this point.
- 3.13 The intention of the reimbursement model is to incentivise PSPs to put in place tools and controls to reduce levels of fraud. As the PSR will be aware of, PSPs are currently unable to put in place controls that are as robust for Open Banking as are in place for Direct Channels, in large part because some of the key risk indicators that enable PSPs to operate these controls are only visible to the PISP as they are in direct contact with the customer.
- 3.14 This is a particular problem for Open Banking payments involving beneficiary (payee) details that aren't prepopulated by the PISP, being paid to third party accounts that are not tightly coupled into the PISP's payment journey as these are typically likely to be more prone to fraud than prepopulated payees where the payee is the merchant that is contracted to the PISP to accept Open Banking payments.
- 3.15 For these reasons, we strongly believe that PISPs should be directly held liable in the reimbursement model. We recognise this would require a separate consultation.
- 3.16 However, should PSPs be mandated to support PISPs in identifying and stopping fraudulent PISP-initiated transactions, it is of the utmost importance that, at the very minimum, the following measures are put in place:
- 3.16.1 **Evaluate the mandatory adoption of Transaction Risk Indicators (TRIs) by PISPs.** The current standard accommodates a range of TRIs, covering

extended payment purpose codes, beneficiary account type and payment characteristics such as whether a contract is in place between the PISP and payee (e.g. where there is immutable pre-population of beneficiary payment details). Increased and mandatory usage of these factors would help reduce fraud and drive increased payment completion rates.

3.16.2 **Evaluate mandatory Confirmation of Payee** for any payments that are not being paid to prepopulated payees contracted to the PISP as a merchant looking to receive a payment for goods or services. This would require new development of the Standard and could in time support greater confidence of a bona-fide recipient. Either (a) the PISP would be able to flag a payment as “CoP checked” and the nature of the response as “Full / Partial / No match”, and the PSP would be able to manage accordingly. Or (b) the PSP could perform the CoP service as a chargeable service to PISPs for improved fraud management.

3.16.3 **Revisit the restrictions on PSP’s preventing additional language, warnings, or controls in the Open Banking payments journeys**. In our direct internet/mobile banking channels we show a range of tailored messaging targeted at reducing APP fraud. We are prevented from doing the same in Open Banking payment journeys as part of the Open Banking Standard, even though this addition of positive friction could prevent fraud and improve customer outcomes.

3.17 These Open Banking consumer protection measures will also have a positive contribution to the development of the A2ART ecosystem. If A2ART is to successfully compete with other established payment options, it will have to provide a comparably high standard of protections and mitigations, to generate trust and incentivise participants to drive switching away from these alternative payment options.

3.18 In fact, the acceleration of A2ART could make it more difficult for consumers to spot scams, unless there are common standards and trusted marques underpinning them, such as mandatory TRIs and CoP.

#### 4. Do you have any comments on our proposals:

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**

4.1 Banks play a crucial role in preventing fraud for the benefit of consumers and our broader society, and Lloyds Banking Group is committed to this. We recognise that the risk of fraud is frightening for consumers, especially the most vulnerable. It is therefore essential that consumers understand the steps they can take to protect themselves and prevent the fraud from occurring in the first place. Fraud prevention must be a shared societal aim where we all have our part to play.

4.2 Consumers taking a degree of responsibility for their own actions, alongside firms, is not a new concept. It exists as a core principle under the Financial Services and

Markets Act which underlines 'the general principle that consumers should take responsibility for their decisions'.

- 4.3 We therefore agree that there should be a consumer caution exception to mandatory reimbursement.
- 4.4 While we agree that consumer caution should be the exemption, we do not believe that gross negligence is the appropriate definition of customer caution. Gross negligence is an exceedingly high bar and creates a very significant risk of legal complexity and ambiguity. Gross negligence has been defined in a number of different ways by the Courts, so there is no final, settled definition that can be clearly understood by consumers or institutions. This creates a high risk of inconsistent approach, to the potential detriment of customers. Additionally, consumers may see the term as judgemental, potentially adding to their distress.
- 4.5 In order to protect consumers and ensure robust fraud prevention, it is crucial that consumers are confident on the steps they can take to protect themselves from fraud. As such, we recommend the introduction of a "*minimum level of caution consumers must take when making payments if they are to be reimbursed following a scam*" (referred to in this response as 'minimum level of caution').
- 4.6 We propose that the minimum level of caution is agreed upon and applied at industry level, with support and input from consumer groups. A minimum level of caution understood by both PSPs and consumers will provide greater clarity and certainty, thereby ensuring consistency in application and outcomes.
- 4.7 For minimum level of caution, we suggest that the customer should take two actions where it would be considered reasonable for them to do so:
  1. take heed of any bank warning that is very clear and specific in nature, and
  2. demonstrate that they have completed a basic check or seen some evidence to validate that the recipient is genuine.
- 4.8 Taking heed of any specific bank warning would include a Confirmation of Payee "no match" warning, along with specific warnings given online or verbally through telephony and branch channels. This should include invoking the Banking Protocol where the police also try to intervene when we believe a customer is involved in a scam and insists on sending payments.
- 4.9 What constitutes a basic check or some evidence to validate that the recipient is genuine may vary depending on the scam type and supplementary guidance would be required. We view this as a lower requirement, and therefore better for consumers, than the CRM Code's "reasonable basis for belief", this should consequently increase reimbursement across the industry.
- 4.10 As a starting point, examples of a basic check for consumers could be:
  - Calling a company using the number from a trusted source (an official letter or the company's genuine website, sourced independently rather than using the

website the fraudster might have provided), before replying to a text or e-mail seeming to be from this company

- Checking a company's reviews on an independent website (e.g., TrustPilot) before placing an order, particularly for an item or service that sounds 'too good to be true'
- Verifying an investment firm is genuine by using the FCA website to make sure the company is authorised to sell investments

- **not to provide additional guidance on gross negligence?**

4.11 The minimum level of caution should reduce the need to rely upon a gross negligence exception to mandatory reimbursement and removes the legal risk and precedent as a result of claims focusing on defining gross negligence. However, for completeness, gross negligence should remain as an exemption to reimbursement.

4.12 As outlined above, given the legal complexity of interpreting gross negligence, we are supportive of the proposal not to provide additional guidance. This support is contingent on the PSR adopting the minimum level of caution exemption to mandatory reimbursement, along with additional guidance.

4.13 As we mentioned in our response to the consultation in November 2021, following the launch of the CRM Code the Financial Ombudsman Service (FOS) received a large number of escalated APP scam cases which implied that there was a lack of clarity on how the CRM Code should be applied. If a clear definition of the 'minimum level of caution', equally understood by Consumers, PSPs, and the FOS, is not provided to accompany the reimbursement requirements, we risk seeing a repeat of the escalations to the FOS.

4.14 While we recognise the role the FOS will play in helping to provide clarity to firms on their interpretation of regulations, we do not believe this should be used in place of guidance provided to help firms when regulations are implemented. It is important that an over reliance on the FOS to define minimum level of caution or gross negligence is avoided.

4.15 We recommend the PSR works collaboratively with the FOS, the Financial Services sector and consumer groups, ahead of the policy statement, to provide this definition to ensure certainty and clarity around requirements for consumers and firms - thereby creating a sustainable model.

## **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

5.1 We understand the role we play in supporting customers in vulnerable circumstances. We have a dedicated strategy in place, including to understand and respond to the needs of customers' individual circumstances, supporting customers to receive fair outcomes.



- 5.2 Therefore, we welcome the broad principle that vulnerable customers should be reimbursed even where there was no minimum level of caution, or they acted with gross negligence.
- 5.3 However, while some vulnerable customers may be more susceptible to falling victim to a scam and may not have had the ability to take action to protect themselves, this will not always be the case. It is essential that vulnerable customers receive the right treatment and outcome, in relation to their individual circumstances.
- 5.4 For this reason, as we outline in our response to Question 6, the application of the FCA's definition supports the view that not all characteristics of vulnerability will make a customer more susceptible to falling victim to a scam, in which case a blanket exemption from gross negligence, or our proposed 'minimum level of caution' will not apply.

## **6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

- 6.1 We are supportive of the proposal to use the FCA's definition of a vulnerable customer. This should specifically be in relation to the risk of harm through "scams and financial abuse".
- 6.2 The FCA definition is that a vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care.
- 6.3 We note that in the FCA's guidance when considering "scams and financial abuse" it highlights that "consumers with some characteristics of vulnerability *may* be more likely to fall victim to scams, including misleading online financial promotions". The use of the word "may" indicates that the FCA accepts that not all consumers with some characteristics of vulnerability *will* be more likely to fall victim to scams.
- 6.4 We believe the FCA definition provides flexibility for firms to assess the relevance of the circumstance to the APP claim. This would be based on the impact of the consumer's personal circumstances and how this made the consumer especially susceptible to harm at the time of the scam.
- 6.5 We do not interpret that the use of the FCA's definition would provide all customers with characteristics of vulnerability a blanket exemption from gross negligence, nor our proposed 'minimum level of caution'. For example, if a customer has a physical health condition it does not always mean they were more susceptible to falling victim to a scam.
- 6.6 It is important that the PSR and organisations such as the FOS apply the FCA's definition consistently.
- 6.7 We understand it is not the role of the PSR to ensure firms understand and apply the FCA's definition correctly. However, while the FCA's vulnerable customer guidance is



extensive, there is limited consideration given specifically to APP scams. We believe it would be beneficial for the PSR to work with firms to develop additional guidance to be provided alongside the reimbursement model.

**7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

7.1 While we understand the intended objective of the PSR is to create some incentive for consumers to take care, we do not believe that an excess is the appropriate mechanism for this. We recommend that the PSR withdraws this element of the reimbursement model.

7.2 Section 77 of the PSR17 allows PSPs to pass liability on to the customer up to £35 in the case of unauthorised transactions. However, PSPs do not generally make use of Section 77, suggesting that an excess of £35 does not create significant benefits.

7.3 An excess will likely be confusing for consumers and create unnecessary operational burden for PSPs.

7.4 From a consumer's point of view, we believe there would be confusion as to the purpose of the excess. This could be viewed as an excess comparable to that of an insurance policy, or a fee for processing the claim.

7.5 As we have outlined in response to Question 4, we believe that the incentive to take care would be by the introduction of the minimum level of caution a customer should take when making a payment. If the customer has taken care, they should be reimbursed in full.

7.6 Furthermore, as we outline in response to Question 8, the minimum threshold will provide the appropriate incentive for customers to take caution when using Faster Payments to pay for low value purchases.

**8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**

8.1 We welcome the introduction of a minimum claim value to enable greater focus on the most life changing scams. However, the ability for PSPs to set their own minimum claim threshold would create a confusing landscape for consumers who may hold accounts with multiple PSPs across which the thresholds differ.

8.2 We recommend that in order to provide clarity and consistency of approach for customers the minimum should be set at an industry level, defined within the reimbursement requirements.

- **any threshold should be set at no more than £100**

8.3 We do not believe that £100 is set at a level which will disincentivise buyer seller disputes and promote 'buyer beware' for purchase scams.

8.4 Our analysis shows that over █% of claims under £250 are purchase scams.

8.5 We therefore recommend that the minimum threshold is set at £250. Furthermore, this may need to be revised over time to account for changes in the fraud, or wider economic landscape. We recommend that this should be reviewed on a regular basis, and at a minimum every five years.

- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

8.6 We believe that the minimum threshold should be the industry boundary above which the reimbursement model is effective across all consumers, including those with characteristics of vulnerability. However, PSPs will of course continue to have the discretion to reimburse outside of the model, particularly taking into consideration customers for whom the loss of a small amount of money is particularly detrimental to their financial wellbeing and stability. This reimbursement would not be subject to the other requirements of the model, e.g. 50:50 allocation.

## **9. Do you have comments on our proposal not to have a maximum threshold?**

9.1 We agree with the PSR's statement that "PSPs typically have the strongest safeguards in place for the largest payments". However, the PSR should note the highest value scam claims typically represent a customer sending multiple payments over a period of time. The PSR should be clear in the requirements that both the minimum and maximum threshold apply to the total claim value not individual payments.

9.2 We propose there should be a maximum threshold for claims that are automatically subject to the mandatory reimbursement model articulated in the PSR directions.

9.3 However, customers with higher value claims should not be disadvantaged by this limit, and therefore, we propose that in order to evaluate the more complex, high-value cases, there should be an extraordinary process developed through industry working groups to ensure consistency for consumers.

9.4 We ask the PSR to work with the industry to both define at what level this process is triggered and how this process should differ from the "standard process". We also recommend that the extraordinary process would require additional time with which to evaluate the claim.

9.5 We also reiterate our position in our response to Question 3 that the final rules should confirm that only payments authorised after the reimbursement model comes into force will be eligible for mandatory reimbursement.

**10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

10.1 We agree that there should be a time-limit for customers making an APP scam claim. However, we disagree that PSPs should be able to set their own time-limit for claims under these reimbursement proposals.

10.2 We reiterate the importance of industry wide alignment which is clear and consistent for consumers.

10.3 Our analysis shows that approximately 80% of scams are typically reported within 2-3 months of the final payment, with 99% reported within 13 months.

10.4 We agree that setting a time limit for claims at 13 months, from the final payment involved in the APP scam, seems appropriate. However if the industry view was this should be extended to 24 months, we would be comfortable with that approach.

10.5 We also reiterate our position in our response to Question 3 that the final rules should confirm that only payments authorised after the reimbursement rules come into force will be eligible for mandatory reimbursement.

**Section 5: Allocation of reimbursement costs**

**11. Do you have comments on our proposals that?**

- **the sending PSP is responsible for reimbursing the consumer**

11.1 For first-generation, non-PISP-initiated payments, we agree that sending PSP has a direct relationship with the consumer making the claim and therefore it is best placed to issue the reimbursement.

11.2 However, as we highlight in our response to Question 15, multi-generation claims are complex and require further consideration. The reimbursement requirements for each type of multi-generational scam, and associated victims, should be established as part of the review we have proposed.

11.3 In addition, in order for the sending firm to recoup the 50% share of the reimbursement for which it is not liable, it is imperative that a set of industry-level Service Level Agreements (SLAs) are defined. These should clearly articulate what is expected of the receiving PSP, and where applicable the PISP, in terms of reimbursing the sending PSP. These must be defined ahead of the model coming into force, to ensure efficiency and PSP confidence in the model. We support an enforced fine system to address receiving PSPs' failure to reimburse the sending PSPs within the agreed SLAs.

- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

- 11.4 We agree that reimbursement should be made within the shortest timeframe possible and there should be an industry-wide standard to provide a consistent consumer experience. However, as part of evaluating the claim, firms need time to both gather the information from the customer and engage with the recipient PSP.
- 11.5 We recognise the PSR's intent that customers be reimbursed in line with claims for unauthorised fraud. However, for APP fraud, in order to assess a claim the sending PSP must gather the required information from the customer and then engage with the receiving PSP to clarify the validity of the claim. 48 hours is not operationally achievable due to the complexity of some claims, the time required to investigate thoroughly, the operating hours of certain firms (not all PSPs work 7 days/week), and/or the receiving account being with a non-financial services company (which tend to be more difficult to contact).
- 11.6 Due to the high emotional impact that scams have on customers, they may not be able to recall the full facts of the scam on their first engagement with the PSP. This is something that we have found common, particularly where a customer is vulnerable, or where the scam took place over an extended period involving multiple transactions. Setting an unrealistic timeframe and requiring the customer to provide all the information in a very limited timeframe could cause additional, unwarranted distress.
- 11.7 Even in cases where the PSP was able to gather information from the customer within the 48-hour timeframe, there is still the risk that it might arrive at incorrect outcomes due to insufficient time left to properly assess the case.
- 11.8 The CRM Code currently applies to a significant proportion of Faster Payments. Given this is already in place, we recommend that the PSR adopts the current CRM Code timeframe of 15 working days with an extension to 35 working days for more complex cases.

## **12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

- 12.1 As mentioned in our response to Question 11, we believe that all cases should have an extended period to reimburse customers.
- 12.2 The timeline we have outlined would be sufficient to investigate the claim, make the decision and where appropriate reimburse the customer.
- 12.3 This timeline should be included in customer literature relating to the reimbursement model and explained to the customer on the initial contact, setting their expectation of the process.

12.4 We do not believe it is helpful or appropriate to suggest that additional time is required due to a suspicion of first party fraud (which carries the risk of 'tipping off') or gross negligence.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

13.1 We welcome the inclusion of the receiving PSPs in the allocation of reimbursement cost. There is inconsistency of approach across the industry in preventing the ability of fraudsters to gain access to bank accounts and monitoring the ongoing use of accounts. Receiving PSPs sharing the liability costs should incentivise firms to implement more prevention measures.

13.2 However, as mentioned in our response to Question 1, the responsibility to prevent fraud should be shared by all the actors in the wider ecosystem, including social media giants and telco firms. Unless all participants in the chain are obliged to take anti-fraud measures there will always be opportunity for fraudsters to exploit gaps to defraud customers. This responsibility must include shared liability for reimbursement.

13.3 We would welcome the PSR's assistance in gaining support from other regulatory bodies covering upstream actors to create a mechanism for wider sharing of responsibility. However, if the reimbursement model is implemented before other actors can be brought into scope, we agree with the proposal for a 50:50 allocation of reimbursement costs.

13.4 We believe this should be fixed at 50:50 to reduce complexity and should be reviewed when other actors are brought into scope.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

14.1 We strongly believe that, if the reimbursement model is implemented before other actors can be brought into scope, the future reimbursement model should not allow PSPs to be able to choose to depart from the 50:50 default allocation by negotiation, mediation, or dispute resolution. The reimbursement model should operate with fixed 50:50 allocation of reimbursement costs between sending and receiving PSPs.

14.2 Tackling fraud requires a great amount of collaboration across the industry and we are keen that this collaboration is encouraged and supported as much as possible.

14.3 We are of the view that a departure from an equal split of the reimbursement costs could inadvertently damage collaboration between firms and sectors, which would ultimately affect consumers.

- 14.4 We believe that initially, on a case-by-case basis, there may be more that the sending firm or the receiving firm could have done to prevent the fraud. However over time the reimbursement model will incentivise PSPs to individually and collectively do more both as a sending and a receiving firm.
- 14.5 A dispute framework would also add an unnecessary layer of complexity to a process which is already likely to present significant operational challenge for firms, particularly those that have not participated in the CRM code.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

- 15.1 We cannot support the inclusion of multi-generational scams within the reimbursement model unless significant work is undertaken by the PSR with assistance from the industry to develop a robust solution to multi-generational scams including the role of all PSPs within the chain, both for reimbursement of each victim and the allocation of the reimbursement costs.
- 15.2 Even the most 'simple' cases of multi-generational scams are intricate and make it difficult to identify with certainty the sending PSP. We have given consideration to a number of scenarios to operationalise a multi-generational model however, through current legislation it is not possible for firms to share the necessary data concerning multiple victims and beneficiaries across PSPs for end-to-end analysis of the case. This is one of the reasons why we support measures in the Economic Crime and Corporate Transparency Bill and Data Protection and Digital Information Bill to ensure appropriate data sharing.
- 15.3 In addition there is currently no framework for repatriation of funds across multiple payment generations where funds are frozen in an account further along than first generation payments.
- 15.4 Due to the complexity of multigenerational claims and current reporting and tracking mechanisms it is not possible to accurately quantify the number of claims this would exclude. However, no matter the scale of the issue, a solution must be sought for the consumers affected as soon as it is reasonably possible.
- 15.5 Further, we believe that fraudsters, knowing that multi-generational scams were out of scope, may target this as an area of vulnerability.
- 15.6 We would support the inclusion of multi-generational scams in the initial implementation of the model if the issues raised have been addressed beforehand.
- 15.7 We would urge the PSR to work at pace to solve this by setting up and leading industry working groups which should also consider the role of non-PSPs (i.e. crypto wallets and foreign exchange firms). These discussions should also consider the controls and tools required to ensure there are the correct level of mitigations in place to prevent fraud.

15.8 If this work is not concluded ahead of the implementation of the model, the industry must have clear standards to identify and therefore exclude multi-generational scams. Industry misalignment on definition of this type of scam could lead to the potential for an inconsistent approach across firms. We believe that this issue further supports our recommendation to pause the consultation.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

16.1 In line with our responses to Questions 13 and 14, we support a fixed, 50:50 split of repatriated funds, between the sending and receiving firm.

16.2 Furthermore, as mentioned in our responses to Question 11, it is imperative that a set of industry-level SLAs, clearly articulating what is expected of the receiving PSP in terms of reimbursing the sending PSP, is defined ahead of the model coming into force, to ensure efficiency and PSP confidence. We would support an enforced fine system to address receiving PSPs' failure to reimburse the sending PSPs as per the agreed SLAs.

16.3 Where a consumer has not been found to be eligible for reimbursement, any repatriated funds should be returned in full to the consumer.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

17.1 We agree with the scope of the PSR's proposal to apply the rules on allocating the costs of reimbursement to all direct and indirect participants sending and receiving payments over Faster Payments.

17.2 Our strong preference is for the PSR to give a specific direction to mandate all direct and indirect PSPs to comply with the reimbursement proposals that it makes – this is in line with the PSR's specific direction to extend the implementation of Confirmation of Payee (a decision which we strongly supported).

17.3 The consultation recognises a trend of fraudsters migrating to receiving PSPs who are not participating in existing safeguards including the CRM Code and CoP. Therefore, we strongly recommend that the PSR implements the reimbursement requirements for all PSPs unilaterally, at the same time rather than via a phased approach.

**PART B: How we propose to implement our requirements**

**Section 6: Our long-term vision for Pay.UK's role**

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

- 18.1 We agree that the role of Pay.UK as Payments System Operator (PSO) is valuable and should be galvanised to mitigate and reduce fraud across Faster Payments Scheme. However, we believe that the PSR's long-term vision for Pay.UK requires careful consideration and potentially a change in approach, to enable the successful deployment of the desired reimbursement model alongside fraud prevention measures.
- 18.2 As the PSR highlighted in the consultation paper, Pay.UK already has significant commitments, not least developing and implementing the NPA, which may not leave sufficient capacity for it to productively engage in and deliver another resource-heavy project, which the proposed APP fraud reimbursement model will undoubtedly be.
- 18.3 We strongly believe that, at least in the short term, Pay.UK should focus on building and implementing the NPA, developing and embedding fraud detection and prevention tools across the payments ecosystem (which should be future proofed for the NPA), developing a viable economic model and an enhanced consumer protection framework to underpin A2ART in collaboration with JROC and Open Banking Implementation Entity (OBIE).
- 18.4 As we lay out in more detail in our response to Question 19 it is our strong preference that in the short term the PSR implements the reimbursement model by giving specific direction to mandate all direct and indirect PSPs to comply with the reimbursement requirements and thus ensure consistency across the industry.
- 18.5 We recommend that the PSR revisits the long-term vision for Pay.UK's role as part of its post-implementation review.

## **Section 7: Short-term implementation of our requirements**

### **19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

- 19.1 In the consultation the PSR expresses the preference to implement the reimbursement requirements through changes to the Faster Payments Scheme rules. It notes the alternative would be for the PSR to impose the requirements on all PSPs through directions, and for Pay.UK to operationalise the requirements.
- 19.2 Our strong preference is for the PSR to give the specific direction to all direct and indirect PSPs to comply with the reimbursement requirements.
- 19.3 Indirect PSPs should be held directly accountable, rather than via their IAP. Implementing through a direction on all PSPs would ensure that there is consistency of approach and would be subject to the same enforcement model. This would mitigate the challenges the PSR has noted which would exist if they were to require Pay.UK to implement, or if the direction was on IAPs.



- 19.4 There would be significant negative consequences for IAPs, should the PSR decide not to implement reimbursement requirements via a direction on all PSPs. This is covered in detail in our response to Question 25 & 26.
- 19.5 The direction on PSPs should cover all aspects of the reimbursement model which should be consistent across the industry including:
- When a consumer must be reimbursed by their sending PSP
  - The 50:50 allocation of reimbursement costs (and of any repatriated funds) between the sending and receiving PSP
  - Arrangements needed to enable sending and receiving PSPs to transfer funds between them, SLAs for this and an enforced fine system to address receiving PSPs' failure to reimburse the sending PSPs as per the agreed SLAs
  - Any relevant boundaries including: minimum threshold, maximum threshold, time-limit for claims
  - Exemptions to mandatory reimbursement
- 19.6 Scheme rules could complement the PSR direction by setting the minimum standards PSPs to which must adhere. Scheme rules may include, but not be limited to, onboarding requirements, the provision of payment warnings, data sharing and performance reporting.

## **20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

- 20.1 As outlined in our response to Question 19 our strong preference is for the PSR to impose the requirements on all PSPs (direct and indirect) through directions. The directions should include a rule which brings into scope unregulated firms that have been the recipient of first-generation scam proceeds.
- 20.2 We believe this is the only option that directly holds indirect PSPs to account without intervention or oversight from the IAP. This creates clarity and consistency across the market.
- 20.3 We understand that the form and content of any new Specific Direction and how it would work in practise will need further consideration and consultation.
- 20.4 We also note that any such directions will not cover payments outside of the FPS and welcome the PSR's commitment to give further consideration on how these payments would be brought into alignment with Faster Payments in the future.

## **21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

- 21.1 As noted under Question 14, we strongly believe that the future reimbursement model should operate on a fixed equal distribution of fraud costs, with no option to depart from this via a dispute process.

21.2 However, as we note in response to Question 9, the only exception to this is for the extraordinary process for claims above the maximum threshold. This process may require the ability for firms to mediate through dispute resolution.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

22.1 We support a system that monitors and ensures a high level of compliance, but we are concerned there will be duplication of efforts for PSPs across different regulators and urge the PSR to work with the FCA to remove this risk as much as possible.

22.2 Real time monitoring, however, is unnecessary and creates operational burden. If this is still something the PSR is minded to pursue, then a full cost benefit analysis should be undertaken.

22.3 If possible, the PSR should encourage the industry to build on existing capabilities and systems, such as the Best Practice Standards (BPS) platform operated by UK Finance. BPS is in a good position to allow, in the future, PSPs to share information from the point of the PSP becoming aware of the scam, through to repatriation and the allocation of funds across PSPs.

22.4 Not only have PSPs invested significant resources into building this platform, but they have also developed advanced technology internally, both in the capacity of sending and receiving PSP, to be able to interact with the platform in real-time, or near to real-time, manner.

22.5 While the platform will need additional work to accommodate the PSR's monitoring requirements, it provides a very good starting point as it is being used by a significant number of PSPs which would have already performed information security and data privacy controls that allow them to comfortably utilise BPS.

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

23.1 The costs of developing and implementing a new real-time monitoring system will depend on method of implementation, and final reimbursement model requirements. However, as set out above, we believe it will most likely be unnecessary and create significant operational burden, thereby reducing efficiency.

**24. Do you have views on the best option for short-term enforcement arrangements?**

24.1 Our strong preference is for the PSR to initially implement the reimbursement requirements on PSPs through a direction. As the PSR recognises in the consultation this would mean enforcement of those requirements would also fall to the PSR.

24.2 Irrespective of the implementation method we believe that the best option for short-term enforcement would be for this to sit with the PSR.

24.2.1 While Pay.UK does have a scheme compliance monitoring capability today, its enforcement powers on a day-to-day basis are limited to scheme exclusion if a participant is unable or unwilling to comply. While most PSPs have a robust self-certification regime around compliance which drives any corrective actions, we are concerned that some PSPs may exploit this gap with regards to reimbursement requirements. This would leave Pay.UK in the difficult position of not having the tools to drive enforcement.

24.2.2 Furthermore Pay.UK's powers do not apply to indirect participants. As the PSR notes in the consultation paper, indirect participants are responsible for a significant number of Faster Payment transactions. As we highlight in our response to Question 25 below, the PSR should avoid an implementation method that involves an IAP taking on an additional compliance and monitoring function for its indirect customers.

24.2.3 By contrast to Pay.UK, the PSR already has a range of enforcement capabilities, and covers both direct and indirect PSPs. It follows that the most streamlined option would be for the PSR to enforce compliance. The PSR could also engage and collaborate with the FCA to enforce compliance through the latter's existing direct supervisory relationships with the PSPs.

24.2.4 We are also concerned that if Pay.UK was to be responsible for compliance and enforcement, PSPs would be operating in a fragmented, complicated regulatory landscape where they would need to work across multiple regulators. This could, among other issues, result in efforts being duplicated, creating significant inefficiency.

24.3 As referenced above, we strongly believe the enforcement arrangements should also include an enforced fine system to address receiving PSPs' failure to reimburse the sending PSPs as per the agreed SLAs.

## **25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

25.1 As outlined in our response to Questions 2 and 19, our strong preference is for the PSR to impose the requirements through directions on all PSPs.

25.2 We note the significant negative consequences for IAPs, should the PSR decide not to implement reimbursement requirements via a direction on all PSPs, and instead chooses either of the remaining two implementation options: i) applying the FPS rules on reimbursement to all transactions; and ii) a direction to IAPs to ensure transactions by the indirect PSPs comply with the reimbursement rules in FPS.

25.3 Either of these implementation options will place a significant burden on the IAP to monitor and enforce compliance on its indirect customers. This would therefore be an additional consideration for assessing eligibility for providing services to indirect PSPs, leading to a more stringent risk appetite and thereby reducing availability of indirect access services with the knock-on effect on competition in the market and ultimately consumer choice.

25.4 Furthermore, if an indirect PSP was not able to meet its obligations in the FPS, we do have concerns about the additional financial burden for IAPs. For context, as an IAP, we have circa [REDACTED] agency and non-agency indirect PSP customers. If we were to be held liable for the transactions enabled by our indirect PSP customers, we would need to reconsider the terms and conditions for sponsoring a firm into the FPS to mitigate this new risk.

## **26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

26.1 As outlined in our response to previous questions, our strong preference is for the PSR to impose the requirements through directions on all PSPs. The direction should be on the indirect PSP and not the IAP.

26.2 We offer two types of indirect access to agency and non-agency PSPs:

- Agency PSPs: bound through bespoke contracts to the appropriate Scheme rules, responsibilities, and liabilities of each of the payment systems accessed
- Non-Agency PSPs: supported by standard commercial banking contracts and terms and conditions which do not bind them (currently) to Scheme rules.

26.3 In addition to the significant negative consequences for IAPs, should the PSR decide to implement reimbursement requirements via a direction on the IAP, this would present the need for additional complex review, update and implementation of contracts resulting in further lengthy and unnecessary burden on all parties.

26.4 Furthermore, we cannot distinguish which transactions are made by the indirect PSP for its own purposes or on behalf of its customers. As we cannot see the end-to-end payment flows the PSR would be placing a direction on us, as an IAP, that we cannot reasonably fulfil.

## **27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

27.1 While we understand the rationale behind the methodology applied to the cost benefit analysis included in the consultation paper, it is our overall view that once the proposals have been agreed, the PSR should consider conducting a further detailed cost / benefit analysis. This would ensure that any significant costs, either to industry or consumers, are recognised and are acceptable relative to the benefits

the reimbursement model will deliver once agreed. This aligns to the intention behind the Financial Services and Markets Bill's new Cost Benefit Analysis panels.

- 27.2 In addition, we believe that akin to many other initiatives and previous policy changes in the fraud landscape, the financial benefit may be overestimated. There has been limited consideration to the evolution of fraudsters. History tells us through initiatives such as implementation of CoP that fraudsters may find ways to circumvent the controls firms have in place. Therefore we believe the potential reduction in cost of fraud of £100-150 million to be overestimated.
- 27.3 We would also highlight it is unclear what period this applies to and/or if this is a projected year-on-year reduction.
- 27.4 In relation to the publication of scam data as part of Measure 1, we disagree with the current approach outlined by the PSR. We provided feedback on this in the previous consultation. Our view is that ranking firms' performance overall based on volumes and total value of fraud does not truly reflect the performance across firms. We also believe there may be a risk of unfair and unbalanced reputational damage to PSPs as a result of publishing reimbursement rates. We propose the PSR considers a tiered model of reporting on firms, akin to that of cards – an existing model which we feel provides a proven track record of performance reporting. This would be more effective in understanding firms controls and allow for sharing of best practice across the industry.
- 27.5 The PSR states the policy provides incentives to receiving firms to improve their detection and prevention of APP scams. While we agree to an extent with the PSR's view that financial impact on receiving firms will incentivise them to develop stronger controls, our view remains that additional legislative and regulatory change is required to fully equip PSPs with tools to prevent fraud. Without the appropriate data sharing and tools in place across firms ahead of the launch of the mandatory reimbursement model, firms will be unable to maximise their efforts to prevent fraud.
- 27.6 We appreciate that the PSR believes the impact of mandatory reimbursement on customers failing to take due care is low, and that firms do not have data to demonstrate that customers consequentially taking less care will happen more frequently. However, there is no data to prove or disprove this either way. Therefore it should be acknowledged as a risk to the Cost Benefit Analysis as put forward in the consultation.
- 27.7 We believe the other actors in the ecosystem have a role to play in preventing fraud and should form part of the liability model. Without this in place we will not see the effect desired by the PSR to reduce APP scams, and victims will continue to face the emotional distress and lack of confidence in payment methods post fraud.

## **28. Do you have any other comments on the proposals in this consultation?**

- 28.1 The PSR should take time to further consider the complexity that mandatory reimbursement brings and should guard against implementing interim measures at

pace which would then need to be changed in the medium term. A right first-time approach would avoid confusion for PSPs and consumers in this already complex landscape.

- 28.2 While the consultation does not discuss the future payments landscape, we recommend the PSR considers this in the development of the reimbursement requirements.
- 28.3 While Faster Payments is undoubtedly an innovative platform, it was never built to support customer to business transactions and direct commerce, which is increasingly used for today. Further, there is a substantial imbalance between the protections and security offered when compared to the card schemes (e.g. Section 75, disputes, chargebacks).
- 28.4 These protections should be sufficiently developed before the further widening of Faster Payments use cases, such as through Open Banking, to avoid consumer confusion, market fragmentation, and to promote trust in the payment channel which will in turn provide greater choice for businesses.
- 28.5 It is crucial that consumer protections are underpinned by a sustainable economic model – in part funded by merchants, as the credit and debit card networks are today. In the case of consumer to business payments, a commercial fee arrangement in the style of interchange is likely needed alongside associated checks and balances on businesses. It is not sustainable for PSPs to absorb the costs of all consumer protections, and this may create further market distortions. Therefore, a robust framework and infrastructure for consumer protection must be developed at pace for delivery into the NPA and alongside work by JROC on A2ART. We are keen to support the development of such an approach working with regulators, industry and other bodies and look forward to continuing to work together on this.
- 28.6 In our response to Questions 1 and 3 we have recommended a number of legislative and regulatory changes and reforms. We have summarised these in the table below which highlights our request to the PSR and the issue each addresses.

<b>Change required to complement the PSR reimbursement proposals</b>	<b>Request of PSR</b>	<b>Issue it addresses</b>
<b>Payment friction</b>	<p>Work with HMT to amend Regulation 86 in the PSRs 2017 to give PSPs non-time bound ability to delay payments (which should not usually extend over more than a couple of days) to pause a payment where there is a high risk of fraud.</p> <p>Work with the FCA, which has set an expectation of payments being received within two hours, to update its guidance to allow sufficient time for robust fraud prevention.</p>	<p>PSRs 2017 do not give PSPs comfort to hold a payment for more than one business day to address any high-risk flags that indicate the customer has fallen victim to an APP scam or that the recipient might be acting as a fraudster, or as a money mule.</p>
<b>Data sharing across sectors</b>	<p>Work with the industry to ensure legislation in the Economic Crime and Corporate Transparency Bill and Data Protection and Digital Information Bill is delivered.</p>	<p>Banks and other private sector organisations currently have no clearly defined provisions to permit sharing customer information to effectively assist in preventing and detecting economic crime.</p>
<b>Bring all fraud-enabling sectors into the solution, including sharing liability within the reimbursement model</b>	<p>Engage with HMG, alongside the industry to advocate for social media giants, online services and telecommunications firms introducing robust fraud prevention measures and sharing the costs of fraud where they helped to facilitate it.</p> <p>Online Safety Bill could introduce a requirement for Ofcom to mandate online platforms and services to share fraud liability with the PSPs.</p>	<p>Non-FS, fraud-enabling firms are currently not incentivised to increase their fraud prevention measures, nor are they included in the sharing of reimbursement liability within the current proposals.</p>
<b>Central governmental accountability for fraud</b>	<p>Recommend the government to appoint a Minister of Economic Crime to provide coordinated leadership, supported by a specific Scams Lead to energise and champion change.</p>	<p>There is a lack of clear coordination across the public sector impacting operational and policy coherence.</p> <p>A shared view of threats with better ability to coordinate activity across HMG, regulators, law enforcement and the private sector would help to prioritise threats and support</p>

		realignment of resource against these.
<b>A government-led public information campaign</b>	Fraud is a national security issue and the PSR should encourage HMG to launch a national campaign in partnership with the industry to educate consumers and raise fraud awareness.	Consumers are not fully equipped to recognise and avoid scams.
<b>Mandatory adoption of TRIs and CoP for PISPs</b>	Work with Pay.UK and OBIE to introduce requirements for PISPs on each payment to: <ul style="list-style-type: none"> <li>• utilise TRIs</li> <li>• apply CoP checks either directly or through the PSP (i.e., the PSP performs the CoP service as a chargeable service to PISPs)</li> </ul>	Open Banking transactions do not benefit from robust controls akin to the existing ones for Direct Channels.  These measures would also have a positive contribution to the development of the A2ART ecosystem. If A2ART is to successfully compete with other established payment options, it will have to provide a comparably high standard of protections and mitigations, to generate trust and incentivise participants to drive switching away from these alternative payment options.
<b>Additional language, warnings, or controls in the Open Banking payments journeys</b>	Work with Pay.UK and OBIE to revisit the restrictions on PSPs preventing additional language, warnings, or controls in the Open Banking payments journeys.	In our direct internet/mobile banking channels we show a range of tailored messaging targeted at reducing APP fraud.  We are prevented from doing the same in Open Banking payment journeys as part of the Open Banking Standard, even though this addition of positive friction could prevent fraud and improve customer outcomes.
<b>Increased law enforcement capacity and capabilities to capture and remove criminals</b>	Join industry in proposing that Government increases public spending on law enforcement to enable both recruitment and fraud training.	While fraud is now recognised as the single biggest crime, the focus of law enforcement and prosecution is limited. In 2021 there were c120 suspect interventions made through the Dedicated Card and Payments Crime Unit's (DCPCU) work.  Greater investment would increase capacity and capability within law enforcement agencies to pursue a much higher number of cases.



**We thank the PSR for taking the time to read our views and would be happy to discuss any of the points raised in our response in further detail if it would be helpful. We look forward to working with the PSR and industry to achieve an outcome which is in the best interests of customers and fair and proportionate to all parties involved in the APP fraud landscape.**

# Lyddon Consulting

8<sup>th</sup> November 2022

APP scams  
Payment Systems Regulator  
12 Endeavour Square  
London E20 1JN

### **Authorised push payment (APP) scams: Requiring reimbursement CP22/4**

#### *Introduction*

The PSR's proposal as put out to consultation is tantamount to another admission of its failure to bring about a complete solution of this issue, 7 years after its creation at a point when the existence of APP scams was already known.<sup>1</sup>

Confirmation of Payee (CoP) was subsequently billed as a complete solution in the PSR's Payment Strategy for the UK, emanating from the Payment Strategy Forum.

Contingent Reimbursement Model (CRM) was then billed in 2019 as a necessary measure to complete this incomplete solution, by the PSR's APP scams group.

These were the original promises for these measures. Neither has even succeeded in arresting the increase in APP scams. It is no good continuing to force ever greater adoption of CoP and CRM and expecting a different result.

#### *Failure of CRM*

The Lending Standards Board, which administers the CRM, recently published a misleading article in the September 2022 edition of 'The Banker', written by Emma Lovell, its CEO.<sup>2</sup> The article was self-congratulatory about the CRM's success, and sought to deflect attention onto prevention as the proper focus for further progress.

This approach repeats the strategy of attempting to re-write the original marching orders. In Ms Lovell's case the claim of success only stands up if one both forgets what the original marching orders were – to eliminate APP scams completely in tandem with CoP – and if one overlooks serious logic flaws.

These flaws are contained in the paragraph 'Data shows that in 2018, the number of APP scam cases rose by 93 percent, with the rate of increase slowing to 45 percent in 2019 (when the CRM Code was introduced) and 23 percent in 2020.

---

<sup>1</sup> Confirmation of Payee was first proposed in 'World Class Payments in the UK: Enhancing the payments experience - An Initial Report August 2015' on p. 11, demonstrating that APP scams were already a known problem at that point  
<sup>2</sup> <https://internationalbanker.com/banking/app-scams-putting-prevention-in-its-rightful-place/> accessed on 22 September 2022

These statistics indicate that the CRM Code's prevention focus has stalled what could have been an exponential rise in APP scams. They also suggest that without the Code, cases would have continued to increase at a much higher rate..'

Ms Lovell attempts to bury the reality that APPF is still rising, by using percentages that infer a decline. Setting out real numbers demonstrates an almost straight-line increase. If APPF had a base of 100 in 2017, it increased by 93 to 193 in 2018, by 88 to 281 in 2019, and by 65 to 345 in 2020. That is not a drop-off but a very modest reduction in the rate of increase. It is a testament to the failure of the combination of CoP and the CRM.

Ms Lovell's contention that the statistics 'indicate that the CRM Code's prevention focus has stalled what could have been an exponential rise in APP scams' cannot be proven as no control experiment exists. It also introduces a false basis of comparison, that APP scams might have gone exponential if they had done nothing. Doing nothing was never an option. The real comparators are what would have happened if the CRM had been better written, or what might have happened if a quite different solution had been attempted.

*Important admissions at APP scams virtual roundtable event*

Two important, albeit much belated, admissions were made in the APP scams virtual roundtable event on Thursday 13<sup>th</sup> October 2022:

1. That it is the Faster Payments system that is the main carrier for APP scams; and
2. The contractual situation under APP scams is to do with the issue of defective execution of a payment by a payer's Payment Service Provider and needs to be construed with reference to the 2017 Payment Services Regulations.

The PSR continues to focus on two measures that have no impact on the core processing flow of a payment through the Faster Payments system. That remains unchanged, and will remain unchanged within New Payments Architecture.

CoP is an IT tool but it is configured as an 'overlay' service that bypasses the Faster Payments processing flow. CRM has no connection to the Faster Payments processing flow, is not an IT tool but a code in which the main contingency for reimbursement is that the payer had used CoP.

These are 'work-around' measures that are convenient and cheap for Payment Service Providers to implement but which have not solved the problem.

*The 'payments industry' has failed the UK's non-scammer Payment Service User*

These workaround measures serve to distract attention from the main problem: Payment Service Providers accept a payment order but then pay the wrong beneficiary. How can that happen if digital payments are so wonderful?

The measures serve to distract attention from two subsidiary problems as well:

1. Payment Service Providers opening bank accounts for scammers whose accounts are then accessible through the Faster Payments system;
2. The Bank of England having insisted on raising the Faster Payments system amount limit – now standing at £1 million – in order to make its own life easier and get payments off its CHAPS system which it does not consider systemically important.

The 'payments industry' - Payment Service Providers, the Faster Payments scheme company and now Pay.UK, Vocalink and now Mastercard, the Bank of England, the PSR itself – have contrived, via omission and commission, to create an instant payment system, with a high amount limit, accessible to all and sundry, and not having a basic control built into it – the payee name check.

*APP scams should be the responsibility of Payment Service Providers*

The incidence of APP scams has been accelerated through a multi-year policy by Payment Service Providers to promote digital payments and inhibit the usage of cheques and cash. Faster Payments is a main carrier for this 'digital payments journey'. It benefits PSPs in terms of cost reduction and the transfer of risk onto the Payment Service User. This result fails a basic test of fairness.

Payment Service Providers designed the Faster Payments system to their own requirements, without the involvement of Payment Service Users. APP scams represent an unfair risk distribution between Providers and Users. The re-balancing of the risk distribution requires changes to the 2017 Payment Services Regulations and the Funds Transfer Regulation.

Payment Service Providers will then be liable for defective execution under the terms of the 2017 Payment Services Regulations in all cases where they contrive to effect payment to a different payee than the one named in the payment order by the payer.

*Impact for Payment Service Providers*

Payment Service Providers will then have a simple choice:

1. Pay out the losses; or
2. Alter the Faster Payments processing flow so that a mismatch of the name is returned by the payee PSP to the payer PSP.

The Payment Service Providers can make up their own minds about which direction to choose, without any involvement from or impact on Payment Service Users. They can choose to make an alteration on the Faster Payments system now, or as a Day 1 deliverable of New Payments Architecture, or never. The Payment Service User will be protected under all eventualities, and CoP and CRM can be closed down as soon as the solution we propose has been completed. CoP and CRM have been stop-gap measures at best, and should be closed down as soon as possible given their failure in tandem to solve the problem.

*Our proposal*

Here, then, is our proposal and its rationale.

**Background**

This problem occurs because payment services providers (PSPs), addressable through the Faster Payments scheme, do not ensure that they pay the payee named in the payment. The payer names the payee in the underlying payment order – it is mandatory information, without which the payer's PSP will not accept the payment order for execution. It is transported through the Faster Payments system to the payee's PSP, but the payee's PSP does not check that the name in the payment is consistent with the name associated with the account as identified by the Sort Code and account number.

The Sort Code and account number are required in the payment order, and travel through to the payee's PSP. They constitute a 'Unique Identifier'. Under current UK case law, the 'Unique Identifier' is a sufficient basis for the payee's PSP to credit an account, without checking the name.

This is costing UK businesses and individuals hundreds of millions of pounds per annum, and efforts over an 7-year period by the 'payments industry' have delivered ineffective measures such as the Contingent Reimbursement Model and Confirmation of Payee. Under this latter process, PSPs do check the name against the Sort Code and account number associated with it, demonstrating that the name check is technically and operationally possible.

### **Solution**

The 2017 Payment Services Regulations need to be amended to make the payee name part of the payer's contract with the payer's PSP, and to specify that this is a provision that cannot be opted out of in a Framework Contract.

The Funds Transfer Regulation needs to be amended so as to withdraw the dispensation that a national payment in £pounds can be completed solely on the basis of a 'Unique Identifier'.

### **Outcome**

The payer's PSP will have a payment contract with the payer under which it must honour all of the payee name, Sort Code and account number. If it effects payment to an account with any element in this data out-of-line with the contract, the payer's PSP is guilty of defective execution of the payment contract and must provide full restitution to the payer.

There will be no get-out as is provided by Funds Transfer Regulation now, that permits processing only on the basis of the 'Unique Identifier', whether that be the Sort Code and account number for a national payment in £pounds, or IBAN (International Bank Account Number) for a cross-border payment or one in foreign currency.

### **Pushback**

There will be pushback from PSPs that they cannot be expected to check the details on the payee's account when it is not an account in their books but in the books of a different PSP.

The rejoinder to that is, firstly, that if it is possible in the case of Confirmation of Payee, it is possible for every payment. Secondly, the PSPs designed the Faster Payments scheme as it is today, so they are free to re-design it or invest in another scheme so as to address this issue.

If they decide amongst themselves that they do not want to invest in either a re-design or a new system, they can bear the losses from APPF, but it is not fair that the issue remain unresolved and that end users continue to suffer losses emanating from it.

### **Conclusion**

APPF may occur through the CHAPS scheme and through the BACS scheme, but the vast bulk occurs through the Faster Payments scheme. Concentrating on Faster Payments and implementing the proposed legal changes will eliminate for the end user a major portion of APPF, by simply making the payer's PSP legally liable to the payer for getting the basics right: for paying the payee that the payer named.

Achieving this degree of end user protection was the purpose of the 2017 Payment Services Regulations but there is a loophole. Plugging that loophole establishes the correct baseline of responsibilities and risks when end users have their payments made through a system designed by their PSPs.

*Summary*

We respectfully recommend that the PSR desist with further expansion of CoP and CRM, and instead implement the legal changes we have outlined. This will eliminate the detriments to Payment Service Users more completely and more quickly than any deployment of CoP and CRM.

Yours faithfully,



# Modulr



## PSR CP22/4 – Modulr response 9/12/22

Consultation question	Modulr response
<p>1. Do you have views on the impact of our proposals on consumers?</p>	<p>Modulr acknowledges and understands the PSR’s intent is to protect consumers from APP fraud, however the PSR’s mandatory reimbursement proposals for APP fraud (as set out in CP22/4) (the “<b>PSR Proposals</b>”) in our opinion fail to meet the overarching objective of reducing fraud and will result in a number of unintended negative consequences for consumers, such as:</p> <p><b>Exploitation of the mandatory reimbursement mechanism</b> – the PSR’s strategy includes the need to “<i>make it harder for criminals to defraud people using the payment systems we regulate.</i>”</p> <p>We strongly maintain that focusing on mandatory reimbursement of APP fraud, rather than: (i) driving change in consumer behaviour, (ii) data sharing in the context of fraud, (iii) collaborating across industries like telecoms and social media platforms, and (iv) investing in fraud prevention, is counterproductive as this approach runs the risk of the UK payments sector becoming more susceptible and exposed to targeted fraud at both an individual and organised level.</p> <p><b>Reduced consumer awareness</b> – Modulr maintains that the more appropriate way to mitigate the risk of fraud in payment transactions is understanding how best to protect consumers from falling victim to APP fraud. Significant effort has already been deployed in awareness and education campaigns on the risk of APP fraud, as well as the consequences of such fraud. Under the PSR Proposals there is a danger that consumers will act with less responsibility and awareness of the consequences of their actions.</p> <p>Modulr asserts that, in addition to educating consumers on APP fraud, consideration should also be given as to why existing fraud control mechanisms (such as Confirmation of Payee) and warnings associated with this are on occasions being ignored by consumers.</p> <p>We are not reassured by the PSR’s view expressed in Box 2 under paragraph 4.18. The anecdotal evidence from TSB relates to the voluntary scheme, not a situation where there is a high-profile mandatory requirement across all PSPs. We appreciate there is little other evidence, but this indicates a need for cautious policymaking and more carefully considered exemptions from mandatory reimbursement than are currently being proposed.</p> <p><b>Impact on law enforcement</b> - the PSR’s mandatory reimbursement regime may also result in law enforcement strategies and efforts being diverted away from APP fraud on the basis that most transactions which are subject to</p>

	<p>APP fraud are likely to be reimbursed. The impact here is that offenders will feel even less likely to be subject to enforcement action which will encourage them to commit fraud.</p> <p><b>Diminished efficiencies in payments transactions</b> – Under the PSR Proposals consumers will likely see an increase in delayed payment transactions where such transactions have high-risk characteristics. The competing principles of making payments available to all with limited friction, whilst introducing measures and controls to monitor fraud, may alienate some consumers from using faster payments. This will be especially prevalent for newly established businesses, foreign nationals, those on working visas and those who are vulnerable, where the risk factors may be too high for an institution to make or accept the payment. Financial institutions may also choose to de-risk across certain customer types.</p> <p>We also expect that some PSPs will reconsider their use of faster payments, whether to limit the maximum amount for faster payments transactions, or to cease offering it altogether.</p> <p><b>Reduced competition in the market</b> – A core objective of PSD2 is to encourage open banking and competition in the payments sector for the benefit of consumers.</p> <p>Introducing mandatory reimbursement is costly and operationally burdensome for many PSPs and may result in PSPs saving costs in other areas such as investment in fraud mitigation and prevention mechanisms. On the other hand, well-established financial institutions will have the means to implement these measures with more ease. This unbalanced operational impact and cost burden is counterintuitive to open banking principles and adds barriers to entry in an already highly regulated environment. We anticipate reduced competition and innovation, leading to fewer alternatives to the traditional bank model for payment service users.</p>
<p>2. Do you have views on the impact of our proposals on PSPs?</p>	<p>Modulr asserts that the PSR Proposals will not achieve the anticipated objectives and will result in several unintended consequences (as set out in our response to Question 1 above).</p> <p>It is our view that these requirements may result in funds being prioritised for compensation rather than in detection and prevention strategies, meaning that it would have the opposite effect to that desired.</p> <p>If mandatory reimbursement is to be implemented, then there must be a clear divide between the legal and financial obligations of the PSP and the accountability of the consumer.</p> <p>We are fully supportive of ongoing improvement to standards and data sharing, however, believe this would be best led from a legislative and scheme perspective to ensure industry alignment. A single and uniform approach is clearly the most effective way to build on existing activity, which for Modulr included implementing CoP (the first non-bank</p>

	<p>to do so) and our introduction of messaging in the payment flow. We have also supported UK Finance and FFE on messaging campaigns to educate consumers. Future work that we are committed to includes improving centralised data sharing, targeted education strategies, improvements in identification documents at source, and more detail in what the payment journey/warnings should look like. Again, we support industry standards here to drive uptake and consistent application.</p> <p>Re-imburement within 48 hours will be extremely challenging, and while more time to investigate is allowed, the criteria are not defined. As you are aware, UK Finance has proposed and HMT is considering amends to regulations 86 &amp; 89 of the PSRs to allow PSPs to further delay the processing of payment order, and the crediting of funds to payees' accounts by receiving PSPs, where there is suspicion of fraud. This extra time may be helpful in certain circumstances to reach the customer and explain the situation, so we are in support and have been inputting to this proposal via the Payments Association.</p>
<p>3. Do you have views on the scope we propose for our requirements on reimbursement?</p>	<p>We recognise that the scope for PSPs is consistent with other regulatory applications (e.g. the FCA's Consumer Duty) but our view is that it should not include micro-enterprises or charities. Micro-enterprises and charities are capable of bearing a higher level of responsibility than consumers for protecting themselves from APP scams. They should give training to their staff on the risks that arise from their role, turning this into an issue of corporate competence via fraud risk mitigation rather than mandatory reimbursement.</p> <p>It is also important to note that the majority of APP frauds are against individuals rather than organisations or businesses.</p>
<p>4. Do you have comments on our proposals:</p> <ul style="list-style-type: none"> <li>• that there should be a consumer caution exception to mandatory reimbursement</li> <li>• to use gross negligence as the consumer caution exception</li> <li>• not to provide additional guidance on gross negligence?</li> </ul>	<p>We are of the opinion that there should not be blanket mandatory reimbursement for all APP fraud.</p> <p>We object to the gross negligence as exception (and expand on our rationale for this position under Questions 5 and 6).</p> <p>The exceptions case of gross negligence would require clear and objective guiding principles from the PSR, without which we foresee inconsistency in approach between PSPs.</p> <p>We assert that consumer education relating to accountability and responsibilities in respect of APP fraud is also essential, otherwise there will be a disparate understanding for the consumer in comparison with the PSP and this will be one of the most effective strategies to reduce fraud activity.</p>
<p>5. Do you have comments on our proposal to</p>	<p>This provision creates a risk of gaming the system using first party fraud, given the difficulty of identifying those who could falsely claim to be in vulnerable circumstances. Without clear evidence, firms will rightly and understandably be</p>

<p>require reimbursement of vulnerable consumers even if they acted with gross negligence?</p>	<p>reluctant to challenge these customers, meaning that bad actors could use this to open up opportunities that could be exploited at scale.</p> <p>Firms would need much more rigorous controls and monitoring, as previously there was little incentive for customers to falsely identify themselves as being vulnerable. This also may result in some firms considering the costs of offering services to certain customer types who would be deemed higher risk.</p>
<p>6. Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?</p>	<p>As per Chapter 4.27 of the PSR Proposal, the FCA defines a vulnerable consumer as <i>“someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care”</i>.</p> <p>Chapter 4.28 of the PSR Proposal goes on to stipulate that <i>“use of the FCA’s definition is preferred by the PSR so that, in relation to regulatory requirements, firms are working to a single definition of vulnerability.”</i></p> <p>We are of the view that the CRM code definition of a <i>“vulnerable customer”</i> (as set out at Chapter 4.27 of the PSR Proposal) is more appropriate definition as it requires the consumer to implement a reasonable level of care, whilst allowing the nature of their vulnerability to be taken into account in establishing what is reasonable. The benefits of this definition are that it requires the PSP to consider consumer vulnerability, whilst also retaining consumer responsibility and accountability.</p> <p>By way of example, the FCA’s most recent assessment of the proportion of UK adults with characteristics of vulnerability was 53%, in October 2020. We recognise that the figure for FPS users may differ, but as a guide, we do not consider it reasonable that this proportion of customers should be required to take no responsibility for APP fraud.</p>
<p>7. Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement</li> <li>• any ‘excess’ should be set at no more than £35</li> <li>• PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?</li> </ul>	<p>Whilst we acknowledge the principles and recommendations on a fixed excess to mandatory reimbursement, we assert that these points will not significantly reduce the detrimental effect on tackling the issue of APP fraud and will run the risk of:</p> <ol style="list-style-type: none"> <li>1. Increasing the financial and operational burden on sending and receiving PSPs in implementing the mandatory reimbursement regime; and</li> <li>2. Adding complexity to consumer messaging, potentially causing complaints when they expect the full value to be refunded.</li> </ol>

<p>8. Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to set a minimum claim threshold</li> <li>• any threshold should be set at no more than £100</li> <li>• PSPs should be able to exempt vulnerable consumers from any threshold they set?</li> </ul>	<p>See our response to Question 7.</p>
<p>9. Do you have comments on our proposal not to have a maximum threshold?</p>	<p>We assert that a maximum cap should be implemented in the context of mandatory reimbursement. In uncapped mandatory reimbursement were to be implemented, this would run the risk of:</p> <ol style="list-style-type: none"> <li>1. Disincentivising consumers to be accountable for their payments</li> <li>2. Incentivise fraudulent activity</li> <li>3. Incentivise PSPs to budget for mandatory reimbursement rather than investing in fraud prevention tools.</li> </ol>
<p>10. Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement</li> <li>• any time-limit should be set at no less than 13 months?</li> </ul>	<p>No comments.</p>
<p>11. Do you have comments on our proposals that:</p> <ul style="list-style-type: none"> <li>• the sending PSP is responsible for reimbursing the consumer</li> <li>• reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?</li> </ul>	<p>The mandatory reimbursement implementation timeline of 48 hours would be extremely difficult to implement, particularly if there is evidence or suspicion of fraud or negligence. Further guidance from the PSR will be required to on the exception “<i>unless the PSP can evidence suspicions of first party negligence or fraud</i>”. This exception is subjective and risks disparity in its application amongst PSPs. We query what would constitute “<i>evidence of suspicion</i>” and will this differ depending on the nature of the transaction?</p> <p>This added pressure to review and conclude will also be viewed as something fraudsters will look to take advantage of and result in an increase of fraudulent attacks in our opinion.</p>

<p>12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?</p>	<ul style="list-style-type: none"> <li>• Customer ignores warnings during the payment journey, including <ul style="list-style-type: none"> <li>○ standard warnings</li> <li>○ CoP mismatches</li> <li>○ targeted warning triggered by payment purpose</li> </ul> </li> <li>• Customer, when questioned <ul style="list-style-type: none"> <li>○ gives inaccurate answers designed to circumvent controls, e.g. advising they are happy with the payment</li> <li>○ gives incorrect responses to any questions</li> </ul> </li> </ul> <p>Investigations are likely to require multiple institutions therefore we would recommend 30 days.</p>
<p>13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?</p>	<p>We assert that this is not an optimal means to tackle APP fraud. However, if such mandatory reimbursement is implemented, we agree that a 50:50 allocation would allow for reduced operational complexity and avoid the need to agree to the allocation of the reimbursement between the sending and receiving PSP.</p>
<p>14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?</p>	<p>As per Q13, we maintain that a 50:50 apportionment of reimbursement should apply. Deviation from this position would introduce operational complexity which would be labour and cost intensive for both the sending and receiving PSP. This also runs the risk of prolonging the time frame in which the consumer will be compensated. With this proposal, there is a high likelihood that the body overseeing mediation will become bogged down in lengthy disputes.</p> <p>We are unclear from the proposed criteria whether a particular PSP could apply a blanket approach on reimbursement (offering less than 50%) to a certain PSPs or groups of PSPs, reflecting their customer profile. Again, we see the prospect of negotiation and disputes becoming extremely involved.</p>
<p>15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?</p>	<p>We are of the opinion that in these instances the sending PSP (to the final (fraudulent) account destination) should be responsible.</p>
<p>16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds</p>	<p>Please see response to Question 14.</p>

between sending and receiving PSPs?	
17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?	Subject to our general objection to mandatory reimbursement, we agree that the rules on allocating the costs of reimbursement should apply to all direct and indirect PSP participants.
18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?	We are supportive of rules being set for all the relevant interested parties to adhere to (e.g. PSO, PSPs and consumers), subject to formation of such rules being a consultative process whereby consideration can be given to the practical and operational implications of these rules in the context of differing PSPs and their respective business models.
19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?	We do not agree with the principle that Faster Payment Scheme rules cannot be applied to those indirectly using the scheme. All rules should be applicable to anyone accessing the Faster Payments Scheme.
20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?	No comments.
21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?	This must be done in consultation with all key members and operators in the sector and ensure an understanding of the impacts to different business models.
22. Do you have comments on our preferred short-term implementation	We are supportive of a compliance monitoring regime which sets out clear prescriptive guidelines on fraud detection and prevention.

approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?	
23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?	This must be considered against the different business models and capacities to ensure that timelines are realistic and do not put increased operational pressure on a business.
24. Do you have views on the best option for short-term enforcement arrangements?	As we are against the mandatory reimbursement model, we are unable to support short term enforcement arrangements for those that are meeting the scheme rules for reimbursement.
25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?	This would be the responsibility of the direct participant providing access to the scheme.
26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?	All direct and indirect members should be required to follow the rules of the scheme
27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?	We disagree with the position that the benefits of mandatory reimbursement outweigh the costs incurred. Instead of budgeting investment in respect of fraud mitigation and prevent, PSPs will be required to allocate a budget in respect of the mandatory reimbursement and fraud prevention. We assert that requiring two separate budgets is unlikely bolster PSPs ability to tackle fraud. This higher cost burden will also reduce competition in the payments market.
28. Do you have any other comments on the proposals in this consultation?	A very large number of consumer payments will be impacted by the proposals in this consultation and we feel that the views of all participants have not been adequately considered and reflected in the PSR proposals. We are also concerned that there is insufficient evidence and data to support the changes. We would like to urge great caution given what we anticipate the unintended consequences to be, as expressed in our answer to Question 1.



# Money Advice Trust

**MONEY**  
ADVICE TRUST



Consultation Response:

# PSR Authorised push payment scams: Requiring reimbursement

Response by the Money Advice Trust

Date: November 2022

# Contents

- **Page 2** Contents
- **Page 3** Introduction / about the Money Advice Trust
- **Page 4** Executive summary/ Introductory comment
- **Page 5** Responses to individual questions
- **Page 13** Contact details

# Introduction

## About the Money Advice Trust

The Money Advice Trust is a charity founded in 1991 to help people across the UK tackle their debts and manage their money with confidence.

The Trust's main activities are giving advice, supporting advisers and improving the UK's money and debt environment.

In 2021, our National Debtline and Business Debtline advisers provided help to over 170,400 people by phone, webchat and our digital advice tool with 1.63 million visits to our advice websites. In addition to these frontline services, our Wiseradviser service provides training to free-to-client advice organisations across the UK and in 2021 we delivered this free training to more than 1,000 organisations.

We use the intelligence and insight gained from these activities to improve the UK's money and debt environment by contributing to policy developments and public debate around these issues.

Find out more at [www.moneyadvicetrust.org](http://www.moneyadvicetrust.org).

## Public disclosure

Please note that we consent to public disclosure of this response.

# Introductory comment

We very much welcome the proposals in the paper from a consumer protection perspective. APP scams can have a devastating effect on victims, including ongoing mental health issues and emotional and financial distress. It is vital that the industry moves away from the attitude that consumers are generally responsible for having been defrauded, in a world where ever more sophisticated scams are developed to deceive people into making such payments.

- ✓ We welcome the proposal to require all payment service providers (PSPs) to reimburse victims compared to the ten firms required to do so under the CRM code.
- ✓ We very much welcome the expectation that all consumers will be reimbursed on a mandatory basis, unless they fall into a very small group of consumers where fraud or gross negligence can be proved.
- ✓ We are very pleased to see the proposal that consumers will be reimbursed in full rather than the current situation where many consumers receive only a partial payment under the CRM code.

We hope that as a result of these proposals, PSPs will be incentivised to prevent APP scams occurring in the first place. We would hope to see improved intelligence-sharing and a commitment to blocking suspicious payments more frequently.

We would like to see extensive and rigorous rules and guidance in place to set out to define gross negligence and how this “high bar” can be reached to minimise the potential risk of firms deciding more consumers fall into this bracket to avoid paying compensation.

It is vital that the PSR ensures that the body chosen to enact the regulatory role is adequately equipped with strong consumer protection measures. We would very much hope that the minimum initial set of rules under the scheme will include arrangements to monitor and enforce the rules on mandatory reimbursement from the start. We consider such monitoring and enforcement to be essential to the success of the scheme.

# Responses to individual questions

## Question 1: Do you have views on the impact of our proposals on consumers?

We very much welcome the proposals in the paper from a consumer protection perspective. Scams have an immense impact on people who are affected, including ongoing mental health issues and emotional and financial distress. We would expect the impact of the PSR proposals to be very positive for most consumers affected by the authorised push payment (APP) scams.

The proposals will be beneficial in a number of ways.

- ✓ We welcome the proposal to require all payment service providers (PSPs) to reimburse victims compared to the ten firms required to do so under the CRM code.
- ✓ We very much welcome the expectation that all consumers will be reimbursed on a mandatory basis, unless they fall into a very small group of consumers where fraud or gross negligence can be proved.
- ✓ We are very pleased to see the proposal that consumers will be reimbursed in full rather than the current situation where many consumers receive only a partial payment under the CRM code.

Whilst the proposals may mean greater “friction” for consumers when genuine payments are put on hold or blocked temporarily, we would have thought this a small price to pay for greater consumer protections. We do not expect the majority of consumers to find this level of protection unnecessarily intrusive. As suggested in the paper, with sufficient incentives on PSPs to improve data sharing, this should minimise the number of payments stopped unnecessarily.

## Question 2: Do you have views on the impact of our proposals on PSPs?

We share the expectation put forward in the paper by the PSR that as a result of these proposals, PSPs will be incentivised to prevent APP scams occurring in the first place. We would hope to see improved intelligence-sharing and a commitment to blocking suspicious payments more frequently.

We cannot comment upon whether the proposals will increase the costs for most PSPs for scam reimbursement. However, it would appear reasonable that if costs do increase, this can be minimised by PSPs doing substantially more to prevent scams happening in the first place.

Page 394

We see no reason to allow badly performing PSPs who have high scam rates to continue to take minimal action to prevent fraud at the expense of consumers, or in comparison to PSPs who are choosing to “do the right thing”.

### Question 3: Do you have views on the scope we propose for our requirements on reimbursement?

We would like to see the scope for the scheme to be as wide as possible. We would be concerned that any exemptions could lead to loopholes that could be exploited by scammers. For example, the £100 limit could concentrate scam activity to amounts below that limit.

The PSR and FCA should prepare new rules in advance, so that PSPs are not able to refuse to compensate consumers where the scam relates to an “on-us” APP scam payment.

In point 4.13 of the paper, there is a suggestion that mandatory reimbursement will not apply to private civil disputes. We would like to see this clarified to ensure that this exemption does not apply where scammers pretend to be a legitimate supplier of goods and no goods are ever received.

### Question 4: Do you have comments on our proposals:

- that there should be a consumer caution exception to mandatory reimbursement
- to use gross negligence as the consumer caution exception
- not to provide additional guidance on gross negligence?

We agree with the PSR under point 4.19 that a “*consumer caution exception could put inappropriate responsibility on consumers to spot sophisticated scams, risk PSPs blaming genuine victims for not taking sufficient care and limit the incentives on PSPs to take steps to detect and prevent fraud*”. We are therefore not entirely sure that there is a requirement for a consumer caution exemption due to gross negligence.

We are concerned that even though this is intended to be a “high bar”, some firms already try to argue that consumers have been grossly negligent to avoid paying compensation for scams. We think there will be an increase in cases where firms use gross negligence arguments in the future.

We do not agree with the conclusion reached in the paper that there is no need for the PSR to provide guidance on the application of gross negligence to APP scams. We would like to see extensive and rigorous rules and guidance in place to set out to define gross negligence and how this “high bar” can be reached to minimise the potential risk of firms deciding more consumers fall into this bracket to avoid paying compensation.

Such guidance would need to be easy to amend, and frequently reviewed to ensure future developments in fraud are reflected. If the decision is taken not to provide high-level guidance at this point, we feel this should be reviewed at a very early stage post-implementation, taking into account any rise in gross negligence cases, to ensure that this is the right decision.

### Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?

We welcome the proposal to allow an exception to the gross negligence rules to require reimbursement of vulnerable customers in all cases. However, we are still of the opinion that there should be a gross negligence definition, at least to clarify what would NOT constitute gross negligence.

It will be vital that there is a wide definition given to vulnerability in such cases to avoid firms trying to restrict the number of occasions when they have to reimburse consumers.

### Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?

We welcome the proposal to use the FCA's definition of vulnerability. This makes sense as firms should already be using the FCA's definition when complying with FCA rules. We would also expect firms who are authorised by the FCA to reflect on their obligations under the forthcoming FCA consumer duty in addition to the vulnerability guidance.

### Question 7: Do you have comments on our proposals that:

- sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- any 'excess' should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

We do not support these proposals as they stand. We are concerned that minimum claim thresholds and minimum compensation levels will deter more vulnerable consumers from making a complaint in the first place.

In addition, we do not see how PSPs could exempt vulnerable consumers from any excess amount that they apply. It is difficult to see how this would work in practice. It is more likely that the excess would be applied across the board and anyone vulnerable would not even know that they could have been exempt from this. People in vulnerable circumstances are less likely to be in a position to raise their concerns or make a complaint.



We also worry that this proposal would apply to each payment made by a consumer. If someone was making a series of payments for what they thought was a legitimate purpose, would the effect of the excess mean that £35 of each payment would be lost? This could amount to a substantial amount for someone on a limited income.

#### Question 8: Do you have comments on our proposals that:

- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?

We are not comfortable with supporting this threshold. We are concerned that minimum claim thresholds and minimum compensation levels will deter more vulnerable consumers from making a complaint in the first place.

We note that the proposed £100 threshold matches the minimum purchase amount under section 75 of the Consumer Credit Act (CCA). It would therefore constitute an equivalent level of protection. However, this does reduce the potential compensation for smaller scams significantly. People who are on low incomes and in vulnerable circumstances are not in a position to lose even small amounts of money. We worry that a scam where someone is misled/coerced into transferring their own money is not the same as a willing purchase using a credit card under the CCA.

We are concerned that scammers will turn their attention to high volume smaller fraudulent activity that would disproportionately impact upon the people who are most vulnerable and on the lowest incomes. This group has the most to lose. An equivalent scenario would be the rising levels of online broker fraud scams, where people desperate for a small loan, are paying broker fees for a loan that never materialises.

Once again, we do not see how PSPs will be able to exempt vulnerable consumers from any threshold set. It is difficult to see how this would work in practice. It is more likely that the threshold will be applied across the board and anyone vulnerable would not even know that they could have been exempt from this.

We welcome the proposal that this minimum threshold be reviewed in the post implementation review with a view to reducing or eliminating the threshold.

#### Question 9: Do you have comments on our proposal not to have a maximum threshold?

We agree there should not be a maximum threshold for compensation payments put in place, as it is entirely reasonable to expect PSPs to have strong safeguards for large payments already.

Question 10: Do you have comments on our proposals that:

- sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
- any time-limit should be set at no less than 13 months?

We are not entirely sure why the time limit needs to be set at 13 months if the time limit for consumers to complain to the Financial Ombudsman Service is up to six years. We recognise that FOS will be able to exercise discretion, but this relies upon the eloquence of the person complaining to explain why their case is exceptional. This may not be possible for people subjected to extended and complex scams where they can become traumatised as a result.

We would like to see a longer time limit on claims as it is entirely possible that people in vulnerable circumstances may not be aware of having been a victim of a scam within that timescale. In addition, people may move in and out of vulnerable circumstances, and for example suffer a period of mental ill health that puts them outside the time limit for a claim. We think there should at least be an exemption put in place in the rules to cover exceptional cases.

Question 11. Do you have comments on our proposals that:

- the sending PSP is responsible for reimbursing the consumer
- reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?

These proposals appear to make sense and to be entirely reasonable. We would have thought the vast majority of scams are sufficiently routine to allow for reimbursement within this timescale. An extended timescale runs the risk of PSPs using the extra time to just delay the inevitable outcome, causing extra stress for the consumers concerned.

We believe therefore, that the timescale should not be extended further, except in cases that meet a very high hurdle of evidence and cause for gross negligence or first party fraud.

Question 12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?

It is difficult to comment on the standard of evidence for gross negligence or fraud that would be acceptable to meet the threshold in these cases. It is vital for the success of the scheme that PSPs do not set the bar too low so that too many cases are sent for further assessment. There should therefore be a high standard of evidence required to prevent this from happening and to prevent individual firms making inconsistent decisions.

We would suggest that the scheme rules should set out some standards initially, which can be reviewed if not sufficiently robust or effective in preventing misbehaviour by any PSPs. At the very least, guidance should make it very clear to PSPs and to consumers what should not be treated as gross negligence so that there is less incentive for firms to drag out paying compensation in cases where there is no potential for a gross negligence finding. This should help to minimise the inconsistency in approach between different firms operating under the current code. This inconsistency demonstrates that firms need mandatory rules that are applied across all cases and firms should not be using their own rules and variable quality of discretionary decisions in fraud cases.

We welcome the requirement on the PSP to notify Pay.UK in cases where they believe there is a need for more time to investigate a case. This will allow Pay.UK to monitor firms to ensure that firms do not exceed the envisaged “small minority of cases” that are reasonable to be investigated.

### Question 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

It would appear entirely reasonable for the default allocation of reimbursement costs to be split between the sending and receiving PSPs equally. We accept the point that this incentivises both parties to quickly increase protection for consumers against this type of scams.

### Question 14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?

We do not have any views on these proposals as long as there is no resulting harm for consumers if PSPs depart from the default allocation as described.

### Question 15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?

We do not have any views on how these rules could work for multi-generational scams, as we are not part of the payments industry.

### Question 16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?

We would support this proposal from a consumer perspective. We note that there will be a greater incentive on the receiving PSP to act to recover funds due to the 50:50 default allocation rules. This would appear to be a beneficial step forward in making sure firms put in place robust scam prevention measures. This measure should help to tackle an unacceptable level of inaction by some PSPs currently.

### Question 17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?

The proposals on the scope for rules on allocation seem sensible. The scope should be as wide as possible to ensure all PSPs have incentives to detect and prevent APP scams.

### Question 18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?

We are mainly concerned with consumer protection, so it is vital that the PSR ensures that the body chosen to enact this role is adequately equipped with strong consumer protection measures. This means that as well as rule-setting provisions, Pay.UK must be able to monitor and enforce compliance with the rules, and be given strong sanction powers against PSPs who do not follow the rules. It appears that this is not currently the case.

### Question 19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?

We would very much hope that the minimum initial set of rules under the scheme will include arrangements to monitor and enforce the rules on mandatory reimbursement from the start. We consider such monitoring and enforcement to be essential to the success of the scheme.

The lack of monitoring and enforcement would directly impact upon consumers in our view. If these elements are missing, then there is no way of measuring the scheme outcomes or put right any problems with individual PSPs.

### Question 20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?

We are unable to comment on this question.

### Question 21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?

We believe this is best agreed between the PSR and Pay.UK using the CRM code standards as a basis. We can only urge the parties to ensure that the rules and criteria are developed as soon as practicable to ensure that consumers are protected from the start of the scheme.

**Question 22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

We do not have any suggestions on these proposals beyond reiterating that whatever monitoring regime is put in place is effective from the outset of the scheme.

**Question 23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We do not have any further comments on these proposals.

**Question 24. Do you have views on the best option for short-term enforcement arrangements?**

We do not have any suggestions on these proposals beyond reiterating that whatever enforcement regime is put in place must be effective from the outset of the scheme.

We do not want to see an enforcement regime that has fewer enforcement powers being put in place as this will undermine the scheme. If it is more effective and faster for the PSR to take on the enforcement role rather than Pay.UK, then we do not see why this could not be put in place, at least for the start of the scheme.

**Question 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

We are not close enough to the current rules and practices within industry to comment on the best way to apply the rules on reimbursement to indirect participants.

**Question 26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

Again, we are not close enough to the sector to comment.

**Question 27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

We do not have any comments on the cost benefit analysis.

**Question 28. Do you have any other comments on the proposals in this consultation?**

We welcome the proposals for a post-implementation review by the PSR to assess the success of the initial scheme.

For more information on our response, please contact:

██████████, Policy Lead

██

██████████





### The Money Advice Trust

21 Garlick Hill

London EC4V 2AU

Tel: 020 7489 7796

Fax: 020 7489 7704

Email: [info@moneyadvicetrust.org](mailto:info@moneyadvicetrust.org)

[www.moneyadvicetrust.org](http://www.moneyadvicetrust.org)

# Money Saving Expert



# MoneySavingExpert

## Response to Payment Systems Regulator Consultation

### *APP scams: Requiring reimbursement*

MoneySavingExpert (MSE) welcomes the opportunity to respond to this PSR Consultation on requiring reimbursement for Authorised push payment (APP) scams.

We will be focusing our response on questions outlined in Part A, “The reimbursement requirements we propose” section of the consultation.

#### **Question 1: Do you have views on the impact of our proposals on consumers?**

**MSE welcomes the PSR’s direction of travel on tackling APP scams and is in support of mandatory reimbursement for victims.**

While the voluntary Contingent Reimbursement Model (CRM) code has gone some way to providing protections for consumers who fall victim to APP scams, it is MSE’s view that mandatory reimbursement should lead to stronger, more consistent protection across the industry and a reduction in consumer harm. Coupled with the PSR’s recently announced intentions to broaden the rollout of Confirmation of Payee (CoP), we are pleased to see the regulator taking further positive steps to tackle APP scams.

Prevention is ultimately better than cure and so MSE warmly welcomes planned work to improve intelligence sharing to spot fraudulent transactions and stop them from happening in the first place. Moreover, MSE hopes that the proposal to assign responsibility for allowing fraudulent payments to both the sending and receiving payment service providers (PSPs) would incentivise better industry processes and increase prevention. In cases where APP fraudsters still manage to get through, mandatory reimbursement would provide an extra safety net in efforts to protect consumers’ money and wellbeing.

If mandatory reimbursement of APP scams is rolled out, the PSR and other relevant bodies must ensure they have strong oversight to ensure its success. Moreover, robust monitoring capabilities must also be in place across the industry to mitigate the potential unintended consequence of fraudsters migrating to other forms of criminal activity in reaction to strengthened protections in the APP space.

More broadly, MSE believes cross-sector collaboration is needed to tackle the full life cycle of scams. APP scams and other forms of fraud are not exclusive to the banking or wider financial services sector, as while payments are taken in this space, they are also being enabled by other industries. Continued stakeholder engagement and work is therefore needed to address the role of other organisations outside of the financial services industry in facilitating this crime, such as social media platforms and telecommunications firms, alongside plans to require the reimbursement of APP scams. MSE would welcome work to share intelligence across platforms and industries with the aim of preventing consumers losing money to this type of crime.

**Question 4: Do you have comments on our proposals: • that there should be a consumer caution exception to mandatory reimbursement • to use gross negligence as the consumer caution exception • not to provide additional guidance on gross negligence?**

MSE supports the proposal to use gross negligence as the consumer caution exception to mandatory reimbursement. As the PSR rightly points out, fraudsters are increasingly creative and sophisticated. They use constantly evolving tactics, including social engineering, to achieve their criminal aims and their victims are diverse. Scams can happen to everyone, including – but by no means limited to – those in vulnerable situations. For example, we have seen and had conversations with people of varying ages and genders, across all income and educational backgrounds, who have become victims of scams. MSE believes the use of a gross negligence exception will set a higher bar and therefore drive better outcomes for consumers than the voluntary CRM code currently does, providing improved rights for all of those taken in by scammers’ tactics.

Moving to a higher standard of caution than enabled through the CRM code should also hopefully incentivise PSPs to improve their fraud detection and prevention processes and share intelligence with others, hopefully leading to a reduction in APP scams occurring in the first place.

MSE does not anticipate that the gross negligence exception would lead to a significant reduction in customer caution. Consumers will often take great care and act prudently to avoid scams, but still fall victim to fraudsters’ tactics. We haven’t come across any evidence to support the argument that a gross negligence exception would lead to moral hazard around consumer behaviour.

Moreover, TSB told both the PSR and the Lords Fraud Committee that it has not seen evidence of customers taking less care since the introduction of its own fraud refund guarantee, which sets a higher bar for reimbursement than the CRM code.<sup>1</sup> As the industry initiative which is most directly comparable with the mandatory reimbursement proposals laid out by the PSR, MSE believes this assertion provides further re-assurance.

**Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

MSE supports the PSR’s proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence. As the regulator rightly highlights, this cohort of consumers may be more at risk of being taken in by the social engineering tactics commonly perpetrated by fraudsters, and less able to exercise caution and protect themselves from APP scams than their counterparts. Moreover, the existing CRM code already exempts consumers who are vulnerable to APP scams from its exceptions to reimbursement including that of gross negligence.

It therefore seems logical that this group of customers be reimbursed under all circumstances as outlined in the PSR’s proposals, as this action should place greater incentives on PSPs to improve their monitoring and safeguarding processes for vulnerable customers and stop people falling victim to APP scams.

---

<sup>1</sup> PSR Consultation Paper, “Requiring Reimbursement for Authorised push payment (APP) scams,” November 2022, p.26. <https://www.psr.org.uk/media/kzIncenx/psr-cp22-4-app-scams-reimbursement-september-2022-v6.pdf>; House of Lords Fraud Act 2006 and Digital Fraud Committee, “Report of Session 2022–23, Fighting Fraud: Breaking the Chain,” November 2022, p.116. <https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf> (Links last accessed 30 November 2022).

**Question 8: Do you have comments on our proposals that: • sending PSPs should be allowed to set a minimum claim threshold • any threshold should be set at no more than £100 • PSPs should be able to exempt vulnerable consumers from any threshold they set?**

MSE has some concerns that a minimum claim threshold of up to £100 could lead to the possibility of APP fraudsters migrating to different tactics and adopting a “little and often” approach to target their victims through smaller payments. Where there are gaps in consumer protections, there is always a risk that the problem could move to those areas where safeguards are the weakest. The PSR needs to be taking steps to ensure fraudsters don’t transition to other tactics as rules become tighter elsewhere in the APP space, and avoid scammers taking advantage of a minimum threshold if it’s adopted.

Moreover, what constitutes a significant amount of money vastly differs depending on consumers’ personal circumstances. For someone with low financial resilience, for example, losing an amount of money up to £100 through an APP scam and having no recourse to reimbursement could cause notable financial and emotional detriment. There is a risk that people who can least afford to lose money could end up even more targeted by fraudsters if their tactics change, as these consumers may be more likely to make smaller payments below the proposed minimum threshold. It seems fairer for consumers for there to be no minimum threshold in place, but if the PSR was to go ahead with this plan, MSE supports the exemption for vulnerable customers, to avoid the decision to disregard smaller claims disproportionately impacting the most vulnerable.

There is also a possibility that setting the minimum threshold at a level up to £100 could lead to under-reporting of APP scams under this amount. If the PSR does follow through with this proposal, strong and sufficient industry monitoring and reporting requirements need to be in place to counter the risk of inconsistency in the reporting of smaller scams.

**Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

MSE broadly welcomes the 50:50 default allocation of reimbursement costs between sending and receiving PSPs. There is currently very limited liability on receiving PSPs, who contribute less than 5% on average to APP scam reimbursement costs, despite fraud being perpetrated on their systems.<sup>2</sup> The PSR’s proposal for shared liability between sending and receiving PSPs should help to prompt better outcomes for consumers through placing stronger incentives on the latter group to make faster progress to get ahead of APP scams before they occur. Alongside improved intelligence sharing and near market-wide adoption of CoP, this should lead to better detection and prevention.

---

<sup>2</sup> PSR Consultation Paper, “Requiring Reimbursement for Authorised push payment (APP) scams,” November 2022, p.33. (Data supplied by UK Finance for January to June 2021).  
<https://www.psr.org.uk/media/kzIncenx/psr-cp22-4-app-scams-reimbursement-september-2022-v6.pdf>  
(Link last accessed 30 November 2022).

## About MoneySavingExpert.com

[MoneySavingExpert.com](http://MoneySavingExpert.com) is dedicated to cutting consumers' bills and fighting their corner. The free-to-use consumer finance help resource aims to show people how to save money on anything and everything, and campaigns for financial justice. It was set up in 2003 for just £100, and its free-to-use, ethical stance quickly made it the UK's biggest independent money website, according to internet ranking site Alexa.com, and the number one 'Business and Finance – Business Information' site, according to Hitwise.

It has more than 8.4 million people opted-in to receive the weekly MSE's Money Tips email, and more than 12.4 million unique monthly site users who visit more than 21.8 million times a month. This includes the MSE Forum, which has more than two million registered users. In September 2012, it joined the [MoneySupermarket.com](http://MoneySupermarket.com) Group PLC.

In the event of any queries, please contact the campaigns team:

[campaigns@moneysavingexpert.com](mailto:campaigns@moneysavingexpert.com)

# National Trading Standards

Authorised push payment (APP) scams: Requiring reimbursement  
National Trading Standards Scams Team response  
December 2022

The National Trading Standards (NTS) Scams team welcomes the opportunity to respond to this consultation on Authorised Push Payment (APP) Scams. This response is based on the team's experience working with victims, financial institutions, consumer groups, and law enforcement.

We strongly support the PSR's proposals on mandatory reimbursement of victims of APP scams and believe that they will lead to better outcomes for victims of scams.

As stated in previous consultation responses, the current system has led to inconsistent and frequently poor outcomes for victims, where PSPs' investigations of the circumstances around the scam can increase the victim's sense of shame and feeling that they are to blame for being the victim of a crime.

Mandatory reimbursement with an exception for gross negligence and first party fraud should lead to far more victims being reimbursed and spare victims a distressing investigation process.

While we believe that the proposals are a significant step forward in protection for scam victims, we have some concerns about the details. We are concerned that limiting the scope of the scheme to Faster Payments could leave some victims who are currently covered by voluntary reimbursement rules under the CRM Code unprotected, while payments to foreign bank accounts and cryptocurrency exchanges, which trading standards officers have reported are increasingly common in scams, remain out of scope. The minimum claim threshold could have unintended consequences, including leaving chronic victims unprotected. Victims of some types of scams, such as investment scams, may also be left out due to the short time limit on claims. Our concerns are set out in more detail below.

Fraud is now the most commonly experienced crime in the UK, making up over 40% of all crime. People are becoming victims every day. Not only do they lose money but often experience serious non-financial consequences. The new rules on mandatory reimbursement should be implemented as soon as possible.

Please note that in this response the terms scam and fraud are used interchangeably. The NTS Scams team believes that the division between fraud and scams based on whether or not a payment is authorised or unauthorised is an artificial one that is incomprehensible to victims. Further we believe that distinguishing between fraud and scams has allowed "scams" to be viewed as less serious, downplaying the impact on victims and resulting in weaker public and private action to prevent and tackle them. Our policy is that **Scams are Fraud and Fraud is a Crime**.

For further information on any of the issues raised in this response, please contact [REDACTED]  
[REDACTED]

## **1. Do you have views on the impact of our proposals on consumers?**

Victims of scams suffer devastating consequences, not only significant financial losses but also negative impacts on their mental and sometimes physical health. Getting their money back is an important step in recovering from the impact of the crime. The current voluntary reimbursement system means that some victims are left unprotected, while others are suffering from inconsistent and sometimes arbitrary decision making by PSPs. The in-depth investigations into victim behaviour that are required under the CRM Code reinforces victim blaming and can increase the shame and embarrassment that many victims feel.

The lack of transparency over reimbursement rates under the Contingent Reimbursement Model (CRM) Code compounds the problem, although it is clear that not enough victims are being reimbursed. The high proportion of PSP decisions that are overturned by the Financial Ombudsman Service indicates that decisions are not being made fairly, but not all victims have the knowledge or capacity to take their cases to the Ombudsman. These victims are not getting the reimbursement they are entitled to under the CRM Code and are being let down by the system.

The PSR's proposals should ensure that many more victims get their money back, helping them start the process of recovering from the crime. The proposals will also create more clarity around the circumstances in which victims will be reimbursed, which will encourage more people to report financial losses to scams and reduce victim blaming. Messaging from consumer groups, PSPs, and government will be clearer and less confusing for victims. Consumers will also be able to have greater confidence in making payments by APP as they know there are protections in place where, through no fault of their own, they become the victim of a scam.

## **2. Do you have views on the impact of our proposals on PSPs?**

Although the proposals will result in higher costs to PSPs in reimbursing victims of fraud, we believe that PSPs are well placed to prevent fraud and that the proposed system will provide the right incentives on both sending and receiving banks to do more to prevent fraud. The current voluntary system is not working for victims and has not created strong enough incentives for PSPs to invest in prevention.

We understand that the proposals may result in PSPs slowing down payments, particularly those they perceive as higher risk. We believe that the majority of consumers will welcome the extra care taken by the PSP to look after their money. Anecdotal evidence from the Banking Protocol indicates that most people whose payments have been stopped by the bank because they believed there was a risk of fraud were happy that their PSP was taking action to protect them, even where the transaction was legitimate. We would also like to see PSPs empowering their customers by giving them more choice about the speed of their payments, including allowing customers to choose to have some payments automatically delayed for a short period to give them time to cancel the payment if they change their mind. This could help to combat some of the psychological tricks used by criminals to commit fraud, which make the victim panic and make decisions while in a "hot state".

We believe that the proposals could also incentivise PSPs to do more to identify customers who may be vulnerable because of their circumstances and tailor support to them. Enabling customers to declare their needs and giving them choices about how to manage their accounts and payments would be a good first step.

## **3. Do you have views on the scope we propose for our requirements on reimbursement?**

While we understand that the PSR is only able to regulate Faster Payments, we are disappointed that the mandatory reimbursement proposals cover fewer payments than the voluntary CRM Code. More importantly, we believe that excluding “on us” payments and CHAPS payments will be confusing to consumers.

From a consumer point of view, there is no difference to how they make Faster Payments and “on-us” payments and there is no choice available. Few consumers will notice that they are paying into a bank account in the same bank, and very few are likely to realise that this will have an impact on the protections available to them. We recognise that the PSR have set an expectation that the same rules should apply to on-us payments, but urge the PSR and FCA to urgently implement rules to ensure that consumers are not left unprotected.

While the volume of APP scams using CHAPS payments is low, these are usually payments of high value, which have a high impact on victims. Conveyancing fraud payments are often made via CHAPS and see some of the highest losses to APP scams. We would like to see the PSR work with the Bank of England to ensure that CHAPS payments are covered by similar rules as soon as possible.

The NTS Scams Team would also like to see government and regulators considering how to protect consumers making payments outside the current scope of the CRM Code. There is no protection for consumers who make payments to foreign bank accounts – while we understand that the same rules cannot be applied as the receiving PSPs fall outside UK jurisdiction, we would like to see proposals for how UK PSPs can better protect consumers in this space. We have also seen a huge growth in scams involving cryptocurrency in the last twelve to eighteen months where there are currently very few protections for consumers. Given the lack of protections for consumers in this space, we would like to see PSPs developing specific warnings when consumers are about to make payments to foreign bank accounts or cryptocurrency exchanges, as well as taking the time to make more checks where payments are high value or unusual for the customer. We hope that the introduction of the FCA’s Consumer Duty will encourage PSPs to take these steps and do more to help customers understand the risks they are taking when making foreign payments or converting their money to cryptocurrency.

While the NTS Scams Team does not believe that rules around reimbursement should apply to civil disputes, we are aware that deciding whether a case is a scam or a civil dispute can be complex for PSPs since it often revolves around intent. It is important that this is closely monitored to ensure that PSPs are not treating scams as civil disputes, leading to victims missing out on reimbursement. Cooperation between PSPs and trading standards on these cases can assist PSPs in making good decisions on whether a case is a scam or not. The NTS Scams Team is currently running a pilot working with PSPs to assist them in these cases. We have received a total of 77 queries from 7 different PSPs since the pilot began in July. We are open to working with the PSR and PSPs to discuss cooperation in future.

#### **4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

The NTS Scams Team agrees that it is appropriate for there to be some consumer caution exception to reimbursement to avoid misuse of the system. However, there is a limited amount that the consumer can do to protect themselves from APP scams, many of which are increasingly sophisticated. Perpetrators are known to use psychological manipulation to create a sense of urgency, panic, and fear among their victims, which puts them into a “hot-state” and limits their ability to make good decisions. The sophistication of many APP scams has long been underestimated, resulting in victim blaming.



Moreover, under the current CRM Code, exceptions to reimbursement based on consumer behaviour, particularly “reasonable basis to believe”, have been overused by PSPs to place liability on the victim and avoid reimbursement. Some PSPs have also been unrealistic in their expectations of the checks consumers should make before they make a payment.

We have heard concerns that removing the expectations of consumers which are set out in the CRM Code could lead to a moral hazard. However, we have not seen any evidence that consumers will take less care when making purchases. Indeed, TSB [gave evidence](#) to the House of Lords Fraud Act 2006 and Digital Fraud Committee earlier this year stating that they had not seen an increase in fraud reports after they introduced their fraud guarantee in 2019. No one wants to become a victim of fraud and there are often serious non-financial consequences.

With this in mind, we believe gross negligence is a reasonable balance between the expectation that the consumer take care when making a payment, and the recognition of the sophistication of APP scams.

However, as the use of gross negligence as a consumer caution exception would be new, we are concerned about interpretation and implementation. We do not believe that cases of unauthorised fraud will be of use because it is so different from authorised push payment fraud. In order to prevent inconsistencies in interpretation, especially in the first few months, we would like to see the PSR providing some guidance on what it considers gross negligence in the case of APP scams. At a minimum, we urge the PSR to set out in guidance what it does not consider gross negligence and make clear that PSPs cannot continue to use the same exceptions to reimbursement which are in the CRM Code – in particular ignoring warnings or reasonable basis for belief.

#### **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

The NTS Scams Team supports the proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence. We cannot expect consumers who are made vulnerable by their circumstances to protect themselves from scams and fraud. This will also place incentives on PSPs to do more to proactively identify vulnerable consumers and put measures in place to protect them before they become victims of scams (and to prevent repeat victimisation).

#### **6. Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?**

We agree with the proposal to use the FCA’s definition of a vulnerable customers. However, we would like to see monitoring from the PSR or from the body responsible for enforcing the proposals to ensure that the guidance is interpreted and implemented fairly and consistently by PSPs, including monitoring of the number of victims who are reimbursed because they are judged to have been vulnerable at the time of the scam. We would also like to see PSPs providing evidence of how they are supporting customers experiencing situational vulnerability.

#### **7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement**
- **any ‘excess’ should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?**

We agree with the PSR’s proposal that PSPs should be able to exempt vulnerable consumers from any excess they apply.

#### **8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

We are concerned that a minimum threshold may discourage reporting. There are already many reasons why scam victims do not report fraud and it is estimated that only 5-10% of scams are reported. Mandatory reimbursement could help to increase reporting rates and increase our understanding of this type of fraud. However, a minimum threshold could discourage those who have lost less than £100.

We believe that many PSPs are automatically reimbursing relatively small losses and would not want to see this change under the PSR's proposals.

While we understand that the proposals are intended to give PSPs a choice about whether to apply a minimum claim threshold and what level to set this at, this could be confusing for consumers if PSPs adopt different policies.

If there is a minimum claim threshold, vulnerable consumers should be exempted from this threshold. This is particularly important for repeat victims who have made small payments in response to multiple different scams. The NTS Scams Team works with victims of mass marketing scams, many of whom are chronic victims who have made multiple small payments to criminals adding up to hundreds or even thousands of pounds over time. While many of these payments are not currently made by APP, the push towards internet banking will make this more common over time. The PSR should mandate that vulnerable customers are excluded from the minimum claim threshold.

#### **9. Do you have comments on our proposal not to have a maximum threshold?**

We support the PSR's proposals that there should not be a maximum threshold. PSPs should apply greater scrutiny to high value payments – this is expected by consumers. Moreover, consumers currently have a limited choice as to how they can make high value payments and should not be penalised where they are forced to use Faster Payments to make a high value payment. We hope that this will also incentivise PSPs to increase choice for consumers in how they make payments, including being able to choose slower payments where they wish.

#### **10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

We are concerned that a time limit of 13 months is not long enough. We know that many victims do not realise that they have been victims of a scam for many years, especially but not exclusively in cases of investment fraud. It is common for it to take two years or more for investment scam victims to realise that their investment was not genuine. We have included a case study at the end of the response which illustrates this. While we appreciate that the PSR's proposals leave room for victims to take their claims to the Financial Ombudsman Service after the time limit on claims has passed, we are concerned that victims will not know or understand this, especially when told by their PSP that they have exceeded the time limit for claims.

We do not believe that APP scams can be compared with unauthorised fraud as the victim will expect to see the payment on their statement (they made it), and therefore we do not think the time limit for claims should be the same.

#### **11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**

- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We agree with the PSR's proposals that the sending PSP should be responsible for reimbursing the customer, and this should be separate from the process of sending and receiving PSPs sharing the costs. However, we are concerned that the 48 hour time limit may lead to unintended consequences, with sending PSPs rushing to make decisions in a short time frame which could lead to poor decisions being made.

We understand that the PSP may need to speak to the customer more than once to reach a decision. In some cases they may need to establish whether the case is a scam or a dispute between a legitimate trader and customer. The NTS Scams Team has assisted PSPs with a number of these cases and appreciates that they can sometimes be complex, as PSPs need to complete searches on company history, establish what work (if any) has been completed, and whether the customer is still able to contact the company.

Given that the majority of victims of APP scams will be reimbursed under the proposals, we believe it may be better to extend the time limit on reimbursement to ensure that the right decision is made the first time. However, given the simplicity of the PSR's proposals, we believe that PSPs should be able to come to a decision more quickly than under the CRM Code.

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The PSR should closely monitor how many cases are taking longer to investigate. These cases should not take longer than 15 working days to investigate (the same as the time limits under the CRM Code) as it is unreasonable to leave the victim waiting for a long time for a decision.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

The proposal for a 50:50 default allocation seem sensible to ensure that equal incentives are placed on the sending and the receiving PSP to prevent fraud. The allocation of reimbursement costs between sending and receiving PSP should not affect the victim and they should not be left waiting while the PSPs agree costs between themselves.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

While we understand the PSR's rationale for wanting Pay.UK to be the rule setter, we are concerned about Pay.UK's capacity to enforce compliance with the new rules, in particular the lack of proportionate sanctions for those who are not applying the rules properly, and lack of influence over indirect scheme participants. Monitoring this mandatory scheme, which will apply to over 400 PSPs, will be a challenge on a totally different scale to the current CRM Code.

We are deeply concerned that the lack of capacity identified in the consultation document could lead to delays to implementation of the new rules while Pay.UK consults its members and develops new capacity and sanctions. This would be devastating for victims who would be forced to continue to rely on the inconsistency of the current system.

It is essential for victims that the new rules are implemented as soon as possible, and that as far as possible the rule changes occur all at once in a way that is easy to communicate to consumers. Victims should not be left to confused by a series of changes or complicated evolution of rules.

When the CRM was first launched there were a number of teething problems that caused a lot of issues for victims – decision making was even more inconsistent than it is today and communication with victims was poor. It is important that the new system avoids as many foreseeable problems as possible in order to avoid consumers losing confidence in the system. There must be strong system to monitor the success of the new rules from day one, and to measure victims' experiences of requesting reimbursement from PSPs. This should include close monitoring of how gross negligence is being interpreted, and how PSPs are assessing vulnerability.

Following discussions with other stakeholders, the most reliable and straightforward way to implement the new rules in the short term appears to be a PSR direction to all PSPs. This would ensure that both direct and indirect PSPs are brought into scope from the beginning, and that consumers are able to access key protections. We believe that placing the protections in legislation in the future should be considered as a longer-term solution to place these protections on a par with unauthorised fraud, but appreciate that over time Pay.UK may also be able to build up sufficient capacity to take this on.

It is essential that the PSR provides strong regulatory oversight of the new reimbursement rules, and ensures that PSPs face enforcement action if they fail to meet the PSR's standards.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

**24. Do you have views on the best option for short-term enforcement arrangements?**

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

**28. Do you have any other comments on the proposals in this consultation?**

We would like to see a more comprehensive assessment of what will be lost from the CRM Code, including the provisions on aftercare and education. Aftercare for customers who have been a victim of fraud could be improved. Although the major PSPs do put protections in place on customer accounts after they have been a victim of fraud, often these are not clearly explained to the customer, and they are not made aware of the choices they have. The CRM Code also provided a definition of effective warnings that will be lost if the Code is replaced.

While the warnings which have been introduced have varied in effectiveness, we believe that warnings at the point of payment remain a useful tool for PSPs to prevent fraud.

A key problem that trading standards officers have reported to the NTS Scams Team is the difficulty faced by some victims in reporting fraud. Some victims report that it takes too long to report fraud on the phone – although we appreciate that this has improved since 2019, we are still seeing case studies of people who are spending hours on the phone to report – as illustrated by the case study below. Victims who have been scammed over the phone may be reluctant to report the fraud via the phone and divulge sensitive details as they have lost confidence. Other victims, especially the elderly, cannot hear well on the phone. Many of the victims whom trading standards officers support would like to report fraud in person at their local branch, but this facility is not always available and they are often told to report on the internet.

Trading standards officers have repeatedly requested that PSPs set up a process to allow professionals working with victims to apply for reimbursement on their behalf. Some of the victims whom trading standards officers support find it difficult to report fraud to their banks and may struggle to communicate the details of their case to fraud investigators. While the NTS Scams Team is now working with UK Finance to allow trading standards officers to report fraud and vulnerability to some participating banks on behalf of the victim, we would like to see this scheme expanded so that all PSPs accept reports on behalf of victims from professionals such as trading standards officers, police officers, and adult social care workers.

As the consultation paper sets out, we hope that mandatory reimbursement of scam victims will increase the incentives on both sending and receiving PSPs to do more to prevent fraud. Trading standards officers working with scam victims on the ground have told us that they would like to see greater use of Banking Protocol type systems and flags on bank accounts for customers who may be at increased risk of becoming victims of fraud. We hope to see PSPs slowing down payments when they think a transaction is suspicious, speaking to the customer about that transaction where appropriate, as well as creating options for customers to choose the speed of their payments and other limits that they can place on payments from their account.

Given the scope of the PSR's proposals, we would like to see PSPs placing extra protections and warnings on payments which are not covered by the rules, including payments to cryptocurrency exchanges and foreign bank accounts. When making these payments, customers should be warned about common fraud methodologies and informed that they will not be protected by mandatory reimbursement if they choose to go ahead. PSPs should also apply extra checks on these payments to ensure that they are genuine.

Trading standards officers have told us that many victims are still not aware that they can apply to their PSP for reimbursement in the aftermath of a scam. When the new rules are implemented, the PSR must work with PSPs to make consumers aware that they can ask for their losses to be reimbursed.

#### **Case study:**

“Harry” was referred to trading standards by his social worker. He is an elderly gentleman living alone, he is housebound and a wheelchair user. Harry has a number of health conditions, including OCD and depression, he is a hoarder and has no friends or family. Harry gets confused easily and can struggle to communicate his thoughts clearly and coherently.

Criminals contacted Harry in 2015 with an investment opportunity. Initial contact was made by letter, but later progressed to phone calls. Harry only became aware that this was a scam (and is still reluctant to believe it) when he discussed his finances with his social worker in August 2022. He believes he has lost £44,000 in the scam. His bank statements from Lloyds show that around half of this amount came from his Lloyds bank account. He has invoices from the criminals which show further payments but it is not clear which bank account these invoices were paid from.

The social worker and Harry initially spent four hours on the phone to Lloyds to report the incident, which Harry found exhausting and confusing. Harry then received £10,000 from Lloyds but no explanation as to why the remaining money was not refunded. The trading standards officer phoned Lloyds in the presence of Harry and was directed through a number of different departments. At each department, Harry had to explain what had happened, and each time, he was confused and agitated. Eventually, they were put through to the right department but there was an hour waiting time to speak to someone (they had already been on the phone for an hour), and the trading standards officer had to leave.

In the end, the trading standards officer was able to get in touch with a contact at Lloyds who passed the message directly to the fraud team. Harry has now received reimbursement for the full amount from Lloyds.

# Nationwide

# Nationwide Building Society

## Response to Payment Systems Regulator Consultation on Authorised Push Payment (APP) Scams

Date: November 25<sup>th</sup> 2022

NBS Accountable Executive: [REDACTED]

Sent to: [appscams@psr.org.uk](mailto:appscams@psr.org.uk)

If you have any questions relating to this response, please contact:

[REDACTED]



Contents

2.	Executive Summary .....	3
3.	Summary of overall response .....	4
4.	Questions.....	6
4.1	Impact of proposals on consumers .....	6
4.2	Impact of proposals on PSPs .....	6
4.3	Scope proposed for requirements on reimbursement .....	7
4.4	Consumer caution exception to mandatory reimbursement.....	8
4.4.1	Gross negligence as the consumer caution exception.....	8
4.4.2	Non provision of additional guidance on gross negligence.....	8
4.5.	Reimbursement of vulnerable consumers even if they acted with gross negligence .....	8
4.6.	FCA’s definition of a vulnerable customer .....	9
4.6.1	Definitions.....	9
4.7	Sending PSPs ability to apply a modest fixed ‘excess’ to reimbursement .....	9
4.7.1	Excess set at no more than £35 .....	9
4.7.2	Exempt vulnerable consumers from any ‘excess’ they apply.....	9
4.8	Minimum claim threshold .....	9
4.8.1	Threshold set at no more than £100.....	10
4.8.2	Exempt vulnerable consumers from any threshold they set?.....	10
4.9	Not having a maximum threshold .....	10
4.10	Sending PSPs allowed to set a time-limit for claims for mandatory reimbursement .....	10
4.10.1	Time-limit set at no less than 13 months.....	10
4.11	Sending PSP is responsible for reimbursing the consumer .....	11
4.11.1	Reimbursement as soon possible, and no later than 48 hours after a claim is made.....	11
4.12	Standard of evidence for gross negligence or 1st party fraud & how long to investigate.....	12
4.13	50:50 default allocation of reimbursement costs between sending and receiving PSPs .....	12
4.14	PSPs able to choose to depart from the 50:50 default allocation .....	13
4.15	Scheme rules for 50:50 default allocation to multi-generational scams.....	13
4.16	50:50 default allocation of repatriated funds between sending and receiving PSPs .....	13
4.17	Rules on allocating the costs of mandatory reimbursement.....	14
4.18	Long-term vision, and rationale for PSO being responsible for mitigating fraud? .....	14
4.19	Minimum initial set of Faster Payments scheme rules needed.....	14
4.20	How to exercise powers under FSBRA to implement our requirements.....	14
4.21	How allocation criteria and dispute resolution arrangements are developed and implemented.....	15
4.22	Short-term implementation approach, Pay.UK to implement compliance monitoring regime .....	15
4.23	Costs and benefits of Pay.UK implementing a real-time compliance monitoring system.....	15
4.24	Option for short-term enforcement arrangements .....	15
4.25	Best way to apply the rules on reimbursement to indirect participants.....	16
4.26	Whether we should direct indirect PSPs or IAPs .....	16
4.27	Cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis? .....	16
4.28	Other comments on the proposals in this consultation .....	16
5.	Conclusion.....	17

## 1. Introduction

Nationwide Building Society (NBS) is the country's largest building society, and we are owned by our 16.3 million members. As a mutual we operate in our members' long-term interests, and those of wider society, by working closely with stakeholders across the financial services sector and beyond. We welcome the opportunity to participate in this consultation exercise and fully support the rebalancing of the primary focus away from reimbursement, towards improving protection and greater sharing of liability between Sending and Receiving firms.

## 2. Executive Summary

- 1. In line with our response to the consultation on APP scams in early 2022, NBS aligns with the PSR proposals in principle.** We are supportive of the need for greater protections and have responded individually to each of the consultation questions, with the aim of enabling the development of a solution that is proportionate, efficient, workable, and supports the goals of consumer protection and scam prevention, without the challenges and issues that experienced with the implementation of the Contingent Reimbursement Model (CRM).
- 2. NBS is pleased to see the increased focus on minimising emotional and financial harm for consumers,** disrupting criminality, and reducing the impact of scams in society has long been positioned by NBS as a mutual priority and we are pleased to see the PSR taking these active strides towards improving this aspect.
- 3. NBS welcomes the fairly distributed liability for FP consumer reimbursement between Sending and Receiving Firms.** NBS proposes this should be underpinned by further guidance on a non-exhaustive set of steps and criteria for SFs to follow when assessing claims, and for higher value cases only, a dispute resolution framework between PSPs which is well defined, simple, and easy to operate. We are concerned to avoid a dispute resolution framework that creates a material overhead that draws focus away from prevention activities.
- 4. The application of these proposals to all market participants is a welcomed step forward in consistent consumer protection.** NBS believe this coverage will significantly improve the standards of care and prevention across the industry, will close gaps in operating standards and controls, with very clear and obvious benefits being realised once firms become aware of quite how much can be clawed back from them if they enable high volumes of account misuse.
- 5. These proposals must be part of a long-term strategy for shared responsibility in combatting APP scams.** NBS believes the most effective line of defence to detect and prevent APP scams draws its strength from a mutual responsibility shared across the sending PSP, the receiving PSP, and the customer in between, with other responsible ecosystem players such as social media, fintech and telecoms joining in the fight as soon as possible. We will continue to promote these mutual responsibilities with our members and our colleagues and in the market.
- 6. The PSR proposals are part of an evolving defence against scams** where mutual responsibilities should both continue to include the consumer who makes their own decisions about where they send their money and must expand to include relevant ecosystem players. Our response affirms that with clear principles and conventions to illustrate what gross negligence means in an APP scams context, we may help customer understanding and support avoid unintended outcomes for all. And we are also clear that as we look to develop the wider application of Account-to-Account Retail Transactions, commercial disputes should not be subject to the same reimbursement mechanisms that are set up for APP scams.

### 3. Summary of overall response

1. **The scope and definitions do not fully reflect current industry thinking.** Payments to self (so-called ‘me to me’ payments) are included, cases are not decisioned at a payment level and a different definition of vulnerability to the existing definition could lead to potentially significant unintended consequences.
2. **The proposed 48-hour SLA for decisioning claims is operationally** challenging given the complexity of many APP cases, and may not be workable, especially for smaller firms or those that do not operate 24/7.
3. **Transitional Arrangements and the future of the CRM Code is unclear.** The proposal does not stipulate whether part or all of the CRM requirements will disappear, or how Pay.UK rules and CRM will interrelate.
4. **All domestic push payments should be in scope.** The scope of these proposals should extend to retail CHAPS and ‘on us’ transactions, even if Pay.UK becomes the primary hub for governing standards and rules.
5. **There is little mention of how industry data sharing or the need for cross-industry collaboration will be facilitated.** NBS see this as crucial in the prevention of scam payments at source.
6. **The potential for significant increased payment friction** is not properly assessed. Ideally standardised industry approaches or best practice should lead to ensure consistency and avoid consumer confusion.
7. **The dispute resolution framework is yet to be designed** and will impact operational effectiveness, as a minimum we must monitor the application of these proposals to test and learn through insights following implementation.
8. **We are disappointed that the PSR has not signposted anything tangible around the involvement of other industries (social media, telecoms, etc).**
9. **Further guidance on ‘gross negligence’ is essential** to avoid inconsistent application between firms and FOS (as seen with CRM), clear examples will help with the understanding and support envisaged in the FCA’s Consumer Duty, empowering customers to work with us to avoid the foreseeable harm of APP scams
10. **Liability sharing between SFs / RFs** should be underpinned by guidance and criteria for assessing claims, to avoid disputes.
11. **Repatriation proposals** should extend to developing a standard / default methodology for determining competing claims to co-mingled funds which firms can adopt with legal certainty.
12. **The proposed claim threshold (£100), excess (£35) and time limit (13 months)** should be embedded into the FP scheme rules as the default position and periodically reviewed based on industry data to arrive at the optimal values and time limits. Clarity is needed from FOS as to how it will decision complaints falling below these limits. And these limits should be tested to ensure they are appropriate to their objective.
13. **Management of low value scams needs care** to ensure we balance the cost: benefit for our members and customers as a whole, we therefore support the recommended low value cap. Purchase scams should be in scope, but they need particular care to distinguish criminal activity from civil disputes.
14. **We recognise that the absence of an ‘upper threshold’ for claims** risks smaller firms bearing unsustainable costs and payment limits inevitably being enforced. However, NBS believes all consumers should receive appropriate and equal protections and that greater friction for high value payments is likely to be the ‘price’ for this.

15. **UKF advocates implementation through directions on PSPs**, NBS would prefer to avoid firm-level directions, rather than Pay.UK being directed to develop scheme rules. NBS envisages a governance model in the long term in which Pay.UK runs the operating standards and the rules of participation, with disputes and insights feeding into a continuous cycle of development, especially as new opportunities emerge via overlays and the New Payments Architecture. In the meantime, industry needs to work with the PSR on the transition to this.
16. **The regulatory landscape must avoid becoming too federated** with clarity on leadership, standards, boundaries, and accountabilities, in a set up that enables and empowers Pay.UK to add most value.
17. **There is uncertainty as to the impact of these proposals on consumer caution**. We would suggest therefore that this is assessed as part the PSR’s post-implementation review.
18. **The assumption that any additional friction will affect only ‘a small proportion of payments’ is untested**. To limit friction to a small proportion, much more must be done to support and facilitate data sharing amongst firms, as acknowledged by the PSR under ‘Measure 2’ of the wider proposals.
19. **The technological changes needed to underpin these proposals should not be underestimated**. The UKF BPS portal is our current communication mechanism between Sending and Receiving Firms and if this is now to be used by all market participants there will need to be a significant uplift in the scalability, capacity, stability, security, and performance of that technology. This will need to be in place prior to any industry roll-out.
20. **The impact on claim volumes should not be underestimated**. By widening the ability to ‘clawback’ scam payments from the Receiving Firm to the whole of market and not just CRM members, there is a risk that implementing this proposal could initiate a significant volume of claims, which may not be manageable with the technology and operational models currently in place. NBS request that analysis of the likely/potential uplift in volumes is considered prior to any implementation date being mandated.

---

I think we absolutely need to send a message that individuals need to have some responsibility to understand and make their own decisions about where they send their money, and the risk of moral hazard if we have to accept any and all cases where people feel that their investments and financial dealings have not gone as they expected.

We must also be clear that commercial disputes should not be subject to the automatic reimbursement mechanisms that are set up for APP fraud,

## 4. Questions

### 4.1 Impact of proposals on consumers

Overall, the impact should be positive with increased protection. However, to achieve the ultimate goal of greater scam prevention, firms will need to evolve their advice and intervention measures. Section 3.1 references the expectation of more friction for ‘a small proportion of payments’. The proportion of scams to genuine payments is small, but the assumption that only a small proportion need additional friction is untested. It will rely heavily on a firms’ technical capabilities as to whether they can sufficiently refine the number of payments that require additional friction to avoid larger scale changes to payment journeys.

We note the PSR’s assertion it has not been able to quantify the likely costs of delayed or declined payments (s2.53). However, we strongly suggest some attempt is made by the PSR to quantify this and that this is then reassessed as part of a post-implementation review. It should also be considered that consistent data sharing within the payment message, to better assess scam risks, is likely to require additional information capture from consumers and increased delays to accessing incoming payments.

Our ambition should be an optimal level of friction targeted at high-risk payments. There will doubtless be testing and learning in trying to find this balance of service and security but there are positive factors to remember: First, risk analysis will improve in support of safe levels of straight-through processing as industry develops solutions in data sharing across counterparties as well as transaction data analytics supported by Artificial Intelligence and networked via near real time API interactions. Second, government and regulators can work with the industry to build public understanding and support explaining where more time is needed to protect customers, aligned to the principles in the FCA’s Consumer Duty.

It is also important to note that additional prevention for Faster Payments may simply drive a migration of scams to other payment types, as PSR has noted. Despite card systems having existing protections, authorised card scam payments do not fall within the remit of these protections, and they are already rising. As with APP prior to a consistent reporting regime the scale of the issue is unclear, and consumers may still be targeted just as much by other means.

### 4.2 Impact of proposals on PSPs

The costs of implementation are unclear but likely to be significant and implementation will be challenging, unless very clear and consistent standards are adopted across all firms.

To achieve the ultimate goal of prevention firms must reconsider their approaches to inbound payment processing and risk assessment. This would benefit greatly from further guidance on delaying incoming payments, given receiving PSPs are subject to an obligation under Reg 89 of the PSRs 2017 to put incoming funds at the payee’s disposal ‘immediately’. The FCA’s PSR Approach Document presently confirms that the expectation is for this to take place within 2 hours ‘in normal circumstances’. It would assist intervention measures, if this guidance could clarify that incoming payments considered to be at higher risk of fraud can be delayed beyond the standard 2 hours.

The implementation approach to deploy these proposals will be a factor in the impact on PSPs. Some will argue for the PSR to issue Specific Directions directly on firms, to cover all relevant payments, including Faster Payments, ‘on us’ and retail CHAPS, citing valid concerns around the application of the proposals to indirect participants and the capacity and capability of Pay.UK.

However, NBS envisages a governance model in the long term in which Pay.UK runs the operating standards and the rules of participation, with disputes and insights feeding into a continuous cycle of development, especially as new opportunities emerge via overlays and the New Payments Architecture. We do not see fundamental barriers to the scope of standards and rules being extended to include indirect participants,

supported by their sponsors. Nor should there be barriers to applying common standards and rules primarily associated with Faster Payments to CHAPS and ‘on us’ payments, in a similar way to the current application of CoP.

In the short term, we need to consider the pathway to this potential end state, working with the PSR on the specifics of a simple and efficient governance model. We need to avoid an overstretch of Pay.UK’s capacity and capability in the short term while it is focused on delivering today’s services, plus development of the NPA and, importantly along the way, developing what could be valuable transaction data analytics in its Fraud Overlay proposal.

Other key points to note about the impact of firms in the market include the inclusion of PISPs which must be mandated to share risk data with ASPSPs so APP scams can be detected and prevented – all participants in the Open Banking supply chain need to have incentivised accountability.

The PSR suggests (understandably) more reimbursement, applied more fairly across sending and receiving PSPs will add to the stimulus for more prevention. But we need to be alert to unintended consequences for some smaller and perhaps indirect participants, some of which may operate services less vulnerable to scams (nominated destinations etc).

The PSR must ensure the distinction between protections against APP scams and protections for Account-to-Account Retail Transactions (A2ART). The treatment of civil disputes must not replicate the characteristics of redress in a fraud scenario – the APP scams model is not a precedent for the handling of civil disputes where recognition of payee responsibility and liability is paramount. The PSR needs to underline the differences here to ensure A2ART develops with sustainable protections applied appropriately. We recognise this will become technically easier to do with enhanced data, identifying retailers and payment purposes (etc) as in card transactions.

Until such time as the whole ecosystem (including upstream sectors, such as social media firms and telecoms) is committed, and the best technical options are at play, we will continue to experience high levels of APP scams.

### 4.3 Scope proposed for requirements on reimbursement

We believe it is of the utmost importance that reimbursement is consistently and simultaneously applied across the industry. We have a number of observations we believe must be addressed to achieve this:

The proposed ‘APP scam’ definition where a payment is made ‘subsequent to fraud or dishonesty’ (s4.11) is not aligned to the CRM definition, as it does not exclude ‘me to me’ payments, where the customer has sent funds to their own accounts / wallets without losing control. We believe the definition should either mirror the CRM definition, or otherwise require the customer to have lost control of the funds (as the PSR seems to have envisaged in para 2.1 in identifying loss of control as a defining characteristic of an APP scam).

Voluntary approaches to payment types like CHAPS or ‘on us’ payments could lead to different costs of implementation, and multi-generational scams will become increasingly confusing to investigate and resolve consistently for consumers.

We agree with the exclusion of civil disputes in 4.13 (per CRM) but would question whether purchase scams and disputes can be reliably distinguished in a short investigation timeframe. We need sufficient investigation to distinguish between purchases that are APP scams and purchases that are civil disputes. It will be uneconomic and undermining of developments in sustainable A2ART payments if we treat all purchase related claims as APP scams – but where there is a fraudulent act, this should be investigated, with redress where appropriate for the consumer and fraud intelligence for the industry.

The framework envisages measures applying to claims or ‘cases’ and not payments. This exacerbates the potential for confusion as scams may involve many payment types and journeys over a long period sometimes. A more viable system would be for standards to apply at payment level, as they do today under the CRM because the prevention standards will vary, and measures could be applied to payments clearly in scope and only after the measures are brought in. Otherwise, historic backlogs might create complexity in case handling that counteracts the speed at which PSR envisages refunds and investigations to be processed.

Also key to the scoping question are the responsibilities and liabilities of PISPs. The PSR’s proposals can be enabled by PISPs sharing Transaction Risk Indicators and allowing suitable friction where it is in the interest of the customer – including CoP checks. This is an increasingly important risk vector, and the implications include sharing of responsibilities and liabilities for APP scam reimbursement where appropriate – for example both PISPs and ASPSPs can act as sending PSPs in the Open Banking scenario.

#### 4.4 Consumer caution exception to mandatory reimbursement

We agree that it will be necessary to allow PSPs to decline some claims, where the consumer can be deemed to be responsible, and that this should be a minority.

##### 4.4.1 Gross negligence as the consumer caution exception

We believe consistency of application is a more important principle and simplicity (for consumers and firms) is key. A lower bar than Gross Negligence increases the complexity but wherever it is set, we believe clear expectations need to be defined as to what this amounts to. A core issue with the CRM implementation was differing interpretations between FOS and firms on the expected level of customer care and the wait for FOS guidance post-implementation (contributing to a backlog of complaints). A repeat of this must be avoided with clear guidance available at implementation. We also would suggest that clarity is provided as to whether dishonesty when making a claim amounts to 1st party fraud. In APP claims, there may be questions about circumstance and scope for customer dishonesty over tangential aspects and CRM allows any dishonesty in making a claim to be considered.

##### 4.4.2 Non provision of additional guidance on gross negligence.

We believe the lack of additional guidance will lead to inconsistency in application, or lack of application of the Gross Negligence principle at all. Some clear principles or conventions should be defined or be required to be defined by industry and/or Pay.UK. For example, the principle of a consumer lying about the purpose of a payment, with no credible reason for doing so, or disregarding repeated clear advice when there is an appropriate intervention, should be clearly specific within the definition. This is because some principles will need to be established to help drive consistent application of prevention measures and whether their application influences the extent to which a consumer may have been grossly negligent. This is a weakness in the CRM where the concept is undefined, and guidance under the proposed framework can be provided via industry-developed and PSR-endorsed case studies.

#### 4.5. Reimbursement of vulnerable consumers even if they acted with gross negligence

Consumers who are vulnerable to APP scam (i.e. could not be reasonably expected to protect themselves) should continue to receive full reimbursement, as we believe they do today. In addition, we would also advocate for more guidance and case studies supporting consistent assessments of what may constitute vulnerability in the specific circumstances of the many varied scams which are perpetrated, to help ensure the industry does all it can to be as consistent as possible when determining vulnerability to APP scams.



## 4.6. FCA's definition of a vulnerable customer

We note that the definition is not the same as that which is currently used by firms under the CRM. We would question why this is, and whether the intention is to define a different population from that which CRM aims to protect. This could lead to disparity across the industry and once again lead to FOS disputes.

### 4.6.1 Definitions

We therefore recommend that the definition within the CRM is used. It is more reliable for both implementation, as it is used today, and for its application specifically to APP scams.

## 4.7 Sending PSPs ability to apply a modest fixed 'excess' to reimbursement

We support this, given a large volume of low value claims, many of which may be disputes, and where it is questionable as to whether there is significant detriment. However, defining it as single requirement and value, consistent across all PSPs without the ability to flex it would avoid consumer confusion and receiving PSPs having to accept the excess applied by the sending PSP assessing the claim

### 4.7.1 Excess set at no more than £35

We cannot see evidence of a clear rationale for this threshold. We understand the basis, aligning to the PSRs 2017 in relation to unauthorised transactions and trying to bring consistency for customers. But we believe that Pay.UK should at the very least be required to periodically review this to ensure it is appropriate in supporting an efficient process for consumers which does not cause unnecessary detriment. We also assume the proposals would apply this excess at a case level, despite the protections of a payment scheme naturally being relative to the payments themselves.

### 4.7.2 Exempt vulnerable consumers from any 'excess' they apply

We support this and would go further to suggest that sending PSPs have a discretion to exempt any customer from the excess where they deem this would be detrimental to the customer based on their individual circumstances but, if they do so, that firm should have to absorb that exemption themselves rather than pass on/share with the receiving Firm.

## 4.8 Minimum claim threshold

If a threshold is to be applied, we would question whether it should be applied to payments and not cases e.g., 100 x £10 payments would qualify for reimbursement, despite being very different to a 1 x £1,000 payment in terms of the prevention measures likely to be deployed and the assessment of gross negligence and other factors.

We also suggest FOS is invited to clarify if it will apply these thresholds as this consultations intends, to avoid the potential for inconsistent application during any potential disputes that are raised with FOS.

It is also unclear whether PSPs would be permitted to automatically reject claims falling under these thresholds or be required to still record and report claims below the threshold. We therefore request clarity over this point to ensure the goal of threshold, which must be to prevent a disproportionate operational burden on firms handling large volumes of claims, can be achieved.



#### 4.8.1 Threshold set at no more than £100

We note this threshold replicates that used for s.75 claims, which was last updated in 1983. It is unclear, and we would request clarification, as to why the PSR considers this specific level to be appropriate for APP scam claims to be assessed some 40 years later.

#### 4.8.2 Exempt vulnerable consumers from any threshold they set?

We support this. Vulnerable consumers should receive greater protections.

#### 4.9 Not having a maximum threshold

NBS has taken onboard the view of our industry forum and many of our peers who are concerned at having no threshold. We can see the argument that a maximum threshold would be required to mitigate the risk of unlimited liability, particularly for smaller firms bearing unsustainable costs, and the influence it may have for consumer caution and payment limits potentially being enforced. However, we recognise the principle; that all scams of any value should be treated consistently where at all possible, and particularly where there is significant detriment, and think that any potential intervention in large payments should not be viewed as negative friction, but a protection, so that we are prompted to manage the risk appropriately and intervene and stop large risky payments as we deem necessary and appropriate.

#### 4.10 Sending PSPs allowed to set a time-limit for claims for mandatory reimbursement

We believe it sensible to set clear expectations and to manage the limitations in data and consumer recall of events after a long period of time has passed. However, we note that consumers can complain to FOS after up to 6 years from the payment, which potentially negates a shorter limit.

We therefore believe it would be highly beneficial for FOS to clarify how it will apply the time limit to ensure the PSR's objective is met.

Additionally, we should consider the scenario that a limit will apply from the date of the final payment involved in the scam, meaning some claims may still include payments made well outside the limit. This might present complications for some complex long running scams, and it would be beneficial if PSR could clarify, or work with Pay.UK as part of implementation, to produce guidance as to how a PSP should assess whether individual payments are part of the same 'scam', where they are complex and may involve a resurgence of contact between the scammer and the victim, such as can be the case with romance or investment scams.

##### 4.10.1 Time-limit set at no less than 13 months

As a general comment, the proposed claim threshold (£100), excess (£35) and time limit (13 months) should be embedded into the FP scheme rules as the default position, with flexibility for individual PSPs to derogate from these should they wish, and the precise levels chosen should be reviewed regularly by Pay.UK in view of intervening developments and claims data. The consultation suggests this would be left to the individual PSP to decide whether, and to what extent, to apply these limitations on reimbursement, which we expect would require PSPs to reflect them in their T&Cs (as is the case for the corresponding limitations on UPP claims in operation today).

We firmly believe the better approach would be for these limits to be fully embedded in the FP Scheme rules as default levels, with those rules then permitting individual PSPs scope to derogate from those default levels should they wish.

The benefits of this approach, compared to requiring the limits to be specified in T&Cs, are:-

1. It would provide one consistent and flexible industry source document, and promote more consistent customer understanding of the limits;
2. It would avoid the time & resource of every PSP having to provide a minimum of 2 months' notice of T&Cs changes, and the risk of resulting customer disruption / confusion;
3. Those PSPs choosing to apply more generous limits could do so by way of a waiver, for which T&Cs would not be required;
4. The limits could then be regularly kept under review and adjusted going forward without requiring future T&Cs updates.

#### 4.11 Sending PSP is responsible for reimbursing the consumer

We consider this to be the most workable and simple model for consumers, though we would reiterate our earlier comments concerning the responsibilities and liabilities of PISPs. The PSR's proposals can be enabled by PISPs sharing Transaction Risk Indicators and allowing suitable friction where it is in the interest of the customer – including CoP checks. This is an increasingly important risk-vector, and the implications include sharing of responsibilities and liabilities – for example both PISPs and ASPSPs can act as sending PSPs.

##### 4.11.1 Reimbursement as soon possible, and no later than 48 hours after a claim is made

Currently the standard timeframe for non-complex cases is 15 business days under the CRM, and 35 business days where complexities arise or information not typically available is required. To reduce this to 48 hours, in broad alignment with the treatment of fraud claims regarding unauthorised transactions, is a significant change. We expect this will prove a significant challenge in such a high proportion of cases that it would be unworkable, given the added complexities that arise in APP scams (which has duly been acknowledged by the PSR).

Establishing the consumer's intent, vulnerabilities, actions, potential indicators of (gross) negligence and ensuring they receive sufficient guidance and support requires significant effort and industry set itself a timeline of 15 days, believing this to be reasonable and achievable. We are concerned that a significantly shorter period could lead to less stringent investigations, or investigations having to continue past the refund being issued, cause confusion to the consumer and result in avoidable complaints.

Additionally, it could increase 1<sup>st</sup> party false claims if claims cannot be investigated rigorously and, in cases where the scammer is likely to recontact the victim and continue to target them, it will be important to safeguard that victim from potentially being scammed out of the reimbursed monies soon after. These risks exist today but could be exacerbated by a very short timescale for investigation and refund.

We acknowledge the benefit to consumers of faster processes, and so we advocate continuing to consult industry on whether and how the CRM timescale of 15 days could be shortened, by assessing the barriers to this and defining actions which could alleviate any pressures born from any elements of the proposals. We would also request clarification of the rationale for firms being required to notify Pay.UK in cases where the time limit cannot be met. In some cases, notification may not be permissible due to tipping-off constraints and there is not an equivalent notification obligation for unauthorised fraud claims.

We believe it should be sufficient to notify the customer of the delay and the reasons why (so far as they can be provided under current regulatory restrictions) and at the same time to provide complaint rights, as per the arrangements of the CRM. We are unsure as to the benefits of reporting any intentions to extend the timescale on a case-by-case basis, but fully accept a system must be devised which tracks the adherence to the timeframe at an aggregate level. We believe this aim can be achieved via summary reporting more efficiently.

We should note that in some cases, indirect participants may face particular challenges. Practically it is not clear how indirect firms, operating their clearing compliantly in D+1, but not in near real time nor 24/7, will be able to meet the obligations of the reimbursement proposals.

Finally, such a short timescale has the potential to detract from rigorous investigatory efforts, and if PSPs are not afforded time to assess the MO of scammers and make use of these insights to enhance future prevention measures, there is some potential that this could make the UK a more attractive destination for scams in the longer term.

#### 4.12 Standard of evidence for gross negligence or 1st party fraud & how long to investigate

Gross Negligence: the concept of ‘a very significant degree of carelessness’ should be underpinned by specific guidance, set against a small number of simple principles with supporting industry agreed case studies (see response to Q4). If such guidance and clarity exists, then the standard of evidence can be related to these documented principles. NBS has provided examples of our view in a separate offline version of this response.

#### 4.13 50:50 default allocation of reimbursement costs between sending and receiving PSPs

We welcome the fair distribution of liability between sending and receiving firms and more responsibility to be taken by the receiving firm. Defaulting to an even split in the first instance is a simple model that should not present any conceptual barriers to implementation as both PSPs can apply controls which mitigate the risk of an APP scam being successful.

We do have a concern, however that the receiving PSP must effectively accept or underwrite the liability assessment of the sending PSP without having direct control or oversight of that assessment. At an aggregate level, potential concerns over the approach taken by a sending firm to liability would hopefully be discernible by the Payment System Operator or oversight body, but this assumes such mechanisms will be in place, and are reliable and functioning correctly. It is therefore important to arrive at clarity over these arrangements as soon as possible.

For example, sending PSPs may be motivated to introduce ‘floor limits’ whereby lower value claims, up to a given threshold are auto refunded without a robust investigation for operational reasons and if so, they may be introducing more liability to a receiving PSP than would be the case if the sending PSP investigated each claim. The prospect of a receiving PSP having to bear additional reimbursement costs solely as a result of the particular sending PSP’s operational approach would undermine the principle of this model and clear guidance may be required by Pay.UK, or the PSR as to whether such approaches are permissible.

We also believe that to incentivise PISPs to ensure that they have in place necessary fraud prevention tools, an alternative model may place 50% of the sending PSP liability on the PISP, i.e., 25% reimbursement by the sending PSP and 25% by the PISP. There needs to be more consideration of the role of PISPs in APP scams and how they will fit into the framework. Strategically, public policy through law and regulation must also bring the responsibilities of wider ecosystem players into the fight against APP scams – this may in turn influence the balance of funding redress in the longer term.

#### 4.14 PSPs able to choose to depart from the 50:50 default allocation

The principle that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution is logical, as there may particular be cases where control failings on the part of one firm have occurred, or where the balance of liability is appropriate to rest for the most part with one or other PSP.

However, to be a workable process, it would be important that this proposal is underpinned by a specific and granular set of assessment standards for the sending PSP to adhere to. In order to minimise the number of disputes between PSPs, we also believe that a minimum value threshold below which disputes cannot be initiated should be considered. Without this, the framework could create a significant overhead and we would question whether the benefits to scam prevention are significant enough to justify the proposal; it possibly risks diverting attention and resource into disputing cases and not control improvements.

There may be value in assessing the inclusion of APP scam performance data into the mix (Measure 1, metric C data, proportionate to PSP market share and used within the PSP liability model). In such a model of reciprocal dependency, this may guard against some receiving PSPs disproportionately bringing risk into the market if their performance over time is evidenced to be weak – and this may in turn lead to a shift in the liability from 50:50 to 40:60. for example, as a stimulus to improve controls.

#### 4.15 Scheme rules for 50:50 default allocation to multi-generational scams

We reiterate the point we made in response Q3 regarding ‘me to me’ payments being included in scope. Only when control of the funds is lost can it be reliably and clearly defined as requiring assessment, which removes the issue of multi-generational scams. It cannot be appropriate for a PSP to be liable for a loss incurred as a result of a payment they did not facilitate. FOS currently typically holds sending PSPs liable for the 1<sup>st</sup> payment the customer makes, even if control over funds is not lost. That approach overlooks the fact that ‘me to me’ scam payments are significantly harder for the SF to detect and intervene in because the recipient is not suspicious. The PSR’s acknowledgment of this would be welcome.

We think the simpler approach would be to mimic the scope of the CRM by providing that the APP scam arises at the point the customer transfers the funds to ‘another person’. The initial ‘me to me’ payment would then be excluded and the subsequent transfer out to the fraudster would (subject to other exclusions) be in scope. We acknowledge this may lead to a potential lack of protection in cases where the customer transfers funds by FP to a crypto or FX wallet held in their own name. However, there is little justification for holding the sending PSP liable for a loss arising from an onward transfer of the funds facilitated at another firm, over which it has no control or visibility. In our view, risks and losses arising outside of the payment scheme cannot fairly be underwritten by its participants.

#### 4.16 50:50 default allocation of repatriated funds between sending and receiving PSPs

We agree that allocation of repatriated funds should mirror the default allocation for reimbursement. However, to provide legal certainty to PSPs, the sending PSP assessing the claim would have to obtain confirmation from the customer that they are waiving their right to any repatriated funds up to the reimbursement amount. The practice for the SF seeking such customer declarations (and, where applicable, the receiving PSP seeking NCA consent to enable repatriation) should also then be standardised across the industry under the tailored criteria envisaged by the PSR, and of course obtaining this may delay the 48-hour threshold for reimbursement.

The establishment of this criteria would also provide an opportunity to standardise and embed an industry-wide methodology for allocating co-mingled scam proceeds between multiple victims.

#### 4.17 Rules on allocating the costs of mandatory reimbursement

The proposal to apply uniformly across all relevant firms is appropriate.

#### 4.18 Long-term vision, and rationale for PSO being responsible for mitigating fraud?

Overall, it's NBS' view that it is reasonable for Pay.UK to develop its strategic outlook as the primary interbank Payment System Operator with scam protections in mind

For APP scam reimbursement specifically, NBS envisages a governance model in the long term in which Pay.UK runs the operating standards and the rules of participation, with disputes and insights feeding into a continuous cycle of development. Strategically, this approach could lever the proven skills of Pay.UK in creating standards and maximise the emerging opportunities that Pay.UK is supporting and exploring – these include pre-transaction data sharing of standardised risk factors via APIs between the sending and receiving PSPs. In addition, Pay.UK's focus on APP scams includes an ambition to develop Transaction Data Analytics leveraging the intelligence (and Artificial Intelligence) capabilities of specialist vendors. Plus, Pay.UK's engineering of the New Payments Architecture affords a real opportunity to exploit the benefits of enhanced data (via ISO 20022 standards) in making the actual payment transactions more secure.

We do not see fundamental barriers to the scope of standards and rules being extended to include indirect participants, supported by their sponsors. Nor should there be barrier to applying common standards and rules primarily associated with Faster Payments to CHAPS and 'on us' payments, in a similar way to our current application of CoP.

#### 4.19 Minimum initial set of Faster Payments scheme rules needed

There should be more clarity over the application of the CRM Code post implementation as the scope and substance of the PSR's proposals are not the same as the CRM. For example, there must be clarity on which parts of the CRM will cease to apply, to which payments, and by when. We recognise the Lending Standards Board (LSB) must enact these changes but anticipate they will want to achieve the same goals as the PSR,. The recent MOU between the PSR and LSB will help here.

In particular, the relationship between the code and these proposals must be clearly defined.

If the code were to remain in full for CHAPS (which is not in scope of PSRs proposals) this would create disparity of assessment over different payment types which is not favourable and might not achieve an increase in consumer protections (see Q3).

Specifically: the minimum rules PSR proposes for Faster Payments would enable those payments to be reimbursed against the desired principles but would not address all the related matters consumers require, in order to be treated consistently across firms and across payment types.

#### 4.20 How to exercise powers under FSBRA to implement our requirements

We are of the view that it is quite reasonable for the PSO, Pay.UK, to build the functionality to design, build and implement the rules - with connections to UKF's industry data in their BPS system - and to develop suitable enforcement capabilities, with possible regulatory escalation.

#### 4.21 How allocation criteria and dispute resolution arrangements are developed and implemented

The development of a framework for these principles was a goal of the CRM implementation which has not fully materialised. It is unclear how the PSR's proposal will achieve the consensus described in 7.9 as being left to Pay.UK, which in turn could be delegated to industry. If so, industry has struggled historically to define these, so it may be necessary for PSR to, or require the PSO to, define such criteria.

They are noted in 7.13 as covering the relative contribution of PSPs to the scam but the extent to which a process can determine this in a short investigation timeframe will be dependent on the criteria being very clear and not open to interpretation. This may inevitably lead to them being a 'high bar' that is rarely utilised.

As a minimum, the early production period should have some form of close and continuous oversight activity that produces insights on operational experience with recommendations for improvement in the reimbursement model. The Best Practice Standards (BPS) platform run by UK Finance may be the optimal post scam information sharing system as it has c90% of UK retail payment accounts.

#### 4.22 Short-term implementation approach, Pay.UK to implement compliance monitoring regime

The PSR acknowledges Pay.UK may currently lack the capacity and capability for effective monitoring. NBS would want to see a monitoring regime in place to ensure effective implementation and reporting on compliance.

The PSR might consider in conjunction with UKF and Pay.UK if the BPS system might serve as a compliance monitoring platform to be further developed and to feed into an overseeing body. That body may need to evolve over time and should have appropriate powers of enforcement – so it may be that in the short term the PSR monitors performance as the longer-term options are considered, including Pay.UK as the overseeing monitor and enforcer of compliance as we suggest in earlier comments.

#### 4.23 Costs and benefits of Pay.UK implementing a real-time compliance monitoring system

As above, we have commented that monitoring and insights are crucial to the development of an effective approach to the reimbursement of APP scams. Not only will this prompt iterative learning and continuous improvement it may also inform the need for, and design of, a disputes process. However, the PSR needs to work with Pay.UK and industry participants to work out an optimal approach – overengineering at an early stage may be counter-productive. For example, the PSR's proposals include a suggestion for disputes around the 50:50 allocation to be, in effect, escalated for review in near real time – this may not be practical or efficient, certainly in the foundational phase of this process.

#### 4.24 Option for short-term enforcement arrangements

Embedding enforcement into the arrangements for Payment System Operator to ensure compliance should be the long-term goal. At the moment, it is likely Pay.UK would not be ready. This does not preclude implementation of the framework across PSPs, and a foundational compliance monitoring regime which later matures, perhaps ideally being integrated into Pay.UK but spanning relevant payment types elsewhere including CHAPS and 'on us' payments.

Currently, there is a scattered dispersal of monitoring and compliance and this has partly hampered efficient development on APP scam reimbursement so far (involving various bodies, including the Lending Standards Board, PSR, FCA, FOS). The next steps before a long-term governance model may need more analysis – we



welcome the opportunity to work with the PSR on options and expect the PSR (supported by UK Finance, Pay.UK and PSPs) could play a role in coordinating the early evolution.

#### 4.25 Best way to apply the rules on reimbursement to indirect participants

Overall, NBS feels scheme rules are more agile and appropriate than regulatory directions here but there are issues to work through including the application across other relevant payment systems and across indirect participants as well as their direct sponsors.

If the PSR's perspective sees the FPS rules applying at the level of the payment transactions then some of the obvious issues to work through include responsibilities being clearly demarcated between the indirect and sponsoring PSPs, and compliance be reasonably adjusted if, for example, an indirect participant had an operating model that in reality could not align with a 48-hour turnaround and presented low risk (such as a non 24/7 operation offering payments only to nominated destinations).

The PSR needs to guard against unintended consequences here – such as barriers to entry and competition in the market and possibly credit risk if there is any expectation that indirect access providers or sponsoring banks are expected to mobilise reimbursement and settle later with their indirect customer PSP.

#### 4.26 Whether we should direct indirect PSPs or IAPs

NBS is not a sponsor offering indirect access provision to the clearing systems but feel it appropriate that standards, rules and if necessary, any direction should reflect where the scam could be prevented, via warnings, education, or fraud detection. Direct sponsoring PSPs will need to develop the relevant processes within their contractual arrangements with their indirect customers, but the PSR should recognise there may be variations in the practicalities where some indirect PSPs may have operating models that are limit their processing of Faster Payments and other relevant transactions.

#### 4.27 Cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?

The PSR should specifically assess whether the prevention of scams has been influenced significantly by these measures, as well as reimbursement being increased as part of any post implementation review (which will likely occur and benefit consumers and provide more incentive for prevention in industry). 7.39 notes scam rates as a 'performance' measure but (as we pointed out in our consultation response to CP21/10) this metric – if used as a success measure – may be heavily influenced by payment traffic and mask whether absolute scam levels are being managed better or worse.

Other success criteria should be developed for prevention assessment.

The PIR must also assess each factor of the implementation and each assumption separately and against clearly defined criteria, such as the increased friction consumers may see and whether a lack of guidance on gross negligence or scope issues have prevented a high-quality implementation. Whether this should be arrived at via a submission of views, or via a form of independent monitoring may depend on whether Pay.UK's monitoring regime is mature and can address most aspects of such a review.

#### 4.28 Other comments on the proposals in this consultation

We would reiterate our firm view that a significant change in the prevention of APP scams is most reliant on the progress of industry data sharing, which does not have a clear plan at present. Additionally, the government must address the responsibilities and regulatory tools available to appropriately influence more prevention at upstream scam facilitators, such as social media platforms, telcos, and ISPs, to fully protect consumers and the industry from these crimes.

The power of data in APP scam prevention must be a key focus for 2023. This should include both UK Finance’s proposals around pre-transaction sharing of standardised risk factors exchanged via trusted API network in high-risk cases and the leveraging of Transaction Data Analytics in Pay.UK’s fraud overlay initiative by innovative vendors drawing on the predictive power of disbursement data hosted by Pay.UK and augmented with AI/machine learning etc.

## 5. Conclusion

In conclusion, prior to the proposed changes being initiated, we believe that all parties involved would benefit from more specific, sharper standards, and clear leadership in preparation for an effective implementation.

Importantly, the PSR should continue to influence HM Treasury to reflect the need for upstream facilitator accountability and inclusion of other industries within the defined reimbursement framework, in order to ensure the best possible consumer experience and avoid scams from being initiated in the first place. Alongside the active progression of industry data-sharing which is absolutely key to prevention success.

We believe there would be significant benefit to all participants from simplification, and this comes from defined standards, guidance, and consistency in implementation across all participants.

\*\*\*\*\* **END** \*\*\*\*\*



Natwest

# PSR CP22/4 Consultation Response

## FINAL Ver 1.01

NatWest welcomes the opportunity to respond to the consultation on Mandatory Reimbursement for APP scams. The implications of the proposed changes are far reaching and we have given this a great deal of thought. Whilst the 50:50 reimbursement model and the inclusion of all PSPs are in our view welcome proposals, there are a number of key elements of the proposals that NatWest does not agree with, including but not limited to the following headline points:

- The use of Gross Negligence sets the bar too high and introduces the risk of moral hazard
- 48 hours to reimburse consumers is not practical and causes further unintended consequences
- Pay.UK readiness is key to a successful industry implementation - it is critical this is well considered through a detailed planning phase to avoid any phased roll out
- NatWest strongly advocates an industry wide consistent upper limit as well as a revised lower limit for consumer claims to further constrain the risk of moral hazard

Additionally, we have set out an alternative view of how we think funds could be repatriated to incentivise receiving banks.

Full details of these points alongside all the others are set out in the responses below and we will of course be available to clarify and discuss any points raised.

## 1. Do you have views on the impact of our proposals on consumers?

NatWest<sup>1</sup> (NW) believes that the broadest possible market participation is key to fighting financial crime. Our response to Consultation CP21/10 stated our view that it was important that all Payment Service Providers (PSPs) were required to participate in a refund model to ensure that consumers were offered a consistent approach to scam refunds regardless of where they chose to bank. We welcome the proposal to include all Faster Payments participants, both direct and indirect, as a consumer benefit.

You state that your proposals should lead to more genuine payments being stopped and we agree that the proposals could lead to a detrimental impact on customer service. Payment delays are an effective means of preventing financial crime and well targeted delays should be supported as an indirect consumer benefit. We have contributed to industry discussions on Risk Based Delays to Payments, seeking greater clarity around the length of time a payment may be delayed when there are reasonable suspicions of financial crime.

We also stated our view in response to CP21/10 that there were already incentives for Contingent Reimbursement Model (CRM) code signatories to invest heavily in their systems and controls to prevent financial crime.

We welcome the incentive the proposals will bring to non-code members to do the same, which should lead to enhanced consumer protection. However, we note that these steps alone will not prevent consumers from being exposed to harm. Prevention must be considered on a wider scale than a PSP's role in payment journeys. We expand on this view in our responses to subsequent questions.

We strongly believe that a mandatory refund could potentially lead to consumer harm, as criminals seek to exploit consumers who may spend irresponsibly under the protection of a mandatory refund.

Customers must be required to exercise due care and attention and more should be done to consider how and when a customer has contributed to their loss. We expand on this view in our responses to subsequent questions.

There is the chance that APP scams will increase in the coming months as consumers seek ways to improve their finances during the forecasted cost of living crisis. Mandatory refund could lead to an increase in scams, as criminals seek to exploit the increased number of customers who may be eligible for a refund from their provider.

We have already seen a worrying increase in the reported volume of card scams across the industry, with losses in the region of █████ p.a. and growing. This is an area we would ask the PSR to look into as we should anticipate migration of fraudulent activity as the defences in APP scam prevention are enhanced across all participants. Current card scheme rules are predominately focused on unauthorised fraud and we consider they need to adapt to the emerging trend in card scams. We are also engaging with card scheme relationships leads on this.

---

<sup>1</sup> NatWest refers to our three brands (NatWest, RBS and Ulster Bank which subscribe to the CRMs code)

Fraud is currently the most reported crime in England and Wales and the volume of APP in that cohort continues to increase. The level of police resource targeted towards reducing fraud is not commensurate with the harm it causes.

There is a risk too that mandatory refunds lead fraud to be seen as a victimless crime and that this could, in turn, lead to a further de-prioritisation of fraud.

Mandatory refunds are not the solution to the fraud epidemic. The introduction of a revised scheme must be accompanied by strong guidance issued via the Government or the PSR, supplemented by awareness campaigns on social media channels, that informs the public of their rights and responsibilities, and that signposts how they can avoid many of the risks that still remain. All parties, regulatory, industry and social media firms, have a role to play in keeping customer safe from scams.

## 2. Do you have views on the impact of our proposals on PSPs?

NW is supportive of elements of the proposals, such as increasing the number of participants in the fraud refund ecosystem and plans to share the liability for refunds on a 50-50 basis.

The key to ensuring a smooth operating rhythm on the running of this within the industry will be the ability to have simple, repeatable processes between Sending and Receiving PSPs – with time built into the planning phase to test this widely. It will be critical to have simple SLAs and or strict time limits to the various elements of the process with exceptions managed via a central body such as Pay.UK or UK Finance.

We believe that mandatory shared liability will deliver a clear incentive for firms to improve their financial crime prevention tools. Broadening the number of PSPs who are in scope for the proposals will also help to protect the wider fraud ecosystem as criminals will have fewer soft targets to attack. These changes should deliver benefits to customers, firms and the ecosystem.

There are, however, a number of questions around the implementation of the proposals and we believe further discussion is needed in advance of delivery.

For example, there is a lack of clarity around how the changes will be applied to direct and indirect participants. Two of the three options outlined in the consultation may force us into a quasi-regulatory role over our indirect participants or could require us to make changes to our indirect access contracts. We acknowledge that the proposals may also lead some firms to raise concerns around the competitive impact on the market through prudential or innovation risks.

There is also a lack of detail around how the refund process will be administered. For it to be effective, the design must focus on it being simple, repeatable, and bound within strict time limits so that direct and indirect participants can operationalize the process.

Participant banks to the CRM code expend considerable time and cost in recovering and resolving claims from receiving banks. These costs will likely increase as more resource is required to process the projected uplift in eligible cases. Current tools may not be automatically effective or transferable to new participants into an expanded process. The cost of participation may also prove prohibitive to current or future participants, stifling competition and innovation in the market.

We believe that the proposed requirement for refunds within 48 hours fails to recognise the challenges that firms have in determining the validity of a scam. NW currently refunds █████ of scams within 48 hours. However there remains a volume of cases that require further investigation such as civil disputes, as noted in your proposals. We recommend this timescale is extended to allow firms to reach the correct outcome for customers and to protect the ecosystem against abuse.

We recognise there may be a need for dispute resolution, however we believe that this must be reserved for the most material of cases to avoid the scheme being burdened with vexatious cases. Clear rules, such as minimum claim levels, must be agreed by all in advance.

There are also questions around the role Pay.UK will play in the administration and oversight of the new process and of their capacity to fulfil this new role in a timely way to support the PSR's

expectations, and on their capacity to fulfil that role in the timescales set out in the Financial Services and Markets Bill (FSMB).

Delivering a process to a timetable that does not appropriately recognise the difficulties participants will face in administering it risks destabilising the entire venture.

We believe that further clarity is needed on these and other questions to fully assess the impact the proposals will have on PSPs. These issues must be fully considered in advance of any implementation timescale being agreed.

We address these issues in more detail in our responses to subsequent questions.

### 3. Do you have views on the scope we propose for our requirements on reimbursement?

NW is supportive of plans to broaden the scope of reimbursement to all PSPs once the scheme is in place as per our comments in the answers above. A phased implementation should be rejected in favour of an extended delivery timescale

We are also supportive of the proposed claimant definitions. It is right that larger business payers rely on robust internal controls to prevent losses.

We would also welcome consideration of whether certain scam types should be excluded from payers, for example romance scams from micro-enterprises or charities. In these circumstances a legitimate question could be raised around this loss being as a result of misappropriation of funds by an employee rather than a scam. The same is true where a consumer willingly and knowingly enters into a Ponzi or Pyramid scheme, doing so at their own risk.

We believe more clarity is required on how a Sending Bank would be expected to notify a Receiving Bank regarding a payment made by a customer outside of the scope of protection. We believe it is reasonable to expect that a Receiving Bank will take steps to secure funds for recovery in accordance with the rules agreed for 50% liability.

We welcome the suggestion that the rules would only apply to APP scams where the most recent payment was authorised after the new regulatory rules come into force. Customers who are unknowingly in the process of being scammed should benefit from the new protections once they become aware of their loss. We are also in favour of preventing retrospective losses from being considered individually and via Claims Management Companies who may seek to benefit from the revised rulebook.

We are supportive of a civil dispute exemption, although we will provide further comments in our responses to subsequent questions on how these should be defined, and the challenges firms will face in identifying a civil dispute within 48 hours. The distinction from purchase scams is particularly important in this regard.

We acknowledge the definition of an APP scam provided in the FSMB, however we believe the new process should have a more granular definition that sets out how multigenerational scams are considered and the scope of coverage over payment innovations such as Open Banking and the growth of e-wallet services. In particular, we agree with the UK Finance position that the definition of an APP scam should be limited to specifically one generation, i.e., the payment that places in the funds in control of the criminal.

For example, where does the liability lie in a bank impersonation scenario where the victim is scammed into opening an account in their own name with a new provider? If funds move from their account at Bank A to the new account at Bank B, we assume that Bank A doesn't hold any liability over the subsequent movement of funds from Bank B.

The growth in scams being sent to e-wallet providers also requires a specific response in the rules. Where does the liability lie for a payment sent to an e-wallet in the customer's name that is

subsequently sent on as an interbank payment or via an exchange to a criminal? Will the new process consider funds sent to an account set up and controlled by the criminal on the customer's behalf that are subsequently moved by the criminal via unauthorised fraud rather than a scam?

All of these payments can be said to have been executed "subsequent to fraud or dishonesty", yet there are questions around who should be considered the sending bank. Any rule set that extends to direct and indirect participants must deliver absolute clarity on liability.

We believe that in circumstances where a consumer sends monies to an account held in their own name, the receiving bank should be considered the sending bank for any subsequent movement of funds initiated under their controls and subject to their authorisation and therefore liable to refund the customer. The volume of payments, and resultant false positives, between accounts in the customer's own name at two different institutions is simply too high for the first bank in the chain (i.e. Bank A in example above) to assume liability – it is common for customers to move large volumes and sums between accounts in their own name genuinely, whether it be movement of funds to higher interest-bearing accounts or movement of salary to a bill paying account. This is particularly true where new market entrants are the new normal meaning customers are increasingly opening multiple accounts in their name with various institutions.

We note your comments regarding low value payments. We will discuss our concerns with your proposed approach in answers to subsequent questions.



#### 4. Do you have comments on our proposals:

- that there should be a consumer caution exception to mandatory reimbursement
- to use gross negligence as the consumer caution exception
- not to provide additional guidance on gross negligence?

NW agrees that there needs to be a consumer caution exception to mandatory reimbursement. NW disagrees that gross negligence, as it is today, is a suitable consumer exception caution principle. The term gross negligence remains undefined and untested in law, to the point that different PSPs will interpret the term in a multitude of ways, leading to inconsistent outcomes for consumers depending on who they bank with. The reason there are different interpretations is that the difference between negligence and gross negligence is one of degree only and goes beyond a person simply failing to exercise proper care.

For these reasons, we would strongly request that either an alternative standard to gross negligence is defined or that the PSR provides more meaningful guidance on it. If the latter, we would expect the PSR to consult on this. In outline, we would expect this guidance to provide clear steps that a consumer could reasonably be expected to take for each of the different scam types that are currently recognised and reported, per UK Finance definitions. These steps should be straightforward for all firms to assess and implement, ensuring consistency in consumer outcomes.

If the aim of the PSR is to reduce the occurrence of APP scams, NW believes that consumers need to have an incentive to protect themselves against all values of APP scams. Without a requisite level of care, we are concerned that consumers will take less care than needed to protect themselves, particularly when making lower value purchases. This is currently driving an increase in APP scam volumes (low value claims are already the dominant driver of volume).

We agree with the PSR that there is limited evidence one way or the other to accurately forecast consumer risk aversion where there is a wholesale expectation of reimbursement. We would also agree with the principle that consumers do not want to fall victim to scams due to the emotional distress but remain concerned that a wholesale reimbursement expectation without consequence will drive the wrong consumer behaviour. At the very least, it is fair to say that wholesale reimbursement will not make the problem any better which should be the primary intent of those involved in the ecosystem, including consumers. This is particularly true for low value purchase scams (even in excess of the £100 threshold) where it stands to reason that consumers will be less risk averse if they believe they will be reimbursed for their loss where it goes wrong. These also happen to be the toughest APP scams for PSPs to prevent due to the volume of genuine payments. We note recent comments from the House of Lords citing<sup>2</sup>:

*“399. Reimbursing victims cannot be seen as the primary focus of counter-fraud policy, yet it is a fundamental part of securing justice for victims. While we recognise the case for mandatory reimbursement of victims of APP fraud, we are concerned that a blanket reimbursement policy may lead to increased levels of moral hazard and fraud, and the perception that it is a ‘victimless crime’. In some cases, it may even lead directly to new*

---

<sup>2</sup> House of Lords publication - Fighting Fraud: Breaking the chain  
<https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/8703.htm>

*avenues for APP-reimbursement frauds. We also recognise how much banks have done to reimburse their customers. However, banks are the last link in the fraud chain and cannot be expected to foot the fraud bill alone. Furthermore, the inconsistency in the application of the CRM code across the sector demonstrates the need for uniformity*

*400. The Government must revise its proposals to legislate to allow the PSR to mandate blanket reimbursement of APP fraud conducted via Faster Payments. The Committee suggests that further exploration on the long and short-term risks of this approach is required and recommends that the Government seek a solution that achieves a level playing field for all customers.*

*401. To incentivise companies to act on fraud and more accurately reflect the balance of responsibility for fraud, the Government must establish a mechanism by which fraud-enabling sectors—in addition to the outgoing and recipient PSP—are required to contribute to the costs of reimbursement in cases where their platforms and services helped to facilitate the fraud. In making these changes, the Government must ensure that these reforms do not complicate the victims’ experience of reimbursement; they should retain a single point of contact.”*

On a daily basis, NW is dealing with cases where consumers are making payments directly to unknown 3rd parties (without using traditional online payment methods) for goods that they have never seen with no guarantee that the goods will be delivered. Despite detailed and specific warnings which are presented to customers as part of the payment journey, customers proceed to make payments at risk. Going forward, we anticipate that consumers will set aside any caution knowing that the Bank will act as a financial ‘back stop’ if things go wrong. Financial institutions alone cannot and should not be the insurance policy against unnecessary risk taking.

Low value payments are incredibly hard for banks to profile due to the number of genuine payments of similar values, and for this reason NW believes that purchase scams should be excluded from the Regulations, subject to a minimum threshold which we would suggest is considerably higher than £100. NW data shows that the average NW purchase scam value 2022 YTD is [REDACTED] therefore NW proposes a minimum threshold of [REDACTED]

Another scam type where NW believes consumer caution needs to be explicit and a lower bar than gross negligence is investment scams. In these scenarios, the customer is motivated by the opportunity to increase the value of their wealth rather than action out of fear of losing their money. In a non-fraud scenario, we would reasonably expect a consumer to consider the risks of losing their investment given that the value of investments can go up as well as down and to consider the feasibility and soundness of the investment, perhaps by taking independent financial advice and investing with a regulated firm. We find in a large proportion of investment scam cases that consumers have failed to undertake even basic due diligence on the investment opportunity presented to them and are instead motivated by unrealistic claims of high yield returns on investments, including investment with unregulated firms. The PSR should consider whether investments with unregulated entities are to be included as part of the reimbursement proposals.

Any consumer caution exception needs to be supported by clear expectations on consumers that can be applied consistently across PSPs to drive consistent outcomes for consumers regardless of

who they bank with – a good example of an exception may be where the consumer is a multiple victim of the same APP scam type (or very similar), and the PSP can evidence strong education given to the victim – should PSPs continue to reimburse in these circumstances? If yes, there needs to be due consideration to the downstream impacts whereby PSPs will likely need to take risk based decisions to limit their ongoing exposure.

We provide the following case study as an example of consumers taking undue risks:

[REDACTED]

This case illustrates the importance of putting a volume limit on the number of claims that a customer can bring under the revised regulations. The Bank would recommend that unless the customer is deemed to be vulnerable, a customer would be refunded under the revised regulations for the first case only, providing the customer is provided with specific and general customer awareness messaging.

As stated above consumer caution exception, regardless of the definition, needs to be applied consistently by all parties involved in a claim. As an example, the same standards need to be applied by PSPs at the first point of claim *and* by the Financial Ombudsman should the case require independent adjudication due to a disagreement in outcome. Any unwarranted departure by the Financial Ombudsman will only serve to undermine the rules set by the PSR.

Further to the points above we would also agree with the consensus view of Industry as outlined in the UK Finance response that gross negligence should not be the only exception for reimbursement. We would also advocate that

- consumer negligence determination should be simple, easily communicated and should evolve over time.
- If a customer's negligence has facilitated the successful completion of the scam payment, the customer reimbursement should be proportionally reduced.
- The cost of the remaining reimbursement would then be shared 50:50 by the sending and receiving PSPs.

## **5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

As referenced in our response to Q4, the proposed measure of gross negligence as a starting point to determine customer liability is unhelpful in the absence of a clear and workable definition, regardless of whether the consumer is deemed vulnerable or otherwise.

NW agrees that vulnerable customers (within reason) should be treated differently when considering consumer caution exceptions to reimbursement. We agree that vulnerable consumers may be more at risk from social engineering and scams with added complexity and less able to exercise caution and to protect themselves from APP scams. It is important though that vulnerability is not taken at face value as a reason to refund a customer. To be taken into consideration, NW strongly considers that a consumer's vulnerability should be relevant to the APP scam and their vulnerability meant that the customer was unable to reasonably exercise caution or protect themselves from an APP scam (in line with the existing CRM Code). Where appropriate, NW would expect to obtain and assess evidence of our customer's vulnerability before coming to a reimbursement decision to account for the potential for false claims.

## 6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?

NW understands the willingness of the PSR to reuse definitions of vulnerability where appropriate but does not agree that the existing FCA definition of vulnerability should apply in the case of APP scams. Instead, we feel it is important that vulnerability is taken in the context of the specific APP scam that the customer fell victim to in order to fairly assess a reimbursement claim. The existing CRM definition provides a better guide to vulnerability considerations in the relevant context.

*'A customer is vulnerable to APP scams if it would not be reasonable to expect that customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered.'*

We would request clarification on whether the term 'vulnerable' should apply to those running micro enterprises and charities. The Bank's view would be that the term should only apply to personal customers, sole traders and two-man partnerships but consideration needs to be given to differing rules for personal customers vs. business customers where we should expect a higher bar to apply for business customers. For example, the assumption should be that an individual involved in the processing of payments for a micro enterprise is capable of making informed and risk-based decisions. The standard should be included that a business would be expected to have in place systems and controls to validate payments, such as with invoice diversion or CEO scams, where we would expect the business to independently verify instructions received by email / WhatsApp / SMS. Where controls are in place within the business, we would expect them to be followed.

**7. Do you have comments on our proposals that:**

**-sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**

**-any 'excess' should be set at no more than £35**

**-PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

NW is not planning to implement an excess charge at this time, as it would introduce angst into a customer journey leading to increases in complaints from customers who have genuinely lost funds through APP scams. Furthermore, it is contrary to our Purpose of *Championing potential, helping people, families and businesses to thrive*. Additionally, the administrative costs of charging the excess are likely to be significant and eat into any saved losses.

However, it should be noted that we have no fundamental objection to a modest excess being implemented by other PSP's, noting that industry inconsistency should be avoided as this would cause consumer confusion and to that extent any excess should be at a consistent value. Furthermore, NW will continue to review this policy in line with the delivery of the scheme and market developments.

We believe that PSPs should be able to exempt vulnerable consumers from any excess applied.

**8. Do you have comments on our proposals that:**

**-sending PSPs should be allowed to set a minimum claim threshold**

**- any threshold should be set at no more than £100**

**-PSPs should be able to exempt vulnerable consumers from any threshold they set?**

NW would support the PSR implementing a minimum threshold and per our comments in Q4, we would advocate a minimum threshold of [REDACTED]. Any case reported under the minimum threshold would be at the PSPs discretion as to whether to reimburse the victim as a gesture of goodwill. Any minimum threshold would not apply to cases where a relevant vulnerability is identified (see response to Q5 & Q6). Consumers should still be encouraged to report cases under this value to ensure a clear understanding of scale and to enable intelligence sharing between PSPs, i.e., to identify mule accounts to which the scam was paid and enable network analysis across the industry. It also provides an opportunity for funds recovery should funds remain in the beneficiary account. For these reasons, we would caution that any minimum should be consistent across all PSPs who choose to implement it to reduce consumer confusion.

NW would propose that this threshold is reviewed periodically in line with the delivery of the scheme and market developments.

## 9. Do you have comments on our proposal not to have a maximum threshold?

Given that consumer claims under these proposals would be for the total value of all transactions linked to an APP scam (and not at an individual transaction level) we strongly disagree with not having a maximum threshold.

Despite strongly believing that to serve consumers in the market, PSPs should be readily equipped with stringent fraud protections, we also recognise that some smaller PSPs could be severely financially impacted if either no maximum, or a maximum level that was too high, is adopted. Getting this wrong could ultimately lead to unintended consumer disruption if impacted PSPs were to go out of business.

Our suggestion is to implement a suitable maximum claim that captures the majority volume of cases and that this should be [REDACTED]. As per the guidance on minimum values any implemented value should be consistently applied across industry for consistent consumer messaging and understanding.

Claims above this level could be taken on a case by case basis by the PSP but should not be mandatory.



## **10. Do you have comments on our proposals that:**

**-sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**

**- any time-limit should be set at no less than 13 months?**

NW agrees that there should be some element of time-limit for claims to be considered for mandatory reimbursement. However, we would suggest that the time-limit principle needs to carefully consider at what point the time-limit begins and when it should be applied from for newly reported cases post enactment of the PSR rules.

NW suggests that the wider reimbursement rules take effect from the point of the PSR mandates changes on how APP cases are handled. The new regime would therefore apply to cases where the final payment towards the scam was made from day 1 onwards. If the new regime is in place from 1st January 2024, any scam reports where the last payment was made from 1st January 2024 would be in scope.

Furthermore, we would suggest that where the case has previously been reported (i.e., prior to the PSR's proposed changes) and a decision has been reached with the customer, these cases should not be reopened.

NW also proposes that a consistent 13-month time-limit should be applied from the point that a customer makes the last payment to the criminal. This will serve to drive consistency in consumer understanding but more broadly consistency in how PSPs handle claims generally.

If sending PSPs take a decision to reimburse for longer dated / linked transactions beyond 13 months at their discretion, the 50:50 liability split would only apply to those transactions undertaken within the 13-month timeframe and not beyond. Whilst NW appreciates that these decisions are subject to individual PSP risk appetite, the complexity of such an approach needs to be carefully considered.

## 11. Do you have comments on our proposals that:

### - the sending PSP is responsible for reimbursing the consumer

NW agrees that the victim's bank should be responsible for reimbursing the customer in the first instance. The allocation from the receiving bank to the sending bank in line with the 50/50 allocation should follow thereafter. That said, there needs to be consistently applied rules of engagement between sending and receiving PSPs including periodic assurance to ensure accurate reimbursement settlements are being delivered.

There are two suggested routes that could be taken to manage or oversee the reimbursements.

- i) Under the CRM Code, banks expend a great deal of operational resource chasing outstanding funds or matching unlabelled reimbursement payments back to the underlying victim. Having spoken to UK Finance and members, we believe that a BPS style system could be developed that would calculate the amount owed by each bank at the end of an accounting period (week or month), with the inbuilt capability to provide a clear view on the values that are attributable to individual cases.
- ii) Equally a 'straight through' process could be adopted to avoid a month end backlog being administered.

The thinking on this process needs to be carefully undertaken and NW would welcome feeding into a pre implementation phase to help develop this critical element to the implementation.

### **-reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

NW agrees that reimbursements should be as soon as possible but strongly disagrees that 48 hours is a reasonable timeframe in which to investigate and make a decision on reimbursement. We would suggest that we maintain the existing 15 business day investigation timescale (35 business days in exceptional circumstances) under the CRM code and refund within 48 hours from the point a liability decision has been made, except where safeguarding measures need to be put in place.

The PSR's proposal for a 48-hour refund timeline, does not reflect the fact that:

- The Bank often requires additional information or evidence from the customer. Obtaining this information can take longer than 48 hours.
- In some cases, particularly purchase scams and investment scams, it can be difficult to quickly assess whether a case is an APP Scam or a civil dispute. To resolve this may require engagement with the Receiving Bank and the Receiving Bank may in turn need to speak to their customer. These cases may take considerably longer than 48 hours.
- 48 hours is not considered sufficient to assess a customer's vulnerability, establish gross Negligence or eliminate First Party Fraud.

NW endeavours to deal with all cases as soon as practicable, and currently refunds █████ of all cases within 48 hours. NW proposes that the CRM timescales should apply at the outset, and once the PSR's proposed changes have been embedded, timescales should be reviewed after 12 months.

## **12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

### **Evidential standard:**

- The evidential standard should be that the PSP has a reasonable belief that the customer is attempting fraud or has been grossly negligent (or any alternative adopted, as we set out in our comments above) and therefore requires additional time to investigate further before coming to a decision. This reasonableness test will ensure PSPs are not simply able to delay the decision without good cause but does not set the bar inappropriately high given the short timeframe (whether 48 hours or something longer) and the complexity of many APP scams.
- For customer fraud, the PSR should not carry across the obligation on PSPs to file an Internal Money Laundering Suspicion Report (IMLSR) or Suspicious Activity Report (SAR) before delaying a refund. This requirement does not make sense where a customer is attempting to commit fraud by obtaining a refund and does not then have criminal property in their account.
- Fraud is a predicate offence, not a money laundering offence under POCA – a money laundering offence will only take place if the customer successfully receives the refund and deals with funds in their account. The requirement to file and trigger an IMLSR/SAR is where the PSP suspects a money laundering offence (that someone else is “engaged in money laundering”), which will not yet be the case. Given this, making POCA reporting a pre-condition to withholding an up-front refund is inappropriate and could encourage PSPs to submit incorrect, low-value SARs to the NCA.

### **Timeline to investigate:**

- As we refer to elsewhere, although for more straightforward cases a shorter, a default period may be appropriate. For most cases and in particular those that are more complex cases, an extended period is required to investigate the case as the timelines in the CRM and PSRs (for complaints) set out.

### **Customer engagement:**

- In all cases, the rules should make clear that customers need to engage in a timely, open and honest way with reasonable requests from their PSP for information relating to the scam; there should be no expectation of a refund after either the initial period (whether 2 days or longer) or a longer investigation period without this engagement.
- PSPs would need to give customers a proper opportunity to respond – it would not, for example, be appropriate to refuse a refund at the end of the initial period (assuming it is not a much longer period) where a PSP sent a letter to the customer after the fraud report and has not received an answer in time.

### **13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

NW agrees with the principle of 50:50 default allocation. As suggested in our answer to question 11, there needs to be an agreed set of standards and a mechanism to assess and reconcile reimbursement costs between sending and receiving PSPs. NW believe this should be a centrally managed and assured mechanism that enables PSPs to seamlessly raise claims and reconcile. Having discussed this with UK Finance, we believe that the existing BPS system could be repurposed for this. However, we do feel that the system requirements need to be thought through carefully to ensure that claims and claim refunds are captured in real time, with the capability for each case to be tracked individually.

We agree that there need to be strong incentives for Receiving banks to improve standards. This can be tangible with investment in near real time inbound payment profiling and allocating resources to investigate alerts and to suspend funds where there are grounds for suspicion awaiting contact with the sending bank. As outlined in our response to Q16 we would strongly recommend that receiving bank liability is determined giving allowance for effort to suspend and repatriate funds to the sending bank, i.e. receiving bank liability (loss) can be mitigated by offsetting funds frozen and repatriated.

We would make a point on the dynamic of the indirect PSP proposals where, depending on the option selected, it might see NW take on a quasi-regulatory role over our indirect participants, when due diligence to prevent and therefore reconciliation should lie with the indirect PSP, which is best able to assess its own liability. This should not be a role for the direct PSPs to manage on their behalf, recognising that this may cause complexity for some providers.

We support the PSR's proposal (a) to give a direction to all indirect PSPs to comply with the reimbursement rules in Faster Payments. We do not though support the PSRs proposal (b) to give a direction to indirect access providers (IAPs) to ensure transactions by their indirect PSP customers comply with the reimbursement rules in Faster Payments or to (c) the Faster Payments rules on reimbursement being applied to all transactions, making the IAP responsible for the transactions of its indirect PSP customers.

If scheme rules are introduced with upper and lower value thresholds and or time limits on claim periods, a sending bank may choose to reimburse their customer on a good will basis. We would recommend that any goodwill reimbursements i.e. outside scheme requirements would not fall within the 50:50 liability model although the receiving bank should be notified of the potential mule account. Furthermore, we would suggest that the PSR should consider how goodwill settlement cases should be reported and any consequences for performance tables.

We will consider whether it is necessary to update our indirect access contracts. As reimbursement will be a directed obligation for an indirect PSP to adhere to, we do not consider this as an indirect access service, but a direct scheme obligation on an indirect PSP. If the PSR direction on indirect PSPs is not the selected option, then we will review what may be required by way of contract change.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

Whilst recognising the overall intentions of a dispute resolution process the better option would be a very clearly articulated set of criteria agreed alongside the capability to centrally administer such cases efficiently, fairly and consistently.

NW supports the premise of the default 50:50 split on reimbursements and considers that for the scheme to work efficiently any deviation from this default would need:

- to be on a by exception basis only
- to avoid the risk of a significant volume of low value disputes that would not help serve customers efficiently we would recommend some basic principles such as a Minimum dispute claim level of [REDACTED]
- The central administrator would need to be fully established and tested well ahead of the overall proposals being implemented
- Any disputes would also need clear tracking principles to be implemented.

## **15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

We need to be clear what the PSR means when referring to multi-generation scams. These can sometimes refer to a situation where a family member has been convinced by a fraudster to make a payment but does not have the means to do this and requests a family member to send the money for them.

Then there is the more usual type of multi-generational scam, where someone makes a payment to a fraudster and the money is moved on in several separate payments to mule accounts, which then transfer the funds to other accounts in smaller amounts. These payments are difficult to follow, and it would be difficult to incorporate this complexity into a scheme rule.

The current proposal is that the focus should be on the payment where the customer is scammed. Here the proposed new process would be followed by the sending and receiving PSPs. For the onward payments, the receiving PSP may be able to recover further funds, and these would offset some or all of its loss.

The PSR's example of a two-stage payment, with only the second one seeing the customer pay funds away, is not typical of most multi-generational scams.

If Pay.UK were to develop a procedural approach to developing the scheme rules/procedures, it would be possible in time, with engagement of the fraud community to develop more detailed rules/procedures which reflect this situation and potentially others that may occur in future.

We would expect that Pay.UK will seek feedback from both the payments and fraud communities on the development of the rules/procedures to ensure that the scheme rules allow sufficient future clarity and flexibility to adapt as scam types evolve.

## 16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?

We do not agree with the proposal to share recovered repatriated funds equally between sending and receiving banks and build on our comments in response to Q13.

We would ask the PSR to consider that a receiving bank's 50% liability should comprise;

- (a) the value of funds protected (suspended) or recovered and available for repatriation, with
- (b) the residual value up to 50% of the APP claim taken as a loss.

If the receiving bank is successful in freezing funds in excess of 50% of the scam payment(s), the value over 50% would be repatriated to the sending bank.

To illustrate with an example, we envisage the process could work as follows;

- (1) Sending bank notifies receiving bank of APP scam £10,000 promptly and that customer has no liability. Claims 50% from the Receiving bank £5,000.
- (2) Receiving bank has managed to secure £3000 due to inbound / outbound profiling and manual intervention.
- (3) Receiving bank remits £5000 as settlement comprising funds frozen £3000 (at the RB's risk) and a liability payment for £2000.

In this example, if the receiving bank secured £8000, i.e. in excess of £5000 (50%) the excess amount £3000, would also be repatriated to the sending bank together with the £5000 as the liability share.

Our rationale for this approach follows;

**Investment and Resource Allocation** - The PSR's principle that the "scheme" must "incentivise PSPs to do more to prevent APP scams, whether as a sending or receiving Bank/PSP" is well founded. We also strongly support a 50:50 liability model, despite this being a blunt approach which does not consider the varying degrees of investment and resources receiving PSPs apply to profile, suspend and investigate inbound payments assessed as being high risk. Nor does it consider the effort some PSPs undertake to recover 2<sup>nd</sup>, 3<sup>rd</sup> generation funds. This effort is evident from our data on funds recovered and repatriated across the sector by receiving PSPs and indeed in our relative performance as a receiving bank.

**Stick and Carrot Incentives** - The PSR's incentive as drafted is a "stick" approach where the "carrot" would be for PSPs to mitigate liability by improving performance in funds recovery / repatriated. A 1% improvement in funds recovered prevents c£6m of loss to the industry / customers and importantly prevents £6m of funds reaching criminal gangs.

**Manage mule risk through account life cycle** - This approach would also incentivise PSPs to consider the risk of mule activity through the account management life cycle. It is a misconception that mule accounts exist and operate because of weak onboarding / KYC controls. This is a factor, but a larger proportion of mule activity occurs through genuine accounts, taken over by criminals or through

witting or unwitting customer involvement. PSPs should have some opportunity to directly mitigate receiving bank liability / loss throughout the account lifecycle.

**Disincentive and fairness?** - Sharing proceeds of repatriation may be seen as a disincentive to invest and prioritise resources on inbound profiling, i.e. Bank A recovers and repatriates 25% of scam proceeds, Bank B only 5%.

**Recognise risk taken by Receiving bank through repatriation** - Funds are recovered and repatriated to the sending bank typically without any indemnity. If the receiving bank beneficiary account customer subsequently makes a claim or complaint the receiving bank has to manage the risk / loss.

**Consequential harm to society** - focussing on reimbursement has failed to reduce the growth in funds reaching criminal gangs and the consequential harm to society. Providing a tangible positive incentive to protect / repatriate funds recovery will reduce consequential harm.

PSPs would have to consider POCA requirements with this model but manage these issues today under the CRM.



## **17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We fully support the proposal that 50:50 allocation of the costs of reimbursement extends to all direct and indirect PSP participants. As described in the consultation paper we agree this is essential so that all PSPs are equally incentivised to prevent APP scams. We must avoid a repeat of the displacement / migration of criminal activity to several non-CRM Code PSPs which was seen when the voluntary CRM Code was launched.

Sponsor banks may have a role to play in supporting questions from their indirect PSPs on how they have adopted the necessary procedures and by sharing best practice on scam management. Indirect PSPs may offer different or limited propositions and have good anti-fraud practices in place which they can adapt as needed. The approach to allocation of costs will also impact indirect PSPs and act as an incentive for some to invest more in their procedures and processes.

We agree with the PSR that the rules on allocating the costs of reimbursement should apply equally to all directly and indirectly connected PSP participants sending and receiving payments over Faster Payments, although there may be PSP models where this is more impactful, such as for e-money institutions where funds are held for safeguarding to make a payment. The PSR will need to assess the feedback it receives. All PSPs should act to detect and prevent APP scams.

## **18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

We agree in principle that in the longer term Pay.UK as the system operator should be capable of undertaking the role of making, refining, monitoring, and enforcing compliance with scheme rules that address fraud risks in the system. We understand that Pay.UK is currently in the early phase of building this capability. PSR is also aware that Pay.UK has two significant delivery programmes to manage – NPA (New Payments Architecture) delivery and transition, plus the CoP (Confirmation of Payee) expansion project. Both are planned to be in transition or complete by end 2024/early 2025.

Realistically, unless Pay.UK can demonstrate to both the PSR and direct and indirect participants that they can effectively take on this additional significant role earlier, we support PSR's view that it is more appropriate to defer Pay.UK taking this on fully, until appropriate Pay.UK resource is in place and participants are familiar with the new reimbursement arrangements.

NW does not support a staged adoption by direct and indirect participants as this will lead to consumer and industry confusion and will add unnecessary complexity to the process. We understand that the PSR does not favour a phased approach. We believe that the options the PSR has proposed will support adoption by all participant types, although accepting that those not used to the current processes may take some time to adopt and adapt to them. We also envisage that this will avoid a move of fraud to those firms covered by the scheme rules.

The benefit of all participants going live at the same time will help to ensure consumers are aware of their added protection through firm and consumer body communications and offers an opportunity for participants to reinforce how consumers can protect themselves from being scammed.

PSR's proposal for a separate supporting document containing the criteria for allocation of reimbursement costs in support of dispute resolution arrangement has merit. It does raise the question of why the PSR has not proposed Pay.UK to lead the work on this, particularly if dispute resolution is also to fall under its remit. We suggest the PSR provides clarity on this.

Faster Payment scheme documentation is already split into formal agreements between direct participants and the scheme company, together with separate detailed documents that sit under them for certain service elements, such as Credit Payment Recovery. This could be a suitable option for the APP scam reimbursement rules and procedures and the document could be made available to fraud specialists at both direct and indirect participants.

As we have stated in response to question four, it is crucial that any new rules are applied consistently and any unwarranted departure from the accepted interpretations by the Financial Ombudsman will only serve to undermine the rules.

## **19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

We support the PSR's view that as much as possible, its ambition for comprehensive scheme rules on APP scam reimbursement should be achieved from the outset. PSR will need to work closely with Pay.UK to understand what is achievable.

NW's view is that if Pay.UK can only amend its rules to incorporate APP scam victim reimbursement covering direct participants, PSR may need to direct all indirect participants to comply with the Faster Payment reimbursement rules at the same time. Pay.UK will need to develop these rules in a format which can be made available to both direct and indirect participants (please refer to our response to Q18).

We believe it would be inappropriate for a direct participant to take on PSR reporting for its indirect participants. We also believe that the majority of our indirect participant customers would prefer to undertake this themselves.

## **20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We agree that FSBRA Section 55 contains relevant authority for the PSR under 55 (1) (b) to change the Faster Payment rules in a specified way, to achieve a specified purpose.

It remains debatable however whether changing the rules to apply directive requirements on firms to deal with APP scams is something which could have been anticipated as an expectation of a payment system operator when FSBRA was enacted. We assume that the PSR expects the FSM Bill enactment to give it sufficient powers and authority to require Pay.UK to amend both the procedural and scheme rules to achieve the desired outcome.

## **21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

It is imperative that the allocation criteria and any dispute resolution arrangements are ready well in advance of Day 1 of the implementation of these proposed changes. We would advocate utilising Industry bodies such as UK Finance to help co-ordinate industry thoughts on the detailed allocation criteria arrangements.

To re-emphasise previous responses above, NW supports a dispute resolution process provided it is clear, simple, centrally administered and on a by exception basis. NW would be happy to provide further thought on the details of how this might work as part of the pre-implementation phase.

## **22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

NW agrees that an effective compliance monitoring regime is crucial to the success of the PSR's proposals. The regime should include independent oversight of compliance with the reimbursement requirements, the application and assessment of a consumer standard and SLAs for reimbursement. The regime should include identification of any areas requiring improvement as well as providing an insights function that would serve to share trends, good practice, provide guidance and support evolution of requirements. Furthermore, this would provide an opportunity to have an independent single source of truth on data to enable consistent reporting.

Whilst NW appreciates the difficulty and timeliness of introducing such a system of compliance, we would suggest that it needs to be as close to the definitive version for go-live of the requirements as possible. It will be important to ensure there is reporting consistency and collaboration between PSR's and Pay.UK's data to develop the reporting requirements would support this.

Given the potential complexity of what may need to be monitored, it may be necessary for there to be a trial run of data to allow issues and errors to be removed before formal reporting begins. We would also like to see a review of the data after an agreed period to ensure it is delivering aligned data, and to report to firms on the insights that it is providing, and which may lead to firms needed to take action to improve performance or show the improvements in recovery and reimbursement hoped for.

Finally, noting the aspiration in the consultation to reimburse victims within 48 hours and the existing reporting requirements due mid-2023, PSPs focus should be on delivering the outcomes of the requirements and not diverted to another reporting requirement

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

As suggested in our answer to question 11, there needs to be an agreed set of standards and mechanism to assess and reconcile reimbursement costs between sending and receiving PSPs. NW believes this should be a centrally managed and assured mechanism that enables PSPs to seamlessly raise claims and reconcile periodically. Having discussed this with UK Finance, we believe that the existing BPS system could potentially be repurposed for this.

## **24. Do you have views on the best option for short-term enforcement arrangements?**

Pay.UK appears to be the only viable option, however we are concerned that they do not have the resources or expertise to deliver a credible oversight and insights function given the existing commitment to deliver the NPA.



## 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?

Our view is that all PSPs should be accountable for managing APP scam risks from both a sending and receiving PSP perspective. This means that both direct and indirect PSPs should be responsible for their own performance on reimbursement.

If the PSR is comfortable that Pay.UK has the capability and resource to incorporate reimbursement into the Faster Payment rulebook (see our response to Q18), and oversee its operation, with a PSR direction to achieve this, if necessary, we think this is the simplest option.

We do not agree with the proposal that the PSR would ask indirect access providers (IAPs) to ensure transactions by their indirect PSP customers comply with the reimbursement rules in Faster Payments. This would create a high overhead and would see IAPs intervening in the business activity of both an IPSP client and a competitor institution.

The alternative of requiring the IPSP to commission an annual audit of its reimbursement activity and to provide this to its IAP, might be seen by IPSPs as intrusive, and may also be disproportionate for smaller IPSPs. The proposal that IAPs would include the requirement on IPSPs in an amendment to their indirect access contract seems unnecessary if the IPSPs are directed to adhere to the new scheme rules.

We do not believe that it should form part of an IPSP's indirect access service provider role to monitor its indirect PSPs adherence to the reimbursement rules. This needs to come either from a PSR direction or the Faster Payment rule change covering indirect PSPs.

We also note the PSR's comment in 7.34 on the provision of transaction data to IPSPs. We agree this is essential and support our IPSPs with timely data. The PSR needs to be mindful of the different capabilities of IPSPs to receive data, based on their technology capability.

In 7.32 the PSR notes that the rules will apply to all FPS transactions. This is sensible, but the extent of fraud impacting Standing Order and future dated payments will be lower than that of single immediate payments. It will also be necessary to revisit this once the NPA is live and the proposed new payment types are introduced

## **26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

If it were necessary to direct firms, logically this would cover only IPSPs which are not bound by scheme rules. Any direction should incorporate clear guidance on what is required of firms.

As we say in our response to Q25 we do not consider it appropriate to direct IAPs to ensure transactions by their indirect PSP customers comply with the reimbursement rules in Faster Payments. This would be difficult to do, as we would not have sight of which transactions sent by an IPSP might be an APP scam, nor how well they dealt with the reimbursement process.

If a complaint were to be made against an IPSP which we sponsored into the Faster Payments scheme, where Pay.UK needed to inform us of a reimbursement issue with one of our IPSPs, we would raise this with them. We do not see a requirement to direct an IAP to do this, unless PSR believes it needs to be made visible to the IPSPs.

We would prefer however for Pay.UK to be given adequate powers to achieve delivery of the reimbursement objective for both direct and indirect PSPs and be able to enforce this.

An IAPs role is to support its IPSPs to send and receive payments. We see reimbursement of APP scam frauds as separate and distinct activity which the IPSP must be accountable for.

## **27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

It is evident that all parties across the industry are keen to reduce APP scams, however NW is not convinced on the £100- £150m of projected savings per annum outlined in the consultation paper.

Looking at the various elements of the reimbursement journey NW suggests:

- despite these proposals consumers are not any less likely to become a victim of a scam;
- the CRM banks have been signed up to a voluntarily reimbursement model for c3 years since the CRM implementation. This constitutes most of the faster payment traffic but APP scams in this time have increased across the industry despite the fact there has been significant investment in fraud protections during that period.

The proposals should however lead to a tightening up of controls especially by Receiving PSPs, including the strengthening of mule account defences, leading to an overall net benefit across industry.



# Open Finance Association

## Authorised push payment (APP) scams: Requiring reimbursement

### Open Finance Association (OFA) response to the Payment Systems Regulator (PSR)

#### About the Open Finance Association (OFA)

The OFA represents companies focused on empowering consumers and businesses to access account data and make safe and secure payments through open APIs (application programming interfaces). We represent the open finance providers and users of open finance. Our members include:

- Armalytix
- Crezco
- Nuapay
- FinAPI
- GoCardless
- Ordo
- Plaid
- Token
- TrueLayer
- Volt
- Worldpay
- Worldline
- Yapily

#### Summary

We welcome the opportunity to respond to the PSR's consultation on APP scams. APP scams can have a devastating impact on victims' lives and we recognise the urgent need to tackle the issue. OFA is fully supportive of the drivers to provide an appropriate level of consumer protection. However, as the consultation paper focuses on liability between banks, we have not responded to individual questions but instead highlighted areas for further consideration by the PSR.

We believe that the adoption of open banking payments by business and consumers will itself be an effective countermeasure to APP scams because open banking payments tackle the root causes of APP scams inherent in manual bank transfers.

However, we also believe the PSR's APP scam proposals, as they are currently formulated, put the viability of open banking at risk for the following reasons:

- **De-risking:** Open banking companies already struggle with banks limiting and blocking legitimate open banking payments. Imposing further liability on banks will reduce banks' risk appetites, leading to further limiting and blocking of legitimate open banking payments, and make open banking untenable as a payment option (removing a potential competitor to cards).

- **User experience** - even where banks do not block open banking payments, the current proposals are likely to incentivise banks to introduce additional friction in instant payment journeys (including those initiated by open banking), such as more screens, 'pop up' warnings and/or verification steps for consumers when authenticating payments.
- **Cost of faster payments** - It is likely that the proposed APP scam measures will increase costs for sending and receiving banks (e.g. costs of managing disputes and FOS escalations). These will be passed onto merchants in the form of charges for receiving faster payments. This will make open banking an unattractive option for merchants, because the costs to receive faster payments via open banking will be greater than the cost to receive card payments.

We do not think that there has been sufficient consideration of these impacts of the APP scam proposals on open banking payments, evidenced by the fact that the only reference to payment initiation services in the consultation is a single, undefined footnote at section 4.6.

The PSR has rightly recognised that open banking has *"the clear potential to facilitate account-to-account payments for retail transactions and compete with card systems."*<sup>1</sup> Without further consideration, for the reasons set out above, OFA are concerned the PSR's APP scam proposals present a significant risk to this potential and to the PSR realising its objectives in this space.

### **Proposals:**

Before the PSR implements any final rules, the OFA would ask it to:

1. Explicitly recognise the security benefits of open banking payments and **consider how to support the adoption of open banking payments as an alternative to manual bank transfers and as a countermeasure to APP fraud.**
2. **Conduct a separate cost benefit analysis of its APP scam proposals in light of the impact they could have on open banking payments,** and the detrimental downstream impact this could have on the PSR's work to promote competition from A2ART for card payments.
3. **Delay the implementation of any changes to liability until more data has been collected on whether existing APP scam measures (CoP and CRM) are working.**
  - We note that the latest UK Finance half-year APP fraud statistics (H1'22) showed — for the first time — a significant year-on-year reduction in APP fraud in both volume (-6%) and value (-17%) terms. Although undoubtedly still high in absolute terms, directionally this suggests that existing measures are beginning to have an impact on APP fraud and more time is required to assess their full impact.

---

<sup>1</sup> <https://www.psr.org.uk/our-work/account-to-account-payments/>

4. **Consider whether measures are necessary to ensure banks take liability for blocking legitimate PISP-initiated payments - and compensating end users appropriately - unless they are able to provide clear evidence for the decision.**
  - At the moment, banks carry no burden of proof for declining transactions of any nature and are under no obligation to explain their action even when challenged with specific evidence supporting the legitimacy of a payment. However, consumers may incur financial damage by a payment not completing, for example if they miss a deadline (such as HMRC's tax return deadline). We believe consumers should be compensated in situations when they experience a materially adverse financial impact from a payment not completing (i.e. it should not be compensation purely for the inconvenience caused).

In addition, we note the proposal at section 6.7 of the consultation indicating the PSR's expectation that Pay.UK will *'establish, maintain and enforce cross-market arrangements on PSPs' conduct in a number of areas, including as part of its role in assessing and enabling use cases for the NPA, such as open banking account-to-account retail transactions.'*

5. More clarity is needed from the PSR on what is meant by this, and how it interplays with discussions under the Joint Regulatory Oversight Committee (JROC) to develop a future entity to oversee open banking standards. **The Open Finance Association strongly believes that standards relating to open banking providers should be the responsibility of the future open banking entity, not Pay.UK.**

**The OFA recently responded to the Strategic Working Group (SWG) process informing JROC's work on the future of Open Banking in the UK. We believe one of the recommendations we made in that process could be relevant to assisting with mitigating APP scams:**

6. **We recommend that the Open Banking Implementation Entity (OBIE) or successor entity coordinate the mandatory implementation of transaction risk indicators (TRIs) so that receiving institutions can use them to assist risk-based decisions in a meaningful way.**

### **Further detail**

#### **Why open banking payments can counteract APP fraud**

Open Banking payments to merchants are an inherently safer way to pay than other forms of payment, especially manual bank transfers, which are the main vector for APP scams. The way open banking payments are set-up addresses the risks of APP fraud because:

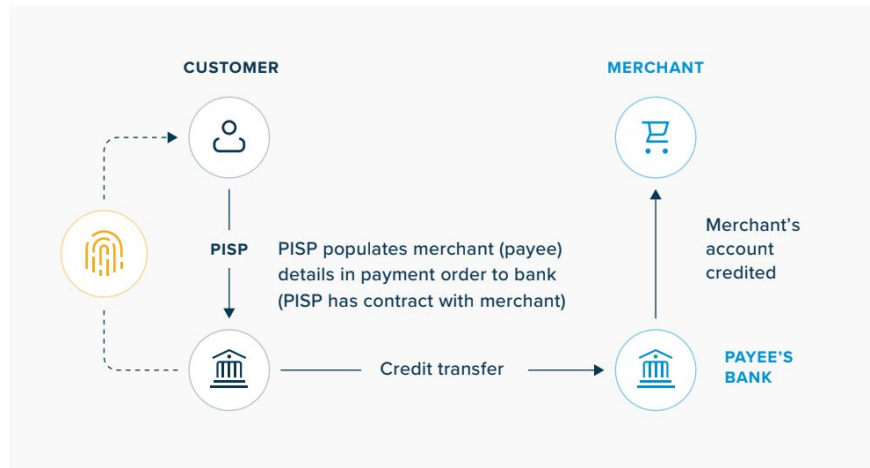
- **Open banking providers onboard and carry out due diligence with the payee -** When an open banking provider enables payments for a business, they enter into an ongoing commercial contract with that business, and undertake due diligence on the business as part of that. This reduces the likelihood that the beneficiary of an open banking payment will be used for fraud. In the unlikely event that fraud occurs, the open banking provider can immediately raise this with their client (the beneficiary).



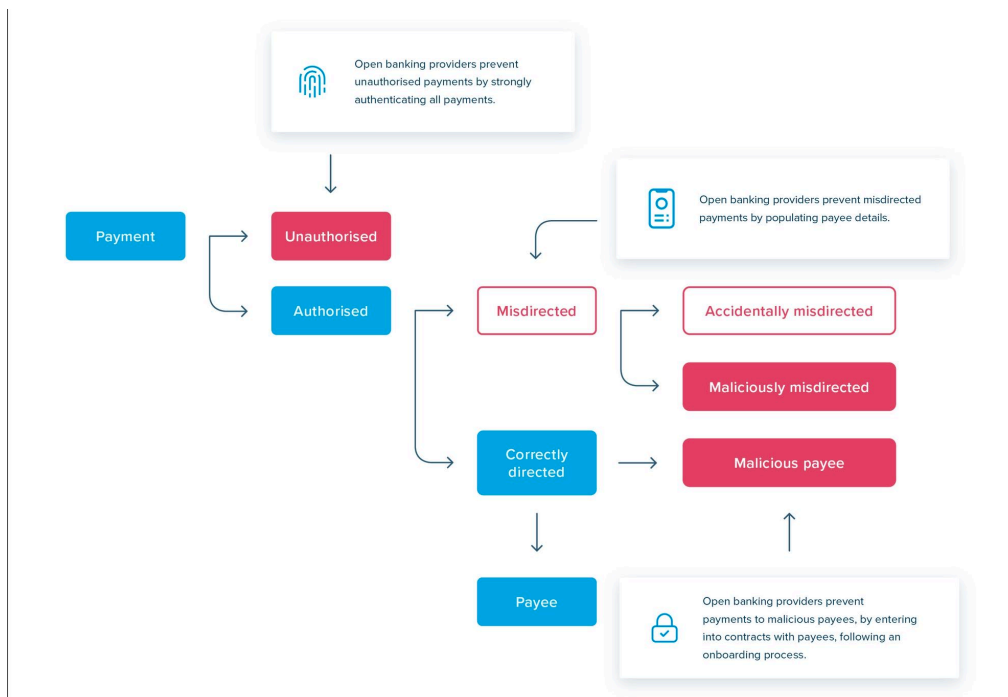
- **Payee details (sort code and account number) are pre-populated by the open banking provider, removing the possibility of human error** when typing payee details or customers being tricked into sending money to an account controlled by a fraudster. The beneficiary's name is also presented back to the payer by the payer's banks in the authentication journey.

Fig. 3

Open banking payment to merchant: open banking provider populates the merchant's account details



How open banking prevents fraud (including APP fraud):



This is why the Open Banking Implementation Entity (OBIE) noted last year that, “the risk of APP fraud in Merchant Initiation via PISP is **exceptionally low**”<sup>2</sup> (emphasis added).

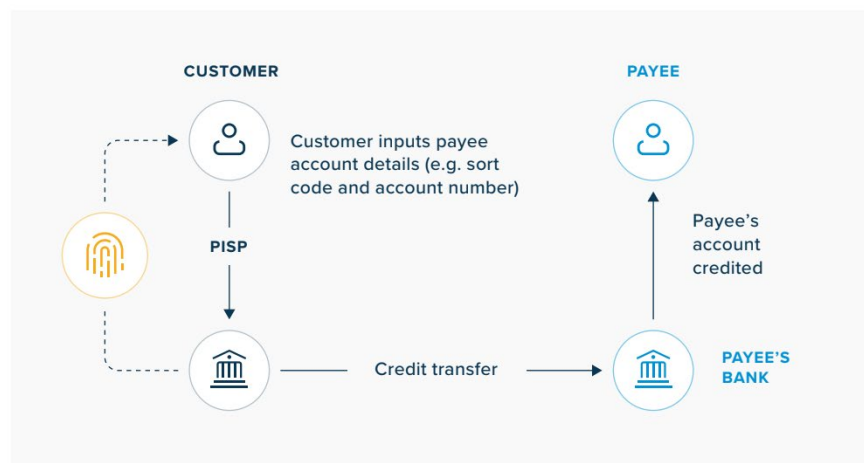
<sup>2</sup> Open Banking, [A2\(d\) - Open Banking Standards Relating to Confirmation of Payee and Contingent Reimbursement Model Code: Consultation Document](#), 2021

Indeed, OFA believes that as open banking payments replace manual bank transfers in day-to-day life, APP fraud will continue to decrease and customers will start to see manual bank transfers as less convenient and less secure. In short, customer uptake of open banking will further reduce the risk of customers being involved in APP scams.

### Do all open banking payments reduce the risk of APP fraud?

Open banking payments can be used in a similar way to manual bank transfers in what are known as 'party-to-party' use cases. In this use case, the consumer (rather than the PISP) populates the payee details which means they could potentially be manipulated into entering the wrong details. However, this use case is increasingly rare ([Yolt Pay](#) enabled this, with Yolt Pay, but has since closed down).

Fig. 2 |  
Open banking payment  
where consumer inputs  
recipient details



### How does a bank know if an open banking payment is low risk of APP fraud or not?

Parties across the open banking ecosystem already apply a risk-based approach to open banking payments. For example, banks in monitoring transactions for high risk factors, and TPPs conducting due diligence on the businesses they offer services to.

There are, however, changes in open banking standards that could be made that would enhance the risk-based approaches applied by open banking ecosystem players.

Current OBIE standards enable PISPs to send 'payment context codes' (PCCs) to banks, which allows them to understand the risk profile of a payment. For example, a PISP can tag a payment with an 'Ecommerce' code if the payment is to a merchant, or 'party-to-party' if the consumer is using the PISP to make a payment to another account of their choosing, such as paying a friend.

The latest version of the OBIE standard (3.1.10) has introduced more detailed transaction risk indicators (TRIs), which are supposed to give banks further information about the risk profile of payments, e.g.:

- **ContractPresentIndicator** - Indicates if the Payee has a contractual relationship with the PISP (the thinking being that if a PISP has a contract with the beneficiary they will have undertaken due diligence, lowering the risk of any payments to the beneficiary).
- **BeneficiaryPrepopulatedIndicator** - Indicates if a PISP has immutably pre-populated payment details in for the PSU (the thinking being that if a PISP rather than the consumer has populated the payee details, the payment will not be vulnerable to APP fraud).

However, the implementation of these TRIs and PCCs is voluntary and is not being coordinated by the OBIE, leading to inconsistent and patchy implementation by both PISPs and banks. It risks the benefits of payment risk information not being realised and a continuation of arbitrary risk management by banks, leading to more PISP transactions being limited or blocked unnecessarily.

We recommend that the OBIE or future entity coordinate the mandatory implementation of TRIs so that receiving institutions can use them to assist risk-based decisions in a meaningful way.

### **De-risking**

It is important to highlight the implications the PSR's proposals for APP reimbursement may have on the development and adoption of Account to Account (A2A) Retail Transactions.

The PSR believe that A2A payments will increase choice for merchants and consumers and give an additional option for both POS and e-commerce transactions, however if the proposals for APP reimbursement were to set the benchmark for A2A this could significantly damage this proposed new payment option.

A 'reimburse first, investigate later' culture applied to A2A payments may mean that banks build such a robust and defensive economic model around them that they are unlikely to be economically appealing as a payment method. In open banking, this could manifest itself by banks blocking and limiting transactions initiated by PISPs to payees they perceive to be in higher risk sectors.

There is already evidence that banks are de-risking in the way that they are blocking payments for entire sectors. The payments sector has faced substantial derisking already in the remittance sector and this 'reimburse first, investigate later' approach will disproportionately impact another cohort of firms authorised under the Payment Services Regulations.

### **User friction**

We believe that the current proposals are likely to incentivise banks to introduce additional friction in instant payment journeys, such as more screens, 'pop up' warnings and/or verification steps for consumers when authenticating payments. This will damage the payer experience and reduce trust in Open Banking overall. The OBIE concluded last year for PISP-initiated payments, "[Confirmation of Payee and Contingent Reimbursement Model pop up] warning messages are of limited utility and that the resultant additional friction together with

*the incremental costs of deployment are not justified. Indeed, emerging evidence from our consumer research suggests that there would be positive benefits from eliminating the overuse of warning interventions; customer fatigue erodes their effectiveness.”<sup>3</sup>*

OFA members also believe there will be an increased propensity for banks to suspend payments for fraud checks and look to generally slow down the payment process. One approach for achieving this we are aware is being discussed is to introduce delays in high value faster payments transactions so that banks have more time to scrutinise payments. Whilst we are fully supportive of appropriate measures to mitigate fraud we are concerned that unnecessary and indiscriminate application of such friction will have a significant negative impact on open banking payment propositions.

It is also contrary to the direction of travel abroad; other jurisdictions are looking to introduce real-time payments rails because of the benefits to the economy they bring. For example, the EU Commission recently proposed a new Instant Payments Regulation with the intention of creating a system that can compete with the UK's Faster Payments System. Reducing the speed with which payments are settled via FPS could impact the UK's perceived and actual international competitiveness.

### **Cost of faster payments**

Changing the liability model for reimbursing APP scam losses may prompt ASPSPs to revisit the economic model they use for instant payments and e.g. increase charges to businesses for instant payments, or even consider introducing charges to consumers for sending or receiving Faster Payments.

Businesses are typically charged by their banks to receive Faster Payments into their bank account, with fees varying significantly and typically being lower for larger businesses (for example, one CMA9 bank offers tariffs charging £0.35 per incoming payment for businesses <£5m turnover and £0.15 for larger businesses). By comparison, when using card payments, low value transactions are typically charged on an ad valorem basis (i.e. percentage of transaction value). The BRC recently reported that merchants on average pay 26bps of turnover to accept debit cards (small merchants can pay significantly more than this). On an absolute basis this amounts to ~3p for a £10 sale.

This means that open banking payments are already uncompetitive with card payments at low values. The APP liability shifts could further exacerbate this problem and prevent open banking A2A payments from being a competitive constraint on card payments.

If you wish to discuss the OFA's response please do not hesitate to contact [openfinanceassociation@fticonsulting.com](mailto:openfinanceassociation@fticonsulting.com).

---

<sup>3</sup> Ibid

# Ordo



PSR Consultation:

APP Scams

Ordo response

Submission to: [appscams@psr.org.uk](mailto:appscams@psr.org.uk) by 5pm 25 November 2022

**PUBLIC**

*The following information is the property of The Smart Request Company Ltd, trading as Ordo (“Ordo”) and is provided to you in response to the above consultation only.*

*The information is only to be used by you in connection with the consideration of your response to authorised push payment fraud, it is not to be used by you for any other purpose. The **REDACTED** version only may be published in response to this consultation, without alteration.*

***This is the REDACTED version of our response and MAY be published.***

*The commission of any unauthorised act in relation to the information may result in civil or criminal actions being taken by Ordo in relation to this matter. Any licences issued by the Copyright Licensing Agency Limited do not extend to this matter. All opinions and forecasts contained herein are the opinions of Ordo and are made in good faith at the time of publishing.*

## Introduction

### What does Ordo do?

Ordo's fully hosted and customisable open banking-enabled payments managed services provide businesses – large and small – with low cost, highly secure, real-time and easy to use Request to Pay, e-commerce, Point of Sale/QR Code, invoice and contact centre payments direct from their customer's ASPSP accounts into their own ASPSP accounts for both single and recurring payments.

Businesses can access the Ordo managed service in a number of ways: through an Ordo Merchant Acquirer/PSP payments partner, such as Pay360 or Contis, directly via Ordo's business level APIs, and for smaller businesses, through our integrations with QuickBooks, Sage, and Xero accounting software or via Ordo's web/app interfaces.

Ordo also uses open banking to enable refunds and secure customer pay outs as well as account validation services and has fully managed VRP enabled services, initially for sweeping, allowing businesses to take advantage of the latest open banking technology with minimal development and integration effort.

Ordo's cloud hosted managed service is fully white labelled allowing business's own brand and look & feel to be incorporated into all customer interactions, giving a consistent customer experience but without the overhead of developing and keeping up to date their own open banking customer journey.

### Who are Ordo?

Ordo was founded by the former management team of the UK's Faster Payment Scheme in 2018 to use Open Banking payments to provide businesses with a much-needed alternative to slow, high-cost card payments and insecure direct ASPSP payments. Ordo is authorised by the Financial Conduct Authority as an Authorised Payments Institution to carry out Account Information Services and Payment Initiation Services (FRN 836070). Ordo is backed by private investors, Nationwide Building Society Ventures and CGI, the global IT services business.

## *Consultation response*

We are pleased to see the PSR consulting on APP scam liability and, particularly, altering the liability model from that which exists under the Contingent Reimbursement Model currently. Going hand in hand with the aim of reducing fraud is ensuring any regulatory interventions encourage and incentivise the right behaviour both from ASPSPs, but also enabling signalling to consumers to adopt more secure methods of payment, like Open Banking, that are available to them today.

### *50/50 liability proposal and consultation process*

Putting aside the role of law enforcement, there are only two parties that can potentially help consumers avoid falling victim to APP scams, the banks involved in sending money under the instruction of the victim and the banks receiving money on behalf of the criminal. As consumers have limited scope to reduce their risk of being defrauded, can be devastatingly affected by the financial losses they incur, and as banks have the greatest opportunity to stop fraudulent payments going to criminals, and greater financial scale to absorb losses on behalf of their customers in the short term, it makes sense to introduce a comprehensive bank funded reimbursement model to remove the financial consequences from consumers and incentivise banks to act to stop APP frauds.

Under the contingent reimbursement model, when reimbursement takes place, this is principally funded by the sending bank on the basis that this incentivises the sending bank to educate and support their customer into not making a payment to a criminal. Whilst this helps in less than half the cases and rarely to the full extent, it also encourages banks to effectively blame the victim for falling victim and be financially penalised (likely coupled with significant psychological detriment).

The PSR has taken on board the suggestion that the receiving bank may also have a role to play and has consequently proposed a 50/50 split of reimbursement funding from the sending and receiving bank. At one level this is welcomed, but simply spreading responsibility in this way on the one hand to be 'fair' to all parties, and on the other, to maximise the potential to stop frauds (belt and braces), while superficially attractive, fails to recognise that there are also consumer and business downsides associated with the steps banks could take to minimise APP fraud. As these actions come at a cost to banks and/or their customers, and could have negative unintended consequences, a more nuanced analysis needs to be undertaken before settling on an equal split of liability between the two banks involved.

To select the most appropriate liability split between the sending and receiving bank it is necessary to consider the information available to each party, the actions available to each party, and what actions the allocation of any liability will cause a party to take. It is not clear from the PSR's consultation that this has been done, and that a broad enough range of allocations has been considered, specifically allocating full liability to the receiving bank.

### *The sending bank's position*

The sending bank (victim's bank) only knows the history and payments patterns of its own customer, so while it may spot an APP scam payment as abnormal due to its size compared to normal payments from the customer, it is very likely to identify many false positives. The infrequent nature of high value consumer payments means that distinguishing between scam payments and legitimate payments (like paying for a car, paying for building work, or making an investment) is very hard for the sending bank due to the very limited information it has access to. Given the limited information available to it the only action available to the sending bank is to interrupt all higher value payments to new payees and seek information from the payer to try and detect a scam. Given the nature of the social engineering used to enable scams, and the fact that this process will have been successful if a customer is about to make a payment to a fraudster, the customer information gathering process can be lengthy and time consuming for both the bank and their customer. As long as the sending bank has some liability for reimbursing a scam payment, it will seek to minimise that liability by discouraging its customers from making such payments, whether scam or actually legitimate. This will continue to make account to account payments harder to execute and particularly get in the way of consumers making higher value Open Banking Payments. Sending banks will never be fans of customer or Open Banking initiated Faster Payments as the bank holds a liability it is not in a good position to mitigate, it



would much rather consumers continued to use cards where, not only is it insulated from liability, it earns significant revenue in the form of card issuer fees.

Putting another barrier in the adoption of open banking and other account to account payments reduces the chances of account to account competing with cards. This lack of competition will mean businesses will continue to pay higher costs for payments, costs ultimately borne by their customers. This is not in the public interest.

**To summarise. Sending banks bearing liability for APP scam payments to criminals can only reduce their exposure by trying to prevent their customers paying scammers. A significant side-effect of this action will be to interfere with and make much less attractive legitimate higher value payments forcing payments off high efficiency Faster Payments/NPA onto expensive card payments. The limited available information to sending banks makes false-positives very likely.**

#### *The receiving bank's position*

By contrast, the receiving bank (the criminal's bank) should have good and growing information about the receiving account, how it is being used, and what person or organisation is running the account. The receiving bank can spot in real time that an account has suddenly started receiving large payments that are inconsistent with the KYC'd purpose of the account, and through KYC should know whether the account is a personal or business account, and if business, what type of business. If the receiving account is a personal account, either opened by a criminal, or a mule account recruited by the criminal, then large receipts will be even easier to spot than large outgoings as they are even more unusual for consumers. The receiving bank also potentially has actions it can take that will mitigate scams, without making Faster Payments too hard to use.

Putting aside tipping-off rules (which might need adjustment or clarifying), the receiving bank, having spotted an unusual transaction could ringfence that transaction on receipt. It can then investigate what the account is being used for, protecting the payer's funds without interrupting the transaction flow and as is the case with sending bank false positives. The bank's enquiries will be focussed either on a criminal scammer/mule, or on a legitimate person or organisation that can easily provide an explanation to the bank for the transaction and then gain access to their funds. Banks already have a clear responsibility to know who their customers are, and what they are using their accounts for to stop Money Laundering.

This delayed availability of funds to a suspicious payee doesn't change the Faster Payments model. The payment has still been received irrevocably and the payee can rely on funds being available unless they are shown to be criminals, in which case they have no rights to the funds anyway and they can be costlessly reimbursed to the victim. If the payee is not a criminal, it is guaranteed that they will receive funds, just after a short delay, and therefore they can supply goods or services to their customer without risk prior to investigations being completed. This means that the impact on transaction flows and businesses and their customers of false positives at the receiving bank end is massively lower than false positives from the sending bank.

False positives will also in themselves be much less likely because the receiving bank has so much better information. The vast bulk of legitimate higher value payments are made to business bank accounts. The receiving bank naturally knowing whether the receiving account is personal or business means most higher value payments, which will go to business accounts, won't need to be reviewed. Higher value receipts into personal accounts can then be focussed on to interdict scam payments. While there will be some false positives, these will be very infrequent for consumers (consumers rarely receive higher value payments other than regular and predictable salary payments). Banks can then quickly contact their customer to establish their bona fides, and if still in doubt can consult the sending bank to validate the sender's comfort with making the payment. Over time, just as banks encourage their customers to notify them in advance of foreign or large card spends, consumers can be encouraged to notify their banks of unusually large receipts. These steps may indeed already be theoretically required of banks to meet their AML obligations.

**To summarise. Receiving banks bearing liability for APP scam payments to criminals (their account holders) can reduce their exposure by preventing criminals gaining access to funds paid into their, or their mule's bank account by ring-fencing suspicious receipts until the account holder has been validated. There are very limited down-sides**

**to businesses and their customers from false positives. The good KYC information available to receiving banks makes false-positives very unlikely for the majority of payments.**

Considering the situations of the sending and receiving banks in the round, we believe there is a very strong case to allocate liability for scam payments made to criminals wholly to the receiving bank and not share any of this with the sending bank:

- It is very hard to imagine a scam payment situation where the sending bank can identify it as suspicious, but the receiving bank cannot – there is little incremental benefit of both parties trying to spot suspicious payments.
- There are very limited downsides from receiving bank false positives, and very substantial downsides (including strategic undermining of account-to-account payments as competition to cards) from sending bank false positives – there is a substantial cost to the economy of sending banks also trying to spot all suspicious APP scam payments.

Full liability on the receiving bank will incentivise the *change in behaviour* that will stop fraud, not payments.

Our assumption in this proposed receiving bank liability model is that CoP (or functional alternatives such as presenting the payee account name to the payer prior to payment authorisation) is mandated for all banks, and where CoP is not used by a sending bank, this switches the liability model and makes sender bank 100% liable. The reasoning for this being the sender bank has not kept up with the latest widely available technology and adherence to best practice. This will incentivise ASPSPs to implement CoP, a service that does enable sending banks to reduce scam payments and misdirected payments without false positive downsides.

It is not clear from the consultation that the PSR has considered this model where 100% liability sits with the receiving bank. Given that for all scam payments, the receiving bank is operating an account for a criminal or a criminal mule and should be liable for this, this seems strange.

As a minimum, the 100% liability model on the receiving bank with its pros and cons needs to be fully laid out against the current (100% sender) and a 50/50 model if a good decision is to be made.

In our view, for any proposal to be robustly enforced, it must be evident broader thinking was carried out before reaching and consulting on a single proposal, and how such proposal best achieves desired outcomes.

At this stage, we cannot conclude this has been done or that the best model is being proposed.

### ***Mandatory reimbursement***

Ordo agrees with the PSR's proposals to mandate reimbursement in all cases but for gross negligence and where the payer is complicit in the fraud. Mandating all fraud (subject to high bar carve outs) supports the argument that this will incentivise *a change* in behaviour, certainly. As far as a change is desired, the PSR's proposal to mandate compensation of all APP scam fraud (carve outs accepted) satisfies that requirement.

### **Method of implementation and Pay.UK's role**

We agree that an appropriate place for implementing an APP scam liability model would be the Faster Payment Scheme rules. Consequently, and in line with the PSR's stated objectives of having a Payment Systems Operator that is motivated to minimise, and enforce prevention of, fraud, that Pay.UK be the body that enforces this framework and it be empowered to do so.

It is imperative that this expansion of Pay.UK's role in this instance, to be empowered to enforce the further prevention of fraud across the payment system that it runs, does not creep into governing, setting standards or frameworks or similar for services that operate extracted from its payment system and instead in the competitive layer of the payments ecosystem, the Open Banking TPP layer. Any governance at this level, regarding services and

TPPs who provide overlay services and do not touch clearing and settlement, must be governed by a wholly independent body, currently OBIE and what this will evolve into as the Future Entity.

### *PSR additional legislative powers required*

We suggest that whilst the PSR is obtaining its legislative powers to have authority to mandate compensation of all victims of APP Scams, it obtains the legislative authority for the following to enable it to function fully and well:

*CoP -*

We state above that we propose the 100% receiver ASPSP liability model be switched where there is an APP scam from a sending ASPSP that does not operate CoP or a functional alternative\*. This will drive more sending ASPSPs to adopt CoP, but it would also be prudent and in the interests of consumers that all levers are used, and the PSR having the power to mandate CoP on all ASPSPs for the good of society is another such lever.

Therefore, all ASPSPs need to support CoP as a sender or receiver of payments, to negate the defect of CoP today where eg First Direct can only perform a CoP check if the receiving ASPSP also supports CoP.

\* E.g., If a PISP presents a payer, via open banking, with the account name of the payee, that has been suitably sourced and validated by the PISP, then there is no incremental benefit to adding CoP to the process. Adding CoP in this circumstance simply complicates the customer journey for no good reason.

*'On us' payments -*

If the argument is accepted that a victim should be (apart from where high threshold exemptions have been exceeded) compensated, then it is illogical for there to be a gap where a payer has inadvertently sent money, in a scam, to an account at an ASPSP in the same banking group, or even the same banking brand!

The victim is unlikely and cannot be expected to know, and cannot be expected to investigate, the receiving account's banking group. If it's decided that it is appropriate for intergroup receiving ASPSPs to compensate victims, there is no difference to the entitlement of a victim sending money intragroup!

We note that the PSR states it expects compensation to victims for APP scams where the transfer has been 'on us' is to be treated the same as for transfers intergroup, but our view is that this is far too weak and leaves APP scam victims vulnerable to larger ASPSP group companies, the PSR needs to require this.

*Unintended consequences*

A consequence of actions ASPSPs take to limit their exposure to fraud as a result of mandating APP scam victim compensation is that it could cause fraudsters to move to using cheques. If ASPSPs have weaker controls with cheques than electronic payments, fraudsters will exploit those weaknesses. It should be noted that cheques already put liability on the receiving bank to check the name on the cheque matches the account name (as the paying bank can't control where funds are paid into) and therefore our 100% receiver proposal already has precedent. Therefore, any liability model regarding APP scams should also extend to cheques to ensure APP scams are reduced rather than just moved. (The threat does not transpose in the same way to the remaining payment methods: Bacs – consumers cannot make Bacs payments; Cash – cannot be traced; Cards – alternative compensation models).

### **Other PSR Consultation points:**

Subject to the above, we do not have dissenting views on the remainder of the proposals in the consultation.

Please do not hesitate to get in touch with the author, [REDACTED], should you wish to discuss further or have any questions.

Kind regards



Pay.UK



PSR CP22/4 APP  
scams: Requiring  
reimbursement -  
Pay.UK response

15/12/2022

Classification: Public



## A model for effective implementation

Pay.UK welcomes the steps taken by HMT to enable the PSR to define a mandatory reimbursement requirement, which will ensure victims of APP scams are not left out of pocket. If done well this, coupled with existing work across the industry on prevention and detection of scams, provides us all with an opportunity to make real progress to help address this urgent issue.

We want to support participants in our schemes to tackle fraud. As PSR are aware, we have a programme of activity underway to develop and roll-out prevention and detection tools, including the Enhanced Fraud Data project being taken forward by industry under PSR's Measure 2. We want to look at fraud prevention and mitigation across all our schemes, considering how we can leverage the NPA to deliver improvements.

We are also ready to play our role to support reimbursement for scams which result in FPS payments, which represent the highest volume of APP scams. We think that the design of the reimbursement requirement should be set by the public authorities. We will work with the PSR and the payment firms to put effective reimbursement arrangements in place for FPS payments as soon as possible. It will be key for the industry to work together to ensure an effective regime is implemented to the timelines set out by HMT and the PSR. We believe this can be achieved through the annexed model – which we are proposing as the most effective way to deliver the government and PSR's policy outcomes. We have engaged actively with PSR throughout 2022 and hope to continue that close working, along with the payments industry, in 2023.

In our response, we have referenced this proposed model which we have been exploring together, for the implementation of the PSR's proposed reimbursement requirements (this focuses on the “how” in the PSR consultation paper). We think this model can provide for effective reimbursement of consumers in a reasonable timeframe, given the urgent need to act. It needs to be tested with more stakeholders – especially payment service providers (PSPs) who will need to develop new processes and procedures – but our belief is that it could be progressed alongside existing plans to improve tools for prevention and detection, which the payments industry is keen to bring to delivery in 2023.

The model represents an evolution of our role - it provides for us to have new rules which bind our customers to outcomes in relation to their interaction with end-users. It also suggests that we would collect and monitor data from all relevant PSPs, not just our direct customers in our schemes or overlays. This would be enabled by PSR in its role to establish the liability framework and set the requirement on PSPs. It will be key for the PSR to be clear on what outcomes it wants to achieve, agreeing appropriate KPIs for monitoring, and undertaking ultimate enforcement through its regulatory powers. Implementation of the model will require close work with industry to ensure they have the relevant operational processes and guidance, supported by technology where needed, to meet their obligations. This is not a small task, but if everyone can get behind a model which builds on the existing powers, experience and competencies of different parties, then it should be possible to act swiftly for the benefit of consumers.

This consultation will gather views on Pay.UK's role in reimbursement and also PSR's long term vision for Pay.UK. We expect the PSR to give appropriate weight to Pay.UK's response when considering its role, capacity and powers in these areas, especially where there may be differing expectations from other stakeholders.



## Delivery of policy outcomes

The PSR has set out its desired outcomes from its proposals. We share the PSR's desire to reduce the number of APP scams and for consistent protection for consumers, regardless of their PSP. Further, we think victims of scams should be entitled to appropriate reimbursement regardless of the type of payment that the scammer requests, and it is therefore important to ensure the arrangements the public authorities put in place now for FPS are flexible and adaptable for the future. The importance of this point was recently underlined by our End-User Advisory Council.

We want to support PSPs' efforts to prevent customers making the payments that result from scams. We agree that these outcomes would prevent any potential erosion of confidence in FPS as a system, or in the payment instruments used to create FPS transfers. We support the public authorities putting in place requirements that will be effective in supporting these outcomes (in an equivalent way to the approach taken to unauthorised fraud).

There are aspects of some of the options discussed in the PSR's consultation that, if implemented, would not lead to an effective solution. However, we believe that these would all be addressed in the model that we have proposed and discussed with the PSR. Key to this is our view that the requirement to reimburse should be placed directly on to the firms responsible, which is most effectively done via a direction from PSR under Section 54 of FSBRA. This will achieve the most comprehensive coverage for the requirement. FPS rules can further bind those who are subject to them into this requirement, including more detail on the precise operational expectations.

Alongside the policy outcomes identified in your consultation, we also think our proposed model supports addressing the following issues – which we believe may arise with other options in the consultation - which we and other stakeholders consider to be important:

- Consistency for consumers
- Level playing field across payment providers
- Credible enforcement
- Management of legal risk to PSO and IAPs

The PSR should consider the market consequences of the proposals as part of its Cost Benefit Analysis, as advocated by our End User Advisory Council. (We appreciate the PSR having taken time to present and discuss its proposals at the EUAC).

## Disaggregating the implementation of an effective reimbursement regime from PSR's long term vision for Pay.UK

PSR's longer-term vision for Pay.UK merits discussion with us and other stakeholders in the round and is broader than APP scams. We are clear that it is important to disaggregate the discussions of the longer-term vision for Pay.UK now, in order not to jeopardise the delivery of an effective reimbursement model. We share some of the long-term ambitions of the PSR, but these are complex areas that will need to be worked through alongside our other priorities and in discussion with our regulators.

It is important that the decision on our role for the on-going design and enforcement aspects of the reimbursement regime should not be made until there has been an evaluation of the operation of the model: we therefore strongly support the PSR's proposed post implementation review.

## Next steps

To deliver this change in its role, Pay.UK will require the support from PSR in three main areas to:

1. ensure that Pay.UK has the necessary legal powers and protection to take on its responsibilities;
2. provide clear and specific guidance on the desired outcomes and expectation on Pay.UK for the PSR to ultimately review and approve; and
3. support the operational delivery with industry through its convening powers and ability to direct firms to deliver the desired outcomes.

In our proposed model, Pay.UK would work with industry to deliver the requirements. Alongside the introduction of new rules, this will involve substantial effort to develop the necessary operational processes and guidance, underpinned by standards and technology, to enable PSPs to deliver consistent reimbursement outcomes to consumers. Pay.UK will also lean in to provide data collection and monitoring, so that the effectiveness of the PSR's proposed requirement can be assessed, and action taken where firms are found to be falling short.

We recognise that the PSR's proposals will evolve through consultation and that and it is therefore important that our work and planning keeps aligned to PSR thinking and expectations of our role. As such we will want to continue the close engagement we have had this year with PSR, to support our business assessment and implementation planning.

# Responses to PSR questions

## 1. Do you have views on the impact of our proposals on consumers?

We welcome the intention to introduce mandatory reimbursement requirements. This, coupled with the existing work across the industry on prevention and detection of scams, should help to address the urgent issue of the level of harm done to consumers by these crimes. The payments industry can only intervene in an APP scam once the victim has decided to make a payment – we want to support those interventions to make them timelier and more effective. Consumers will benefit more from interventions earlier in the development of a scam, and we recognise that actions to address this are outside of the direct sphere of influence of PSR.

We agree there is an urgent need to act in relation to FPS, which sees the highest volume of payments resulting from APP scams: We are ready to play our role in implementation. We will work with the PSR and the industry to put effective reimbursement arrangements in place for FPS payments as soon as possible.

We continue to advocate that any reimbursement interventions need to be effective in the long term, and solutions should be comprehensive and consistent, for the benefit of consumers. There are consequences for consumers (and the market) of requiring reimbursement of FPS payments and not for other forms of payments. Having different levels of protections for different forms or channels of payments does not create a consistent basis for consumers to be reimbursed and could prove confusing for them and lead to further detriments for some consumers. The reimbursement requirement should be cast as widely as possible.

Consumers experience detriment not only when they lose funds through an APP scam, but merely by being a target of such fraud. We are concerned that fraudsters may target consumers who use FPS to make payments, in the hope that the reimbursement promise will cause consumers to be less vigilant and take less caution in their payments. This creates a risk of moral hazard and, even if a moral hazard does not materialise, the perception of one will bring a greater volume of attempts at fraud with the attendant distress for victims.

Our End-User Advisory Council<sup>1</sup> were keen that PSR should place more emphasis on prevention (rather than reimbursement) and should consider the risk that the cost and burden for reimbursement might be shared across FPS in such a way that is detrimental to the consumer and other end-users, such as small businesses. They also requested that any requirements should be broadened out, or retrofitted, to other payment methods to ensure consistent protections for consumers.

We agree with the PSR observation that an impact for consumers could be that they experience more delays or challenge from sending firms before payments are submitted and/or that funds may not immediately be applied to receiving accounts. Pay.UK does not have visibility of this aspect of the bank/customer relationship so PSR should give thought to how it could capture information from sending and receiving firms to measure the impact of its proposals in this regard.

---

<sup>1</sup> [End User Advisory Council - Pay.UK \(wearepay.uk\)](https://wearepay.uk)

## 2. Do you have views on the impact of our proposals on PSPs?

PSPs will be able to supply PSR with a better view of the financial and operational impact of these proposals on their business. We are cognisant that the implementation of the PSR's proposal will be a significant task for PSPs, and will have an operational impact in both implementation and then ongoing BAU. We are keen to support PSPs in this, through coordination, the introduction of operational processes and guidance, systems and automation of data reporting, as needed. This central work by Pay.UK will also require funding.

It is important to note that the same PSPs are also engaged in work to broaden participation in CoP, to introduce prevention and detection measures such as Enhanced Fraud Data and the Pay.UK Fraud Overlay project. We are also engaged heavily with industry on NPA development. We anticipate that there will need to be extensive discussions with industry about their capacity to support this implementation alongside existing commitments in 2023. We imagine this will be a focus for discussions in early 2023, ahead of the finalisation of PSR proposals.

There is a lack of clarity and analysis on the competition impact of the proposals. It will be important for the PSR to work through the impact on PSPs, in particular considering different business models. As LSB and others who are closely involved will most likely explain in their own responses, this is a learning from the initial formulation of the CRM Code, the design of which reportedly impacted on the ability for universal adoption and the further development of the Code.

It would be a concern for us if PSR's final proposals changed the incentives for PSPs to execute payments across FPS or if the cost of reimbursement were to materially affect pricing and access to payments across the board. This is something that needs more exploration by the PSR, to ensure that any unintended consequences of the proposals have been considered and mitigated to the extent possible.

## 3. Do you have views on the scope we propose for our requirements on reimbursement?

We recognise that the duty imposed on PSR in the Financial Services and Markets Bill applies only to scams that result in transfers across the Faster Payments Scheme (FPS). This is therefore the focus of the initial requirements. We understand and agree with the focus on FPS in the first instance, and agree that implementing effective and timely solutions is imperative to providing protections for customers against APP scams. Victims of scams should be entitled to appropriate reimbursement regardless of the payment instrument and resulting type of payment that the scammer requests, and it is important to ensure the arrangements are flexible and adaptable for the future.

We think this means that the PSR's proposals should be designed with all payments in mind, even if PSR choose not to apply them yet across different payment methods, although we note the FSMB provides the powers to do so. This was a key request of our EUAC. The definition of scam in the CRM Code, as an industry-accepted definition, may be an appropriate starting point.

As we further explore in response to question 20, a PSR Direction across PSPs would allow customers to be protected consistently for all scams that results in FPS payments. Such an instrument could be expanded in future to cover all designated payment types. Pay.UK rules will require PSPs to meet that regulatory obligation and support them in operationalising the proposals. This would address some of our concerns set out in response question 1.

It is important to ensure that all victims receive the same level of protection from scams, so we are supportive of the PSR approach to bring into scope all consumer scams that result in FPS payments, regardless of how they are initiated. Criminals adapt quickly. For example, fraudsters have adapted their tactics to exploit the rising cost of living, with new trends in phishing attacks mimicking government support packages such as energy and council tax rebates, or ‘cost of living’ payments<sup>2</sup>. The exclusion of a channel of payment, or category of firm would play into their hands. It is right therefore to include PISPs as well as conventional PSPs.

It is unclear in the consultation document how the proposals will be applicable to PISPs – the PSR must set out its thinking further on this matter.

#### 4. Do you have comments on our proposals:

- that there should be a consumer caution exception to mandatory reimbursement
- to use gross negligence as the consumer caution exception
- not to provide additional guidance on gross negligence?

It is right that the public authorities should set the reimbursement requirements, as they do for unauthorised payment fraud. We will support our customers, the payment providers, to meet those requirements and support their customers.

We believe the industry is best placed to comment on the detail of the requirements in the proposals to work towards such outcomes.

#### 5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?

In August 2022, Pay.UK published research on improving the payments system for financially vulnerable people<sup>3</sup> which aimed to understand the changing needs of end users with focus on account-to-account payments. We want to draw the PSR’s attention to this work as it may support your consideration of this issue. Recommendations from this work focus on prevention and detection:

- That banks and building societies adopt the lessons learnt from our benchmarking research into identifying best practice for a more clear and impactful use of the Confirmation of Payee service in customer journeys and messages; and
- Further research into financial abuse more generally and what the payments ecosystem can do to tackle it in order to understand if purpose codes could facilitate better fraud and financial abuse detection.

Findings more generally from this piece of work may help in shaping the PSR’s proposals on vulnerability:

- Our polling found that in the last month, 52% of people had received some kind of request to transfer money, which they believed to be fraudulent, and 60% of financially-vulnerable people had received some kind of fraudulent request.

---

<sup>2</sup> [Phishing attacks – who is most at risk? - Office for National Statistics \(ons.gov.uk\)](https://www.ons.gov.uk/news-and-analysis/news-releases/2022/08/20220816-phishing-attacks)

<sup>3</sup> <https://newseventsinsights.wearepay.uk/media/t35fktsa/financially-vulnerable-research-240822.pdf>

- Younger people were often more likely to be targeted by fraudsters, particularly through letters and adverts, but many older people also reported receiving texts and emails they believed to be fraudulent.
- Our polling found that people in higher socio-economic groups and financially-vulnerable people were more likely to report receiving some kind of fraudulent APP request.
- We found that whilst 92% of the total population take heed of a CoP alert, some people choose to ignore it. 8% said they would make the transfer anyway, and this number is higher for those with a health vulnerability (12%), life events vulnerability (10%) and low financial resilience (14%)

This demonstrates that financially-vulnerable are targeted by scammers, and may be more susceptible to the scam. Vulnerability in the context of scam may look different to the traditional definition of vulnerability, and this should be considered by the PSR.

## 6. Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?

### 7. Do you have comments on our proposals that:

- sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement
- any ‘excess’ should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?

### 8. Do you have comments on our proposals that:

- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?

## 9. Do you have comments on our proposal not to have a maximum threshold?

We believe the industry is best placed to comment on the detail of the requirements in the proposals to work towards such outcomes.

The areas set out in questions 4 -9 should be considered in the PSR’s post implementation review – it is important that the PSR leads and sets out what outcomes it wants to achieve through these proposals in order for their effectiveness to be evaluated by the PSR.

In order for such an evaluation to be possible, PSR will need to consider what data it needs to collect and to what frequency – we do not anticipate that all of these data points needed to assess these questions would routinely be collected by Pay.UK as a part of its ongoing monitoring. Whilst the PSR refines its proposals post-consultation, it is important to draw out the data required for the post implementation review and who will collect this.

We discuss the post implementation review further in response to question 18.

#### 10. Do you have comments on our proposals that:

- sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
- any time-limit should be set at no less than 13 months?

#### 11. Do you have comments on our proposals that:

- the sending PSP is responsible for reimbursing the consumer

We agree that the firm which has the customer relationship with the victim would seem to be the appropriate one to provide the reimbursement payment.

#### 12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?

#### 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

We support the idea that receiving firms should face some liability for hosting the accounts into which scam payments are made. It is for industry to comment on the most effective way to ensure that this responsibility is introduced in such a way as to drive more effective detection of fraudulent and mule accounts. A 50/50 split, to be reviewed as part of the PIR in the light of MI collected in operation would seem on the face of it to be a pragmatic way forward.

#### 14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?

PSPs will need to reflect on what processes they need to establish in the event that they want to depart from the 50:50 split. It may take time to establish common criteria, building on the experience of operation of the reimbursement framework, and the criteria may need to continue to evolve. This dispute mechanism would need to sit outside of the scheme rules, but could be referenced in operational processes as appropriate.

#### 15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?

Multigenerational scams are a complex matter. The industry, in collaboration with public authorities should explore this further and how liability in such scams should be set. We have asked PSR for further discussions on this question. We are unclear as to how FPS scheme rules can implement this aspect, given that fraudsters will seek to move funds across multiple schemes as one of the methods to hide the trail.



16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?

17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?

We agree that the scope of the reimbursement requirement should encompass all firms who initiate payments on behalf of consumers, not just direct participants in FPS. It is not currently possible for such a requirement to be imposed via scheme rules.

18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?

Pay.UK has implemented a new Strategy, setting a foundation for the future. It is our vision to be the smartest way to move money, now and in the future. We are looking to do more than we have in the past. This ambition is about Pay.UK and all its schemes, it is not limited to APP scams or to FPS.

We are clear that we should disaggregate the discussions of the longer-term vision for Pay.UK from APP reimbursement in order not to jeopardise the delivery of an effective reimbursement solution for 2024. We have discussed this with you and are pleased you have accepted this. We share some of the long-term ambitions of the PSR, but these are complex areas that will need to be worked through alongside our other priorities and in discussion with our regulators. The focus of this response is on the implementation model for 2024, however we include some overall observations here.

We will follow this up through strategic discussions with the PSR on their vision for Pay.UK more holistically. The NPA is one of the ways we will deliver our new strategy and, combined with our rules and standards, plus associated controls and policies, will give us a powerful platform reinforcing our position of leadership in the payments market globally. It would be better to approach the discussion of Pay.UK's future role on this broad basis, rather than through the lens of APP scams.

The consultation document states that it is the PSO that should make, maintain, refine, monitor and enforce compliance with comprehensive scheme rules that address fraud risks in the system. We agree that a PSO needs to have an effective rulebook and the ability to monitor and enforce compliance with it. Each rulebook of the schemes we operate is different, reflecting the scope of the system in its designation and the particular design, use and evolution of the scheme. In addition, Pay.UK is responsible for the rulebook and data standards for overlays such as Confirmation of Payee (CoP) and Request to Pay (RtP). As PSR is aware, work is underway to design and develop the rulebook for NPA and we look forward to continued engagement with PSR as this is developed.

As we have outlined in previous responses to PSR consultations on APP scams, we think that the relative roles of the public authorities and PSOs are clear. Public authorities should establish the overarching high-level principles, which place liability on individual firms in the discharge of their provision of payment services; PSOs should use their rules, standards and technology to ensure that participants in the schemes meet those obligations. Under FSMB, it is for PSR to determine the terms of the requirement, and what good looks like in its implementation.

This is the principle that exists for unauthorised payment fraud. For example in ICS, Pay.UK documentation includes a Fraud Manual and we undertake monthly monitoring of fraud levels with participants to track trends in cheque fraud across the industry. We do not currently undertake



equivalent monitoring for FPS. This is because the legal framework and related FCA regulatory obligations, supported by industry (UKF) guidance delivers incentives, processes and procedures for PSPs to manage and reimburse for such fraud. The absence of an equivalent comprehensive and consistent set of expectations in relation to APP scams will be rectified by the proposals now being put forward by PSR through this consultation. We think it is right that the public authorities should take on this role.

As part of strategic discussions of Pay.UK's future role, we would also like to better understand PSR's view with regard to the role of the card scheme rules. The PSR reference existing rules in the card schemes in relation to prevention of authorised fraud. However, we are not aware of such rules and would be interested to understand this reference. Our understanding from engagement with customers is that they do not report authorised scam levels to the card schemes or UKF and are not required by scheme rules to reimburse these. The scale of authorised card scam across the industry is therefore not known. Our analysis suggests that the card scheme rules implement operational arrangements to allow scheme members to meet their legal and regulatory obligations in relation to unauthorised fraud. We believe that the model we are proposing here aligns to this approach

It is right that we, as a PSO, can do more to support participants in our schemes to tackle fraud. As PSR are aware, we have already implemented CoP and have a programme of activity underway to develop and roll-out other prevention and detection tools, including the Enhanced Fraud Data project being taken forward by industry under PSR's Measure 2. We want to look at fraud prevention and mitigation across all our schemes, what we do and how we can do it better, considering how we can leverage the NPA to deliver improvements. We will also use our rulebook to support better reimbursement outcomes under the proposed PSR framework.

There are challenges to Pay.UK taking on some of the proposed roles set out by the PSR in the near term. We are limited by our existing powers and reach. For example, our ability to undertake enforcement action is limited, and it is not possible for us to require actors in the ecosystem outside of our direct participants to submit to our rules. Analysis of Pay.UK's powers and reach in the context of the proposed roles is necessary to ensure that these are appropriate, both considering legal feasibility and balancing against our core responsibilities. As a Payment Systems Operator, Pay.UK manages the central infrastructure for its payment systems, undertaking a systemic risk manager role whilst providing choice and provision of services to the UK economy – any new roles must not introduce disproportionate risk to this.

We may want to be more interventionist in the future in order to support the management of our system. Our strategy sees us taking a position of leadership in the payments market, and addressing concerns will be a key aspect of this. There may be other concerns which arise in the coming years which require us to act, and we want to ensure we have the powers to do this effectively.

Your consultation is clear that the PSR will undertake a post-implementation review of the interim reimbursement arrangements ahead of transition to NPA. We consider that this should be a full review of the effectiveness of the measures taken, rather than of the FPS rules alone. This will then feed into how reimbursement requirements should look, and our role, in the future.

It is important that the decision on our role for the design and enforcement aspects of the reimbursement regime should not be made until there has been an evaluation of the operation of the model: we therefore strongly support the PSR's proposed post implementation review.

It will be important for the PSR to be specific in defining what good outcomes look like in each area of its proposals, to not only support their operationalisation, but the post-implementation review.

We would welcome clarity on what Pay.UK's role will be in the post-implementation review.

## 19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?

We recognise that the PSR's proposal will evolve through consultation and it will be important that our work and planning remains aligned to PSR thinking and expectations of our role. Our work in this space has moved into a design and delivery phase, so we are prepared to operationalise the PSR's final decision. We must work closely with the PSR between its consultation closing and final decision being made in order that we are able to plan, resource and deliver work required of us in an effective and timely way. We will need time to reflect any changes in PSR policy positions. As such we formally request sight of consultation responses and regular updates from the PSR in its thinking to support our business assessment and implementation planning.

It is right that public authorities set out the reimbursement framework to be implemented by PSPs. This is not within the PSO remit and nor an area of expertise for Pay.UK. We will, as proposed in the consultation, transpose those requirements into FPS rules to require participants' adherence to them as a condition of participation in the scheme. We have proposed to the PSR a more detailed model (Annex A) which explains the role we expect to play in delivering the reimbursement regime and our understanding of what the PSR and PSPs will also do to support delivery of the regime.

We are focusing our work on developing an effective reimbursement model to the expected timelines. Alongside rules, which will set out outcomes and responsibilities, we will need to work with industry to develop operational guidance and processes to enable them to meet the requirements of the rules. Some of these may best form part of the set of FPS operational documents, and be maintained and governed by Pay.UK but others may be broader in nature and require separate governance. For example, we do not anticipate that Pay.UK would develop guidance related to conduct and consumer relationships – this is outside of the payment system and not areas of expertise for Pay.UK. We think it would be necessary to identify the full set of guidance to be developed and agree responsibility for each part across the industry, LSB, UK Finance and PSR. This includes consideration of what should be included, governance and ownership. We need to carefully consider how these will interact with our rules. At a minimum there will need to be requirements on firms related to how they demonstrate adherence to the rules, and operational processes to support that. The content and level of guidance and processes will be dependent on the final decision of the PSR, for example of the level of monitoring and enforcement appropriate for us.

We will also need to secure funding from our customers. Our expectation is that the PSR would be supportive of us requesting this funding from our customers.

## 20. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?

PSR has multiple options for how to require PSPs to implement a reimbursement framework. Below we set out our thinking on the most effective option. Regardless of the vehicle the PSR decides to deliver the requirements, Pay.UK will take an active role in supporting PSPs in their reimbursement

requirements. We will undertake the same role and activities, to implement rules, systems and processes to support our customers in operationalising the reimbursement framework. Our preferred option is based on our belief that it will deliver better policy outcomes; we do not expect that it will impact the activity we will undertake.

The PSR proposes to use their powers under Section 55 of FSBRA to require Pay.UK to amend FPS rules. The PSR notes that the requirements could be imposed on PSPs through directions, but dismiss this as incompatible with the long-term vision. However, we still see merit in this approach as being an effective mechanism to place the liability to reimburse directly on the affected parties – the entity making the payment for the consumer and the entity holding the account on behalf of the criminal.

We think that a PSR Direction on PSPs is a more appropriate vehicle for a number of key reasons:

- A wider range of PSPs could be required to provide reimbursement.
- The requirement could apply to multiple payment channels.
- A regulatory requirement is likely to create a very strong incentive to comply and invest in prevention and detection to reduce fraud overall.
- PSR has effective enforcement arrangements (underpinned by statutory powers) in place, should action be needed.
- It would likely minimise competitive distortions that could occur if Faster Payment rules alone were used.

A working example of where the PSR have utilised this approach is that of Confirmation of Payee. Through Specific Direction 17, the PSR has required all relevant PSPs, both direct and indirect, to put in place and use a system to provide CoP so that a greater number of CHAPS and Faster Payment users benefit from it. In addition, as with Specific Direction 10, the wording of the direction that requires CoP check to be made where a customer provides ‘the necessary information about a new payee’ means that PSPs have applied CoP to ‘on-us’ payments, as well as Faster Payments and CHAPS.

If PSR were to make such a direction in relation to its reimbursement proposals, this could still be supplemented by a Section 55 requirement on Pay.UK to amend the FPS rules to make this operational for those PSPs subject to the rules and caught by the requirement. This is line with our proposed model in Annex A.

Any Section 55 will need to specific and set out clearly the outcomes that PSR want the rule to achieve. We will need to work with the PSR to ensure the Section 55 enables Pay.UK to act lawfully and within its power when implementing the rule.

- It is a requirement of the PSR’s General Direction 4, that Pay.UK, as operator of FPS, actively seek the views of service-users in making decisions concerning FPS rule changes. Under FPS rules, Pay.UK is required to consult ‘as appropriate, will all relevant Participants and other external stakeholders as well as the appropriate Board Committee, on FPS rule changes.’<sup>4</sup> However, if we are implementing a rule change which the PSR has fully specified, it is less likely that a consultation will be needed. The composition of the Section 55 will impact on this.

---

<sup>4</sup> FPS Rule 10.2

- In order to undertake the monitoring role as set out in the PSR’s consultation, the PSR would need direct PSPs to provide their payments data to Pay.UK to be used for fraud analytic purposes, and in a unified format. Whilst the data will be dependent on the outcomes the PSR wants its requirements to achieve, and the KPI’s they set out as an indication for the need for escalation/enforcement, the PSR should grant Pay.UK the power to determine the PSP payment data we consider appropriate for monitoring of the rule.

## 21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?

PSR proposes that a set of arrangements be designed in Faster Payment rules, with Pay.UK responsible for ensuring they are in place and operating effectively.

We see the allocation criteria, for which the dispute arrangement would be based upon, should be developed by the industry, as this is where the liability for scams sit. These will likely need to adapt in response to developments in relation to the fraud landscape, and therefore by their nature would not fit within scheme rules. A Code may be more appropriate.

We would propose that the dispute resolution arrangements are not run by Pay.UK. We understand that the CRM Code dispute resolution arrangements requires the Sending Firm to act as a case handler, chose a dispute resolution firm and manage the process. This could be one approach, or the dispute resolution firm could be sourced by us with a preferred provider. This is an approach currently used with other areas Pay.UK are responsible for, and we believe this would be a balanced and effective approach.

It is important for the PSR to be specific about the outcomes it is looking to achieve and the expectations it has for Pay.UK in achieving those outcomes. It would be imperative for the PSR to further define what ‘operating effectively’ would look like, in order for the implementation of arrangements to have the desired outcome (and for Pay.UK to be able to manage any compliance risk).

As the PSR notes, it would be important for any given criteria to be applicable fairly to all relevant types of PSPs. Similarly, it would be important that all relevant types of PSPs could be a part of the development of allocation arrangements, and would be able to access dispute resolution. This would mean direct, indirect PSPs [and PISPs]. It may mean that the PSR (with support from UKF) would be best placed to develop and implement these, given their convening powers, and reach across the different payment providers, with Pay.UK supporting implementation to direct participants.

## 22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?

It is important for the PSR to define what an ‘effective compliance monitoring regime’ would look like, including what outcomes it should achieve, to support our monitoring activity.

We understand there are three aspects to monitoring and enforcement

- I. PSPs reimbursing in accordance with the required timescales
- II. Reimbursement is being made in all cases of APP fraud, recognising exceptions
- III. Payment of shared liability is being made in all cases

In order to implement effective monitoring of these aspects, all relevant firms will need to provide data on a regular basis on their performance on reimbursement.

A refund by a bank to its customer does not go across Faster Payments, therefore it would not be possible for Pay.UK to extract data in relation to reimbursement directly from the Faster Payments System to support a monitoring regime. A monitoring system would have to be based on reporting from PSPs.

A data set would need to be determined, in collaboration with the PSR and the relevant firms, with a clear reporting template and set of definitions. We need to understand what good looks like for the sending and receiving banks in meeting the requirements. This will aid the identification of data to support the monitoring regime. Thresholds would then be set for the data we receive from each firm, and this would allow us to identify where action may need to be taken.

As noted in response to question 20, it will be imperative that PSR direct relevant firms to provide us with data necessary to monitor compliance with the requirement – including those beyond our direct customers. It is also a key assumption that the data we collect will relate to volumes and values, collected at firm-level, and we would not hold any personal consumer data.

In relation to point II, we understand from discussion with PSR that there would not be a role for us in the provision of consumer-facing guidance, or in disputes between PSPs and consumers. This would be managed as is currently, through the banks' own complaints procedure and the Financial Ombudsman Service, supported by LSB and UKF guidance.

### 23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?

As set out above, we envisage in the short term that monitoring would be based upon PSP reporting of data. The frequency of this reporting will need to be agreed and should relate to the intensity of monitoring required - we do not see anything intrinsic to the proposals that indicates the need for real-time compliance monitoring. Scams are reported by customers once it becomes apparent that the basis for the payment was false and the next step is the decision by the paying bank on whether reimbursement is appropriate. We would ask the PSR to set out why a real-time monitoring system would be necessary, in order for us to understand what such a system would do and requirements for its build. This would inform an assessment of costs and benefits.

Our Fraud Programme is currently investigating how we could automate PSP reporting in order to support monitoring. There would be significant operational impact if we were expected to gather data from indirect PSPs and PISPs without automation, due to the individual reporting nature of our processes. We will keep PSR abreast of our progress.

### 24. Do you have views on the best option for short-term enforcement arrangements?

Due to our current powers, it would not be possible for us to undertake effective enforcement in the short term. As set out in the PSR's options, we could include escalation to the PSR as a part of our post-monitoring activity. We are able to undertake the appropriate monitoring to identify where PSPs have hit KPI's or thresholds, set out by the PSR, however we could not be the party taking action.

We are seeking guidance from the PSR on KPI's and thresholds, and to report to them so they can act. It would also be important for us to understand the extent the PSR would want Pay.UK to undertake any activity prior to reporting to the PSR, as this could have an impact capacity and capability.

If a PSR were to impose the overall high-level requirements on PSPs through a consistent, market-wide Direction, this would remove any questions around enforcement and allow the PSR to undertake this directly, including on the basis of information escalated to it by Pay.UK. We continue to consider that the significant threat of regulatory enforcement would place appropriately strong incentives on firms with minimal regular overhead for the PSR once the arrangements are operational.

## 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?

The most effective approach would be for the PSR to direct all firms which initiate payments over FPS for consumers to implement the reimbursement requirement. The other proposals suggested by the PSR to place the reimbursement obligation on firms are unlikely to be viable. Our engagement has shown that neither indirect access providers, nor indirect participants, were supportive of this obligation being put in place via a contractual business relationship. It is also unclear how enforcement would work in this regard.

As set out in response to question 20, a direction on all PSPs would be our preferred approach, which would also capture indirect participants. This has a range of benefits from a public policy and legal perspective. This approach has been undertaken by the PSR in relation to Confirmation of Payee, as noted in response to question 20.

We understand in the long term the PSR aspires all PSPs to be captured by a PSO rule, likely through the NPA. We don't think there is a credible way we can capture the full range of relevant firms via the FPS rules.

We have focussed in the model proposed on the implementation of an effective solution. We do not think that the constraints we currently have should prevent comprehensive reimbursement for the benefit of end-users. We recognise that PSR has consideration of the future model in developing the current requirements and implementation, however, should impact on – whilst it may seem that Pay.UK maintaining responsibility for reimbursement requirements throughout the short and long term would provide some level of consistency, we think it is more important to focus on what will provide the best outcomes for consumers. In this case, the PSR directing all PSPs now will provide the most effective solution, and would not preclude the NPA rules housing reimbursement requirements in the future.

## 26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?

Our engagement with payment providers suggests it would be preferable for liability to sit with the firm who initiates payment on behalf of the consumer and that there would be considerable complexity and risk to deliver this via contract between IAPs and their customers. This supports our view that there is a need for broad direction of PSPs.



## 27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?

The key benefit of these proposals is identified to arise from a consequent improvement in controls within payment firms resulting in a fall in the number of scam payments made by up to £150million. Our EUAC cautioned that there might be an increase in the number of scam attempts made by criminals in the hope that customers would be less vigilant in the expectation of reimbursement. EUAC said that in this case, even if the PSP were able to intervene at the end of the scam lifecycle, to prevent the ultimate transfer of funds, the victim would still suffer the distress of the social engineering or harassment of the fraudster. There may be fewer successful scams and consumers face less financial loss, but a greater number of potential victims. Whilst costs to consumers would be reduced there is likely to be at least some increase in costs to PSPs.

In terms of these costs, EUAC were clear that the PSR take proper account of the likelihood that PSPs would need to pass on the cost of reimbursement (and of increased investment in fraud prevention and detection) to their whole customer base, including the bulk participants in FPS and corporate users who do not benefit from the reimbursement promise. The CBA acknowledges the cost to PSPs, but does not consider how they might recover this cost and the consequential impact on payments service users.

## 28. Do you have any other comments on the proposals in this consultation?

Whilst we understand the PSR has an obligation placed upon it by HM Treasury, and the industry want to reach an effective solution to the reimbursement of end users in the case of APP scams, we think the PSR should focus on what is the most effective route to meeting its policy outcomes, and consider if it is the best approach.

The legislation specifies Faster Payments, but does not restrict the PSR's actions. You should consider whether better policy outcomes would be produced if the obligation were applied to all push payment methods (including, for example, CHAPS). As noted in response to Question 1, we are also concerned that fraudsters may target consumers who use FPS to make payments, in the hope that they will be less vigilant and take less caution in their payments with the knowledge that they will be reimbursed.

There is also an additional risk that our customers will move to utilising a different payment method to fulfil the role Faster Payment currently holds, for example Direct Credit, as this means they are not held to a reimbursement requirement.

One of the PSR's proposed outcomes from this consultation is "agile payment scheme rules". We do not agree that this should be included as an outcome PSR want to see as a result of the introduction of APP scam reimbursement. We share the ambition - as PSR know - but consider this to be a broader deliverable, which relates to the entirety of the role of us as the PSO.





# Annex A

## Implementation Model – roles and responsibilities

Component of model	Pay.UK action	PSR action	PSP/PISP Action	Comment
<b>Liability framework</b>	Pay.UK would not have a role in setting the liability framework.	PSR would specify the requirements within the direction to PSPs and in the Section 55.	Liability framework would apply to all parties subject to the direction	Pay.UK may include the liability framework within FPS rules, but the composition of “the what” would be the responsibility of the PSR.
<b>Mandating adoption by direct participants</b>	Pay.UK would implement FPS rules to reflect the reimbursement requirement for qualifying PSPs of qualifying payments, in accordance with framework in PSR direction.	PSR would direct all relevant firms which initiate FPS payments for consumers* to implement the reimbursement requirement. PSR would require us to implement an FPS rule to support FPS direct participant compliance with direction.	The regulatory requirement would apply to all firms which initiate FPS payments for consumers. FPS rules could supplement this for direct participants, by inclusion or reference to expectations around adherence to operational processes and industry guidance.	This approach – of introducing the liability for reimbursement via a PSR direction, supplemented by FPS rules will deliver a consistent approach for all FPS payments. It is supported by the PSP community. We will support this in our response.
<b>Mandating adoption by indirect participants</b>	No role for Pay.UK at this stage.	The PSR would direct all firms which initiate FPS payments for consumers* to implement the reimbursement requirement.	The regulatory requirement would apply to all firms which initiate FPS payments for consumers*	This approach is supported by the PSP community and should therefore make resolution of this difficult aspect easier for PSR.

Component of model Pay.UK action	PSR action	PSP/PISP Action	Comment	
<b>Operational Processes &amp; Guidance</b>	Pay.UK would work with industry to put in place the necessary process framework for them to deliver reimbursement.	PSR would specify outcomes and expectations that should be met.	Firms would need to support the development of processes & guidance (contributing their knowledge and experience) and then implement into operation.	Some may be FPS operational documents, others may require separate governance, with assurance to be agreed. UKF and LSB have both offered to support this significant task.
<b>Data requirements</b>	Pay.UK would receive data from <b>all relevant</b> firms for consumer reimbursement, 50:50 allocation of funds and where this is disputed.	PSR would direct firms to provide Pay.UK with data required to monitor adherence to the requirement, in a unified format.	Firms would collaborate with Pay.UK to develop and submit standardised reporting of the relevant data (as required by PSR direction).	If, as proposed, we gather data from all firms, not just our customers, this will require automation. We will seek PSR agreement on the required data points for each aspect.
<b>Monitoring</b>	Pay.UK would produce MI to assess data against KPIs to be agreed with PSR, relating to their required policy outcomes.	PSR would work with us to agree KPIs for monitoring of the direction/rule and receive regular MI reporting on firm performance.	Firms would receive MI reporting on their performance against KPIs.	The degree to which reporting and MI can be automated is to be investigated by fraud programme in coming weeks. Some level of automation would be necessary to monitor the full set of firms.

Component of model Pay.UK action	PSR action	PSP/PISP Action	Comment
<p><b>Enforcement</b></p> <p>Pay.UK would engage with direct participants not meeting KPIs, to explore reasons. This information would be shared with PSR at an agreed frequency.</p>	<p>PSR would use information provided by Pay.UK, supplemented by own engagement to undertake enforcement it sees necessary.</p>	<p>Firms would be expected to provide Pay.UK/PSR with explanations and plans to remediate non-compliance with FPS rules and PSR direction.</p>	<p>We do not currently have the power to undertake the direct financial enforcement necessary for this rule to be made effective. This is something which will be explored further in the longer term / NPA.</p>
<p><b>Post-implementation review</b></p> <p>Pay.UK will provide PSR with the necessary information and support to undertake the review.</p>	<p>PSR will lead a post-implementation review after 2 years of operation ahead of transition to the NPA.</p>	<p>Firms will engage with PIR to provide their perspective on how well the requirement is operating.</p>	<p>In the long term, PSR expect Pay.UK to keep the effectiveness of requirements under review once they are in NPA rules.</p>

## Assumptions

Given where PSR are in the process of finalising their requirements, we have had to base the above model on various assumptions developed from our working level discussions with PSR. Divergence from these assumptions would likely create additional activities or risks for the business to mitigate. The assumptions are listed below.

- |   |  |
|---|--|
| <p><b>#1</b> PSR implements decisions in manner that does not increase Pay.UK legal risk.</p>   | <p><b>#6</b> The 50:50 allocation dispute process is not run by Pay.UK. For example, as per the CRM Code which requires the Sending Firm to act as a case handler, chose a dispute resolution firm and manage the process. Alternatively, this could be sourced by us with a preferred provider.</p> |
| <p><b>#2</b> The PSR will undertake directions to bring all PSPs and PISPs in scope of the reimbursement requirement.</p>   | <p><b>#7</b> There is no role for us in the provision of consumer-facing guidance, or in disputes between PSPs and consumers. This would be managed as is currently, through the banks' own complaints procedure and the Financial Ombudsman Service, supported by industry guidance.</p>            |
| <p><b>#3</b> The PSR will direct relevant firms to provide us with data necessary to monitor compliance with the requirement – including those beyond our direct customers.</p> | <p><b>#8</b> The data we collect will relate to volumes and values, collected at firm-level. We would not hold any consumer data. We currently do not hold personal data.</p>  |
| <p><b>#4</b> PSR will approve KPIs for firms' performance in relation to reimbursement and liability sharing.</p>   | <p><b>#9</b> We will consider how any data collected can be leveraged to support better tools for prevention and detection of fraud by PSPs, but this will not be on the critical path for delivery of reimbursement model in 2024.</p>  |
| <p><b>#5</b> PSR will consider taking enforcement action against firms who have not complied with the directions.</p>   | <p><b>#10</b> The PSR – supported by us - will understand, assess and establish stakeholder support for our role through its consultation process.</p>   |



2022 © Copyright in this document lies with Pay.UK Limited. All rights reserved.

The copyright in this document is owned by Pay.UK Limited. All material, concepts and ideas detailed in this document are confidential to Pay.UK.

This document shall not be used, disclosed or copied in whole or in part for any purposes unless specifically approved by Pay.UK.

# Payments Innovation Forum



**Payments Innovation Forum**

86-89 Paul Street

London

EC2A 4NE

[www.paymentsinnovationforum.org](http://www.paymentsinnovationforum.org)

By email to: [appscams@psr.co.uk](mailto:appscams@psr.co.uk)

**Non-Confidential**

Dear Sir/Madam,

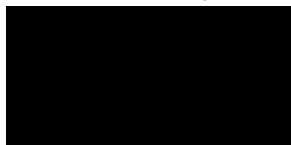
**Re: CP22/4 - Authorised push payment (APP) scams: Requiring reimbursement.**

We welcome the opportunity to respond to the Consultation published by the Payment Systems Regulator (“PSR”) in September 2022: “Authorised push payment (APP) scams: Requiring reimbursement” (the “**Consultation**”). We would be pleased to discuss our response with the PSR in more detail.

The Payments Innovation Forum (“**PIF**”) is a not-for-profit industry body representing providers of innovative payment services for consumers, businesses and public sector organisations. PIF members range from large e-money and payment institutions, including indirect access providers (IAPs) and smaller PSPs, many of whom are indirect participants in Faster Payments. It is in this capacity that we submit our response.

We would like to thank the PSR for taking our comments into consideration.

Yours faithfully



Executive Director

**Payments Innovation Forum Ltd**

## **Introduction**

PIF and its members recognise the importance of tackling APP scams which can result in severe consequences for consumers, and which pose a challenge for the payments and e-money sector. Innovation and competition in payments can only thrive if payment service providers earn the confidence of payment service users. PIF members are, therefore, deeply committed to ensuring that their products and services are not used for illicit purposes.

However, PIF and its members do not agree that making reimbursement mandatory will achieve the PSR's intended aims. We feel strongly that the PSR's proposals, if implemented, will have a negative impact on consumers and negative implications for innovation and competition in UK payments which we expand on below

## **General observations**

### **In our view, the proposals amount to a 'Cheaters' Charter' – APP scams will go up, not down**

We are extremely concerned that the proposed measures will encourage, rather than tackle, APP scams. Apart from making the sector more attractive to organised criminal gangs, there is a very real possibility that mandatory reimbursement will result in increased levels of first-party fraud. The House of Lords Fraud Act 2006 and Digital Fraud Committee report "Fighting Fraud: Breaking the Chain" (November 2022)<sup>1</sup> supports this view, i.e., that a blanket reimbursement policy "**may lead to increased levels of moral hazard and fraud**" and "may even lead directly to **new avenues for APP-reimbursement frauds**." We elaborate on this point further in our response.

### **The proposals expect very little of consumers**

The proposals seem to overlook the vital role consumers can, and should, play in preventing APP scams from happening in the first place. The Contingent Reimbursement Model (CRM) places expectations on consumers to "pay attention to warnings given to you by your bank" and "always think carefully before making a payment". In other words, the CRM expects consumers

---

<sup>1</sup> [Fighting Fraud: Breaking the Chain \(parliament.uk\)](https://www.parliament.uk/publications/2022/11/fighting-fraud-breaking-the-chain)



to have a reasonable basis for believing the payment transaction is “genuine” and “legitimate”. Conversely, the PSR’s proposals seem to expect very little of consumers.

In our view, it would be more effective for the PSR to focus on educating consumers, ensuring they understand the types and risks of fraud, and how to keep themselves protected.

**Customers must understand their responsibility** in deciding when and to whom to make payments.

### **The advantages of a comprehensive, joined-up approach to tackling APP scams have been underplayed**

We welcome that the communications and technology sectors are likely to be impacted by measures in the Online Safety Bill to combat user-generated fraud, but, as far as we are aware, there are no plans to require these sectors to contribute to APP scam victim reimbursement costs.

That the cost of reimbursing APP scam victims should sit solely with PSPs, and not the sectors that enable fraudsters to freely reach potential victims by way of scam text messages, fake websites, or fraudulent advertisements on social media, is, in our view, very difficult to comprehend. We acknowledge that the communications and technology sectors are not within the PSR’s remit, but it is disappointing that there is no attempt at an ecosystem-wide approach to tackling APP scams.

We again refer to the House of Lords Fraud Act 2006 and Digital Fraud Committee report which maintains that as “**banks are the last link in the fraud chain**” they “**cannot be expected to foot the fraud bill alone**”.

Further, we question the basis for the proposals when Strong Customer Authentication (SCA) under the Payment Services Regulations 2017 (PSRs) was intended to make payments more secure, and which has been implemented by PSPs at significant cost. The PSR’s proposals seem to suggest that SCA under the PSRs has not achieved its intended aims. If this is the case, it would be more appropriate to address why SCA has not worked, rather than implement an unrelated reimbursement mechanism for the customer.

### **The proposals will increase financial exclusion**

We represent PSPs who provide payment products and services in support of financial inclusion. If PSPs are required to reimburse every APP scam, they may be forced to create barriers to account opening or worse, exit from the market.

### **Competition in UK payments will be adversely impacted**

It will be very difficult for smaller or leaner PSPs, particularly those with consumer products, to fund the cost of reimbursement under these proposals. They will be unable to compete with larger firms that are better able to absorb the costs.

### **The proposals will deter investment in UK Fintech**

At a time when overseas investment in UK industries is paramount for economic growth, we strongly believe that the PSR's proposals will have negative consequences. Under the PSR's proposals, the UK would be the only country in the world to require reimbursement by PSPs. In our view, the requirement will deter international investors once they know that a significant portion of their investment in a UK PSP is at risk of being lost on reimbursements.

### **The proposals amount to a sticking plaster**

Fraud is complex and comes in all shapes and sizes. Having a blanket requirement does not address the different types of fraud and why they occur. In our view, time and money would be better spent understanding fraud typologies and educating those impacted by APP scams (victims, PSPs, law enforcement, crime prevention agencies) to understand their role in preventing fraud.

### **Impact of the PSR's proposals on consumers**

The Consultation states that "additional friction for a small proportion of payments is proportionate to preventing APP scams". We strongly disagree, not least because the PSR says that it has "not been able to quantify the likely costs of any delayed or declined payments" but mostly because a PSP's fraud prevention efforts are highly likely to result in significant amounts of friction, particularly for higher value payments, given the severe consequences and costs to PSPs should a fraudulent payment be processed.

We do not feel that the PSR has considered the ramifications of PSP's refusing more payment orders than they currently do now. In our view, **the impact on genuine payments and**

**legitimate customers will be significant**, resulting in reduced, and far from improved, consumer confidence. In developing these proposals, we urge the PSR to investigate further the impact of delayed or declined payments on legitimate customers.

Further, if the cost of reimbursement is to be borne solely by PSPs, then we would expect basic **transactional costs to increase for all customers** as PSPs seek to recover their losses by increasing fees. There is also a risk that the proposed measures will lead to lengthier payment processing times due to PSPs reviewing transactions to mitigate risk. For small business customers, payment delays could arguably be much more serious than loss of funds. This potential delay becomes even more acute if a PSP follows the recommendations set out in a Financial Ombudsman Service case study to “contact the Police who will speak to the customer”<sup>2</sup>

We ask the PSR to consider the impact on those consumers who might be deterred from accessing payment services as a direct result of the new requirements, and who may be **forced to access payment services that do not meet their needs**.

We are also concerned that requiring PSPs to bear the cost of reimbursement will harm the commercial viability of PSPs that offer products and services that aim to help the underbanked. With no appetite to pass on the cost of compliance to these types of consumers, it will become impossible for PSPs to service financially underserved consumers, resulting in **negative implications for financial inclusion in the UK**.

Finally, there is a risk that consumers fall victim to scams where they are encouraged to claim vulnerability. These types of scams can lead to significant financial and other detriment to consumers, such as debt, eviction, and a criminal record. We elaborate on this point further in our response.

### **Impact of the PSR’s proposals on PSPs**

We believe that PSPs in the e-money and payments sector will be disproportionately impacted by the PSR’s proposals, and, in some cases, the consequences will be severe.

---

<sup>2</sup> <https://www.financial-ombudsman.org.uk/decisions-case-studies/case-studies/customer-asked-transfer-money-account-threat>

We are extremely concerned that the PSR's proposals **will threaten the existence of PSPs whose entire customer base is classed as vulnerable**. For example, a number of our members provide products and services that are designed to support the most vulnerable, and which support local government authorities in the disbursement of funds. These firms are already taking extra steps to support customers in protecting themselves from fraud, for example, by implementing Confirmation of Payee, by raising awareness of how customers can protect themselves and by monitoring the activity of vulnerable customers in tandem with the local authorities and government agencies with whom they work.

Under the new requirement, PSPs will likely be required to reimburse their customers, **even if they consider them to have acted with gross negligence**. In our view, this is problematic, and it will be very difficult to manage. This requirement assumes that a PSP is aware of changes in a customer's personal circumstances when sometimes they are not, either because the customer does not disclose vulnerabilities or customers themselves may not know they are vulnerable. Knowing whether a customer is vulnerable is subjective and, as such, the likely outcome is that **PSPs will need to treat all customers as vulnerable**. The cost of doing so will make many schemes that are designed in support of financial inclusion no longer viable for these PSPs to continue as a business.

Further, the PSR proposes that the cost of reimbursement should be borne equally between the sending PSP and the receiving PSP. This effectively imposes liability on receiving PSPs **even where they have no power to prevent the transaction from occurring**. We question the "default" 50:50 sharing of responsibility which the PSR indicates could be amended by contractual agreement between PSPs. In a market of over 400 operators, where the overwhelming majority of transaction 'initiations' will be carried out by just a handful of retail banks, negotiating a change from the default will, in our view, be very difficult in practice.

We also question whether the lower payment threshold and the (maximum) excess is set at a high-enough level to genuinely incentivise legitimate consumers to exercise caution and heed warnings they receive from their PSPs, leaving the PSP to bear the brunt of consumer inertia.

In our view, the PSR's proposals introduce significant operational costs which will be difficult, if not impossible for newer pre-profit PSPs, to absorb. We are very concerned that the **cost of reimbursement will impact the ability of both new and established PSPs to remain**

**commercially viable**. These costs will have severe implications for innovation and competition in UK payments, and severe implications for digital financial inclusion.

### **A 'Cheater's Charter'**

PIF and its members are extremely concerned that fraudsters will exploit the reimbursement requirement to operate fraudulent schemes to steal money, safe in the knowledge that a PSP is required by law to reimburse the funds, and that the risk of being investigated by law enforcement is, probably, very low. According to the National Audit Office (NAO), fewer than 1 in 200 cases of fraud lead to police charges, with bank and card fraud the most common type. We reiterate our disappointment that no attempt has been made at an ecosystem-wide approach to tackling APP scams, corroborated more broadly by the NAO which concludes that **"tackling fraud is a complex issue that requires coordinated action from government, bodies across the public and private sectors, and the public"**<sup>3</sup>.

We would like to highlight direct debit scams where fraudsters have created campaigns on social media promoting, for example, an opportunity for housing association residents to claim cash back on direct debits already paid for council tax, rent and other payments with the fraudster taking a fee. The scams are typically advertised as an easy, hassle-free way to claim money back from your bank with no consequences. The reality is that victims could be left in debt, facing eviction or receive a criminal record. With the liability placed on PSPs under the PSR's proposals, we foresee similar scams circulating on social media, where consumers are encouraged to claim vulnerability with no consequences. Shifting the liability to PSPs **will create a new opportunity for fraudsters resulting in severe implications for firms** who, unlike larger financial institutions will be unable to absorb the cost of reimbursement

Finally, it is likely that the reimbursement requirement would be widely publicised to the general public. Rather than educating consumers on the decisions they take and the payments they make, it reinforces a belief that their funds are protected regardless of the decisions they take. This encourages a more carefree and careless attitude to payments. **It is a very dangerous precedence to set, and it is not sustainable by the payments and e-money sector.**

---

<sup>3</sup> [Progress combatting fraud \(nao.org.uk\)](https://www.nao.org.uk/publications/2022/progress-combatting-fraud/)

### **Further observations**

Finally, PIF and its members have identified several other issues which we urge the PSR to take into consideration:

#### **The PSR's proposals, if implemented, will obscure the true levels of APP scam fraud**

The administration required to investigate fraud versus reimbursement means that **it will be more cost effective for a PSP to pay out than properly investigate the case**. This will impact on the true amount and value of APP scam fraud taking place.

#### **Existing approach to customer onboarding is not conducive to preventing fraud**

Customer Due Diligence requirements are inconsistently applied across all firms, i.e., banks and non-bank PSPs. If they are consistently applied, then the sector would have a better chance of rooting out fraudsters who steal or create false identities and preventing them from opening an account.

#### **Working with crime prevention agencies**

PIF members have cited several issues when it comes to working with crime prevention agencies. Cifas, for example, is known to have issues in the way it reports third parties submitting fraud information, which creates problems for APP scam victims wishing to use the Financial Ombudsman Service to seek redress. Members are also concerned about the lack of response from law enforcement in cases of card or account fraud – this does not assist the victim or the PSP. Fraud prevention efforts are also hampered by the National Crime Agency's (NCA) lack of resource; it would be beneficial to have much closer engagement between the NCA and PSPs.

In closing, we strongly believe that if implemented, the PSR's proposals will be detrimental to both consumers and PSPs. The firms we represent are spearheading the development of innovative payment products and services, many of which are designed to support the most vulnerable, as well as to help consumers and businesses mitigate cost-of-living increases.

# Prepay Technologies (PPS)

# Authorised push payment (APP) scams: requiring reimbursement

## RESPONSE OF PREPAY TECHNOLOGIES LIMITED (PPS)

This document contains the response of PPS to the Payment Systems Regulator's (PSR's) consultation on APP scams.<sup>1</sup> PPS (Prepay Technologies Limited) is an issuer and processor providing solutions to start-ups and established brands who are appointed as Agents of PPS and require a scalable, reliable, and flexible partner to manage their processing, issuing and account-based needs. PPS is a Directly Connected Non-Settling Participant in the Faster Payment scheme since 2018 enabling access for customers of Tide, Monese, SuitsMe, CountingUp, Mettle and Ekko and others. PPS is a Mastercard Principal Member and an FCA regulated Electronic Money Institution. PPS is owned by global listed entities, Edenred SE and Mastercard SA

We note that PPS is also a member of UK Finance, whose response should be considered in conjunction with this document.

---

<sup>1</sup> Authorised push payment (APP) scams: Requiring reimbursement ("the Consultation Document").



## Executive summary

We support the PSR's ambition to put in place measures within the UK payments system that help to prevent fraud and protect consumers and at the same time maintain trust in faster payment scheme.

However, our strong view is that substantive further work is required to fully understand the potential detriment that could arise from the proposals in their current form, to ensure that they achieve the intended market and consumer benefit. As it stands, the PSR is relying on a number of key assertions to support its views, which in our view could result in some very significant issues, including issues that could cause significant consumer, small business, and market detriment.

First, the PSR correctly recognises that the proposals will require banks to put in place enhanced controls frameworks to mitigate against fraud. In practice, we expect this to mean accounts associated with a greater risk of fraud – specifically **new accounts** and **accounts held by the vulnerable and small businesses** – are likely to face **substantial increases in friction, including reduced availability of certain services and materially delayed payments**.

Second, as far as we are aware, there has been **no detailed assessment** of the costs and/or timeframe of implementing the scheme. We believe that such an assessment would show a **disproportionate impact** on smaller providers and newer entrants to the market, and it should be expected that at least some of this cost will be **passed through to consumers and that some newer market entrants may have no alternative than to exit the market**.

Third, and crucially, **the PSR has failed to recognise the unintended consequences on competition** – and in turn consumer and small business outcomes – that may arise from its proposals. In particular:

- The substantial increase in friction for both the sending and receiving of payments that will be placed on new accounts risks creating a **dampening effect on the incentives to switch**, putting recent work by the CMA and others at risk of being undermined and **creating further consumer detriment**.
- The disproportionate cost impact on smaller providers, and the aggressive implementation timetable, will **discourage market entry and reduce innovation** in the market, working against the PSR's overarching objectives.
- For some providers we would expect this to result in **market exit**, decreasing competition further.
- A combination of the above will worsen customer outcomes, reduce choice, and risk particular detriment to **vulnerable customers**.
- Increased friction the payment flow that will force small businesses who routinely accept faster payments to switch to cash, cheques, or more expensive solutions such as card payments

We have further serious concerns around the impact of these proposals on first-party fraud, which we consider will be increased as a result of the current proposals.

Given the points above, in our view the level of analysis conducted to date is not sufficient to support such a substantial policy change. **A more thorough cost-benefit assessment (and consultation), taking into account the potential negative consequences of the current proposals**, is required to ensure proportionality and that the best outcomes are achieved for the market and consumers.

Furthermore, we consider that the 12-month implementation timetable put forward by the PSR is unrealistic and risks further unintended consequences. Smaller PSPs, and/or PSPs that operate via a portfolio of Agents in particular, lack the scale and resource required for such a rapid change in requirements. While this timeframe may be more plausible for larger PSPs, we **strongly caution against a staggered approach** to implementation, which would place the smaller PSPs at a competitive disadvantage relative to those PSPs, undermining competition, and innovation. As

stressed above, we also foresee a significant risk of disorderly failures with a result market and customer detriment.

We recognise the PSR's position that reimbursement is an important component in addressing the APP scam problem but believe strongly that it is required as part of a wider approach covering education, legislative change, tech development and effective engagement and collaboration of the wider ecosystem, including for example the Enhanced Fraud Data initiative which has the potential to significantly reduce the APP threat.

We are very keen to continue to engage with the PSR to support the development of the most effective solution as the PSR continues to develop its plans.

## Introduction

The Payment Systems Regulator's (PSR's) consultation<sup>2</sup> on authorised push payment (APP) reimbursements asks respondents to consider 27 questions. Conscious that the PSR will receive a large number of responses, our response focuses on only our most substantial concerns. The response primarily relates to questions 1 and 2 from the Consultation Document, although Section 5 also relates to questions 25 and 26.

Our response is structured as follows:

- Section 2 discusses the key areas of concern we have that need to be considered further, including increased frictions, disproportionate cost impacts and the implementation timetable.
- Section 3 sets out the potential distortions to competition that may arise, given these additional friction and costs.
- Section 4 discusses first-party fraud.
- Section 5 discusses the implication for indirect participants.
- Section 6 discusses our views on the implementation timeline.

We also note the specific feedback raised by UK finance separately in its response relating to

- Need for this change to be part of a series of wider ecosystem controls to stop the scams before they reach payment stage
- Gross negligence
- Moral hazard
- Concerns around use of the Faster Payment scheme rules for allocation of liability
- Need for universal adoption across all PSPs at the same time

## Key areas of concern

The PSR recognises in its consultation document that the proposals will likely lead to:

- increases in **friction** that would be caused by implementing enhanced anti-fraud checks on individual transactions (p19).
- additional **costs** borne by PSPs (p67) – including the cost of developing and implementing the solution in a 12-month timeframe, test and learn methods, and

---

<sup>2</sup> CP22/4: Authorised push payment (APP) scams: Requiring reimbursement | Payment Systems Regulator (psr.org.uk)

costs associated with reimbursement where there is no fault on the part of the PSPs and the fraud could not have been prevented.

High level analysis has been conducted on these consequences by the PSR (Appendix 2 of the Consultation Document). We believe further consideration and dialogue with the sector is essential to fully understand the impact of these two factors including, critically, a more explicit analysis of the impact on small businesses who accept Faster Payments as a method of payment

## Frictions from enhanced processes

The PSR states in its Consultation Document that PSPs should put in place systems of “robust fraud controls” (p.21). In our experience, these controls will inevitably **slow the speed at which certain Faster Payments transfers are made, and disproportionately affect certain cohorts of customers and small businesses**

Certain checks can be made automatically and relatively instantaneously. This includes Confirmation of Payee (CoP) checks, although, as noted by the PSR (p66), only a subset of APP fraud would be impacted by such checks. Instead, **manual checks** will be required for a wide range of transactions – at least prior to the implementation of the ISO 20022 messaging standard. Such interventions on the part of the sending PSP will introduce considerable friction to transactions and increase the time taken for funds to arrive in the recipient’s account. This friction could also result in PSPs being unable to comply with Faster Payment Scheme rules and service level agreements (SLAs) and/or represent a Payment Services Regulations 2017 compliance conflict.

Sending PSPs will have to make some determination of the risk of each transaction to prioritise checks and manage resources. This will result in delays to those transactions determined to be ‘higher risk’ – meaning that **certain cohorts of customers are likely to be disproportionately affected**. For example:

- **New customers:** We anticipate that it will be necessary to manually check and verify the initial transactions of new customers, which will likely involve contacting the customer for additional information regarding the purpose of the transaction. Based on our experience in other markets, it can take several days to gain sufficient information from customers to approve and process such transactions. Clearly, market entrants will have a higher proportion of newer customers.
- **Small businesses:** We anticipate that small businesses will be particularly affected by the current proposals. Many small businesses receive payments that raise the ‘red flags’ associated with APP fraud: large, irregular payments from new accounts. We have provided an example to illustrate this point in the box below.

We therefore consider that it is highly likely that certain customer groups would be at greater risk of being a party to fraud and would therefore be subject to **more scrutiny, greater frictions when sending or receiving funds and a systematically worse experience as a result** (in addition to the increased challenges that they are likely to face from a financial inclusion/access to services perspective). We anticipate that such individuals will increasingly have to revert to alternative payment methods such as cash, undermining the ultimate goal of increasing trust in the payment system.

Finally, a material omission from the PSR's set of questions, and based on its draft, its thinking to date, is recognition that small and medium sized enterprises are a category of end user (distinct from individual consumers) that must be specifically understood and

considered. At the highest level, this group are more likely to be regularly receiving payments in a range commonly observed in APP scams, often from accounts that have not previously sent them funds, and in turn more likely than most to be impacted by the friction cited above. The distinct treatment of this group has been observed previous reviews (e.g. the CMA's retail banking market investigation), which have found issues around small and medium sized businesses need specific analysis. This is another example as to why the PSR should be undertaking substantially more detailed work prior to enacting this level of policy change.

### **Case study – increased frictions for small businesses**

Consider the example of a self-employed plumber. Currently, they will often rely on direct payment transfers at the end of a job, which are fast and convenient. Often, the plumber will stay with the customer until the transfer is made.

Payments received by the plumber will be of a size and nature that will typically match those of APP fraud - with no history of transactions between the sender and recipient. These payments are therefore more likely to be regularly flagged as suspicious and held up, whilst the sending PSP conducts manual checks on the transaction. Where this occurs, several hours or days may be required before the checks enable processing of the transaction. The plumber will clearly be unable to stay with the customer for that period, and instead would have to trust that the funds would be received at a later date.

In our view, it is likely that these inevitable frictions will push certain small businesses towards requiring payment in the form of cash or cheques. We note in relation to cheques that most Agency Banking solutions do not support cheques and so this will restrict small businesses to banking with larger more established PSPs, reducing competition. The alternative of demanding payment upfront is likely to be a barrier to attracting customers. Receiving payment via credit or debit card is likely to be prohibitively expensive due to transaction fees.

## **Increases to the cost base**

The PSR notes in its Consultation Document that the proposals will lead to increased costs of reimbursement and that, “for some small PSPs, this could, in principle, have prudential implications” (p21).

We agree with this assertion. In particular:

- Many smaller PSPs are e-money institutions and **cannot cross-subsidise** current accounts with lending products in the way that many larger PSPs do. If the cost of providing current accounts increases – which the PSR recognises it will as a result of its proposals – this will inevitably need to be passed-on in some form to consumers and small businesses
- Annex 2 of the Consultation Document sets out the analysis that has been conducted by the PSR to quantify the costs to PSPs. However, this analysis is high-level and heavily assumption based, meaning it misses the point above. Furthermore, the analysis assumes that the scheme will only reduce the levels of fraud by 20% - 30%.

In relation to the cost benefit analysis conducted in Annex 2, we further note that:

- Table 1 of the cost benefit analysis (p67) does not appear to include fraud that remains following the introduction of controls, which becomes a cost associated with the proposals to PSPs.<sup>3</sup>
- No analysis appears to have been conducted regarding the actual financial cost of investing in fraud detection, or whether this would impact certain PSPs (e.g., smaller PSPs or those serving vulnerable customers) more than others.

## Unintended adverse effects on competition

In our view, these frictions and costs are likely to give rise to important competition implications, which work against key priorities in the PSR's Five Year Strategy to promote competition and innovation in payments systems.<sup>4</sup> and the BCR Capability and Innovation Fund designed to improve the provision of banking services and financial products and services available to SMEs

In particular we believe the PSR's proposals could result in:

- Reduced incentives for consumers and small businesses to switch provider.
- Disproportionate increases in costs for smaller providers, potentially leading to reduced market entry, market exit and reduced innovation.
- Reduced banking access for certain customer groups (including vulnerable customers).

We have provided further information on each of these concerns in turn.

## Reduced consumer and small business switching

As noted in Section 2 above, one factor that is very likely to be used by PSPs to determine the risk of a transaction is the **tenure of the sending or receiving account**.

In such a scenario, the current proposals would inadvertently cause distortions to competition by disincentivising customer switching between providers. Considerable work has been conducted by the CMA, FCA, BCR and industry participants to promote customer switching, including through the development and implementation of the Current Account Switching Service (CASS) and the investments made by the BCR Capability and Innovation Fund which was designed to limit the distortions in competition that resulted from state support

We are concerned that the current proposals are likely to put in place significant disincentives for customer switching, underdoing the good work that has been undertaken in this area, and resulting in considerable consumer and small business detriment.

We note, for example, that the CMA's Retail Banking Market Investigation estimated that a one percentage point increase in switching rates amongst account holders as a result of its proposed remedies would lead to direct benefits to those customers that switch of £317m over five years.<sup>5</sup> It is therefore clear that **even a small increase in the friction associated**

<sup>3</sup> The Consultation Document (p60) states that these costs "will incentivise PSPs to invest more in fraud detection and prevention". However, it should be noted that only the costs of reimbursements that could have been avoided can act as an incentive to invest in fraud detection; if only a 20-30% reduction in APP fraud can be achieved following the investments made by PSPs, the remaining 70-80% cannot also be considered an incentive to make those investments.

<sup>4</sup> In particular, priorities 3 and 4 relate to increased competition and innovation in payment systems.. <https://www.psr.org.uk/publications/general/the-psr-strategy/>

<sup>5</sup> CMA (2016) Retail Banking Market Investigation: Final Report, p.690 <https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf>

**with switching between PSPs could have potentially significant detriment to consumers and small businesses.**

## Disproportionate increases in costs for smaller providers, potential market exit and reduced innovation

Aside from the cost of reimbursement, there are considerable fixed costs associated with designing, implementing and operating the controls that would be required to identify fraudulent transactions. By their very nature, fixed costs **disproportionately penalise small firms and raise barriers to entry** and as such this needs to be carefully considered in the context of the currently anticipated implementation timetable, particularly whilst efficient specifically tailored technological solutions are evolving.

Furthermore, we note the cost of the reimbursements themselves. Whilst the PSR states that the cost is “an intended effect of our proposals” and that “mandatory reimbursement... is intended to incentivise further scam prevention by both sending and receiving PSPs”, it is important to note that robust systems can only mitigate and reduce the risk that a given transaction is illegitimate. As noted in Section 2.2, it is not possible to eliminate risk altogether and, as such, all PSPs will be required to maintain capital to cover the funds that they may be required to pay out. In relation to smaller PSPs and newer market entrants, the macroeconomic climate, impacts of Brexit and reliance on external investment should not be ignored or underestimated when considering their financial resilience to fixed cost increases.

We note that some successful recent entrants began life not as banks but as e-money institutions. It is a realistic possibility that such an operating model would not have been possible under the PSR’s current proposals, and that challenger bank programmes such as Monzo and Tide would not have attracted the investment required to reach where they are today. **By penalising small PSPs and new entrants, the proposals risk deterring future market entry, resulting in lower levels of competition and innovation.**

PPS is a PSP with a range of business activities, only one of which is “banking as a service” where PPS supports market entrants to offer “accounts” to business and consumer customers. PPS engages in this activity to generate innovation that is of long-term benefit to PPS and its shareholders (as well as to the wider market). This activity generates only moderate revenue, and it should be noted that many Agents of PPS do not achieve profitability for a number of years. PPS to some extent sees itself as a “facilitator of innovation and competition”. PPS has enabled successful, innovative and disruptive firms to enter and/or operate in the UK Faster Payments ecosystem.!

As discussed in Section 2, the proposal will increase the overall costs associated with offering banking services – for both small and large providers. In addition to the fixed costs associated with, for example, designing robust algorithms, which place barriers to market entry and disproportionately impact smaller providers, there are marginal costs associated with facilitating Faster Payments; for example, the cost of conducting any non-automated checks and the liability for reimbursement if it later emerges that the payment was fraudulent. In a competitive market, marginal costs are typically passed on to consumers via increases in fees as they cannot be absorbed by firms.

Currently, most banking services such as Faster Payment transactions are provided free of charge as the marginal costs with facilitating a transfer are small. However, the PSR’s current proposals could introduce material costs to both the sending and receiving PSP to facilitating a transfer; **both the costs of conducting robust checks and exposure to the**



**risk** that the PSP will be required to reimburse the sender. Even if the PSP(s) are able, through checks, to satisfy themselves that a large payment is unlikely to be fraudulent, there is limited incentive to internalise all of these costs.

As a result, there is a risk that the PSR's current proposals lead to **PSPs amending the proposition** in order to cover the costs of proposals, **passing at least some of the costs of APP fraud from those directly affected by the fraud onto the population more broadly**. Banks, whose business model involves lending funds, are able to cross-subsidise other products, so may be able to absorb some of these costs. However, PSPs that do not lend are unable to do so; increases in either monthly account fees or transaction fees are inevitable.

As the PSR's proposals apply to participants across a competitive industry, the scheme meets many of the characteristics for observing pass through<sup>6</sup>, and this should be considered in more detail.

## Reduced banking access for certain customer groups (including vulnerable customers)

A number of firms and products have appeared on the market that are specifically designed to provide banking services to certain customer groups (including vulnerable customers and small businesses) and those that are otherwise unbanked. We noted in Section 2 that, under these proposals, **the increase in cost to serve these customers is likely to be disproportionately high relative to a typical banking customer, due to the increased propensity for them to become victims of fraud**. This is not due to a failure of the firm to implement controls, but due to the inherently riskier nature of their cost base.

As noted by the PSR, it would likely be unlawful under the Equality Act 2010 to refuse to provide banking services or charge increased fees to vulnerable customers. However, a more likely outcome is that these customers **receive a substandard service** since their transactions will be required to undergo more stringent checks than a typical customer and – since the Equality Act requires firms not to discriminate against certain groups but does not place any requirements on firms to offer any given product – **certain products specifically aimed at these customers (and potentially firms more broadly) become unviable and cease to exist**.

## Potential impacts on first-party fraud

The Consultation Document states that “[the PSR's] goal is to significantly reduce the levels of APP scams” and that “these measures will provide greater protection for consumers, ensuring that any victims get their money back (with very limited exceptions)” (p.62).

It is clear that the level of protection for victims will be increased. However, we do not agree that the proposals are likely to reduce the incidence of fraud. In particular, **the current proposals provide increased opportunities to commit first-party fraud** – i.e. account holders falsely claiming to be victims of fraud in order to reclaim reimbursements that they should not be entitled to. It is likely that both certain individuals and organised gangs of

---

<sup>6</sup> [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/320912/Cost\\_Pass-Through\\_Report.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/320912/Cost_Pass-Through_Report.pdf)



criminals will seek to exploit this opportunity.<sup>7</sup> Indeed, evidence from the insurance market shows that first-party fraud is significant and increasing.<sup>8</sup>

We believe it is inevitable that PSPs will be forced to make payments to those committing first-party fraud under the proposals, due to the extremely high bar for withholding reimbursements. **This is an important issue that requires further consideration.**

Furthermore, we note that increases in first-party fraud are not anticipated or included in the PSR's cost benefit analysis in Annex 2. This is not a "short term" cost, either – it should be expected to persist over time. Inclusion of first party fraud increases as a cost would – potentially materially – impact the PSR's analysis and should therefore be considered.

## The impact on indirect participants

The Consultation Document states that the proposals for mandatory reimbursement will cover all APP fraud payments over Faster Payments (p.24). The proposals will therefore apply to all directly connected PSPs, as well as PSPs that are indirectly connected via an 'indirect access provider' (IAP).

The PSR's preferred approach to implementing its proposals is through the Faster Payments scheme rules, which means that they would apply only to direct participants. To implement its requirements in relation to indirect participants, the PSR's preferred approach is to make the IAP responsible for the transactions of its indirect customers (p.47). The Consultation Document sets out several advantages of this proposed approach.

The Consultation Document notes that in many cases, IAPs and indirect PSPs are competitors, such that its proposals may raise competition issues (p.48). We agree that there are potential competition issues – likely material – that should be considered, and find it troubling that they have not already been explored in detail in the Consultation Document. Importantly, if the IAP is responsible for the transactions of its indirect customers – and therefore liable for their share of APP fraud reimbursements – this risks significantly undermining the incentives to provide such a service, and has the potential to **reduce access for indirect participants, or materially impacting pricing and service.** In the absence if IAP's the cost of smaller PSP's and market entrants becoming Direct Participants would be prohibitive.

Crucially, the IAP does not have the ability to control the risks of APP fraud amongst its indirect PSP customers. Critical checks, such as 'know your client' (KYC) are conducted by the indirect participant itself, not the IAP. In our view, the IAP should not be liable for risks that it cannot control. These proposals risk undermining the current IAP business model – and therefore reducing overall competition in the market.

## Implementation

Finally, we have **significant concerns** regarding the PSR's proposed timetable to implement its proposals. In particular:

---

<sup>7</sup> For example, a criminal gang may facilitate a payment between two strangers and instruct the sender to report that they have been the victim of romance fraud, with the profits shared with each party. The PSP may have suspicions that the claims are fabricated, but it is essentially impossible to disprove them. We also note the rate of reimbursement of 41% by Contingent Reimbursement Model signatories in 2020; it is likely that a material proportion of the 59% of claims that are not reimbursed is associated with first party fraud. Further, the relatively low reimbursement rate is likely to be a disincentive to make fraudulent claims. Whilst, in principle, it would be of benefit for all genuine victims of fraud to be reimbursed, for the reasons above, placing the burden of proof on PSPs in such a way that reimbursement rates are substantially higher and approach 100% is not necessarily desirable – the unintended consequences may outweigh the benefits to genuine fraud victims

<sup>8</sup> <https://www.insurancebusinessmag.com/uk/news/breaking-news/revealed--the-most-common-types-of-insurance-fraud-in-the-uk-418587.aspx>

- Smaller PSPs in particular will be **unable to implement the proposals within the 12-month timeframe** as they are starting from a different position and lack the scale and resource required for such a rapid change in requirements. The larger PSPs participating in the CRM Code have already made financial provisions for significant customer reimbursements, and have processes in place to deal with the real-world complexities involved (i.e. receiving, investigating and processing claims). These processes take significant time and resource to implement, which is simply not feasible within the 12-month timeframe proposed.
- While this timeframe may be more plausible for larger PSPs, we **strongly caution against a staggered approach** that would mandate that PSPs above a certain size to implement the proposals at an earlier date than those beneath that threshold. As with the introduction of Confirmation of Payee, this would place the payments to and from customers of smaller PSPs under likely increased friction and subsequently see smaller PSPs at a competitive disadvantage relative to those PSPs, undermining competition, and innovation.

Santander

# PSR Consultation Paper: Authorised Push Payment (APP) Scams

## Requiring Reimbursement

Published 29<sup>th</sup> September 2022

## Introduction

Fraud and online scams pose a serious threat to consumers and to the integrity of the UK's real-time payments system. We are supportive of the activity of the PSR in this space, especially the actions to bring a universal approach to liability frameworks, a workable and consistent liability model and an emphasis on fraud prevention design linked to consumer protection.

However, our overarching view is that solutions to reduce this threat and improve consumer protection require *radical thinking*; APP Fraud thrives in a complex ecosystem, universal fraud prevention alongside consumer protection beyond reimbursement cannot be delivered by banks and payments providers alone. Our view is that to truly protect customers there will need to be an alliance across all the sectors that facilitate or enable digital interactions, from payment service providers to large tech firms, social media companies and telecoms companies.

Given the cross-cutting nature of digital technologies, there also needs to be greater leadership, accountability and investment from regulators, policymakers, and law enforcement agencies. If scams continue to originate from vulnerabilities in telephony services, digital platforms, and online marketplaces in future, then there must also be a serious discussion about ensuring their risk introduction is included in any economic incentive or liability model.

**Please note that we do not consent to the publication of this response, either in whole or in part, without prior discussion. We would be happy to discuss our comments with the PSR and can be contacted at [santanderregulatoryliaison@santander.co.uk](mailto:santanderregulatoryliaison@santander.co.uk) to arrange or with any further queries.**

## Question / Responses

### **Question 1: Do you have views on the impact of our proposals on consumers?**

It is clearly anticipated that responsible sending / receiving firms may increase payment friction or reduce the existing service provisions in place in response to the mandatory (save for the stated exceptions) obligation to refund. Interrupted payments suspected of being an APP scam often require human intervention, and an 'APP dialogue' with the consumer to truly 'break the spell' or to provide tailored guidance is not something easily achieved based on the complexity of the problems at hand. The measures required to effectively protect customers are becoming increasingly difficult to implement, especially as firms are finding that consumers often choose to ignore warnings or have been engineered by a criminal to not heed them. It is our view that by enabling fraud prevention controls within the payment infrastructure, such as separating out payments in terms of *fraud risk*, significant operational and consumer restrictions could be avoided, and such changes could also foster significant benefits for responsible payment service providers.

Further thought is thus needed across the industry in terms of the likely result of risk avoidance. There is a high risk of negative consumer impacts associated with PSPs reducing functionality, interrupting more payments, reducing

their offerings (should they consider it financially unviable to underwrite any payment a consumer is making in an unlimited fashion on a macro level) or even limiting certain payments to certain customer groups.

In essence, there is a concern that the longer-term impacts on 'payment processing' are not truly understood and would be incredibly difficult to predict, as there are many different business models operating in this market, and there has been no historic liability framework to learn from. As such, a proposed model for reimbursement may have far-reaching consequences on the real-time payment market (as liability shifts and merchant monitoring programs have in card schemes) and as such the PSR, Pay.UK and firms involved should prepare for and shape this in a meaningful and beneficial way, rather than allowing this to emerge organically.

There are often claims that 'enhanced' data analysis and tools could assist in identifying APP fraud risk from sending PSP only data currently available (i.e. without asking the payment user more questions, or categorising payments, or giving warnings, all treated as friction). This is not actually possible to the extent to which the reduction proves a deterrent for the criminals. A solution (or combination of solutions) that significantly reduces the ability for a criminal to achieve their aims, for example preventing more than 9 out of 10 attempts, to be a stronger deterrent.

Our view is that by identifying payment types, values and flows that are *inherently low risk* (utilities, low value payments cumulatively, 'own-account' payments, or even payments to 'trusted' recipients of various types) and then separating these out in user flows (i.e., how the payment is requested) or into different products could prove to be a viable solution. Improving the flow of low-risk payments at scheme level and applying appropriate and proportionate friction on higher risk payments must be supported in a universally approved framework, rather than relying on PSPs to make up their own logic based on experience and risk appetite.

Further, we do consider that customer behaviour will be altered because of the proposals, as there will be reduced incentive for customers to take responsibility for their decisions which in turn creates a moral hazard and potential financial harm. Contrary to the suggestion that there is no evidence to support this, we would highlight the statistics on page 4 of the consultation paper itself, which flag that in 2021 losses to APP scams increased year on year - post implementation of CRM (i.e. when customers became aware that more protection was available to them).

In addition, we would call on the PSR to recognise that there is likely to be additional friction required within the outbound Faster Payments journey. As such, the PSR should proactively work with HMT/FCA and UK Finance on updating the Payment Services Regulations 2017 and FCA Approach Document to recognise certain higher risk payments should go beyond the "D+1" requirement for delivery into the Payee PSP Account, and to clearly define the specific point as to when the 'clock starts' on payment timelines. It is important that this dovetails with the expectations on customer outcomes that PSPs are expected to deliver under the Consumer Duty.

## **Question 2: Do you have views on the impact of our proposals on PSPs?**

Whilst we accept that the PSR's powers are limited in this regard we would highlight that, in the absence of any wider regulatory or legislative change, the proposals disproportionately impact PSPs and ignore the role of other industries in protecting customers from the risk of APP fraud. Preventing APP fraud is, of course, one of our key priorities, both internally and with our peers across the industry. However, given the complexities of the fraud types included in APP, and how the victims are approached by criminals, any approach that does not consider the elements of the fraud that are outside the financial firms' control does not go far enough.

Put simply APP fraud is a symptom of unhindered consumer interactions with social media, and the ease in which criminals can create mass fraudulent communications; this has to be dealt with to prevent the fraud at source. We must take away the tools the criminal has to reach their victims.

We agree that there should be strong regulatory and financial incentives to encourage the right behaviours for firms (and their clients in some situations, directly or indirectly) that could essentially bring risk into the ecosystem. This means making all participants accountable, to take ownership of their respective responsibilities and to work towards this common goal. This will, in turn, also link into the PSP's respective share of liability (see question 13 below). It will encourage PSPs to take appropriate steps to mitigate APP fraud as a member of the ecosystem and to be adequately capitalised to meet their share of reimbursement claims. To this point, Open-Banking payments should be in scope of the regime, and the role and responsibility of the PISP in sending and initiating a payment must be defined, and reporting at payment level which is transparent and assessed centrally must be initiated. We encourage the PSR to engage with the OBIE and CMA to solve the tensions with the Open Banking requirements in the interests of consumers.

### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

We agree with the universal application of the reimbursement rule and would like to stress that payment service users see no distinction between payment types, so all UK real-time payments should be in scope. The proposed definition will need significant improvement and further detail added to ensure that all firms, especially those not currently CRM members, can easily apply the rules, and be consistent in that application. On this point, there should be consideration given by the PSR and the major card schemes operating in the UK as to what risks there are to increases in 'authorised' fraud types within card schemes, and if the current reporting frameworks and models there are sufficient or require improvement.

We are concerned that, for example, under the proposed definition, mandatory reimbursement could still be seen to apply to private civil disputes where one party might consider the actions of a merchant or trader 'criminal' or perceive that criminal 'intent' exists, in circumstances where that cannot be proved, and the facts are equally consistent with a poor service/breach of contract which falls within the CRM definition of private civil dispute. Much more unambiguous guidance is required on what constitutes a civil dispute and what is intended to be covered by the proposals.

### **4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**

There should be a consumer caution exception, which should be specific to the fraud type in question and should reference elements such as taking note of warnings provided by the sending bank, at the point of payment.

Providers will need to be able to deploy case decision processes around liability and caution, so anything created should be clear, fair and workable.

- **to use gross negligence as the consumer caution exception**

No clear definition of gross negligence has ever been found that is suitable to be applied to consumer fraud cases, especially those linked to digital or modern payment systems. This is despite it being utilised as part of the regulation around unauthorised payments.

However, we accept that this is an appropriate test if properly and unambiguously defined to avoid inconsistency in approach across PSPs and to ensure that there are clearly defined boundaries to act as a reference point for FOS complaints. Given APP fraud is based on *active requests from a payment service user or a consent from a payment service user to allow payments to be taken from their account*, a model is required that allows an assessment of the caution taken, especially if warnings or advice were given at the point of payment (for example via COP), if the customer has not been truthful with their payment provider, or if the customer is habitually falling victim to APP fraud (especially where such frauds have similar characteristics).

**• not to provide additional guidance on gross negligence?**

Clear guidance is essential. Not providing any clear guidance will lead to confusion and inconsistency in approach across firms, which will in turn lead to differing customer outcomes and undermine the credibility / purpose of the proposals. Our view is that if this is the only key factor that needs to be assessed as part of the operational process to work an APP Claim, definition by examples is clearly required. For example, should a customer ignore a directly relevant warning, or recommendation from the PSP, or provide (at the point of payment) misleading or incorrect details, there is significant risk being placed on the sending PSP to underwrite losses on payments, despite the PSP being misled or the consumer being reckless in proceeding with the transaction despite a directly relevant warning.

There is absolutely a need for clarity and consistency in such areas, given the variety of fraud types included, and the possibility of open interpretation of this being applied to a variety of situations. Relying on any developing, or emerging views, such as those taken by FOS is unpalatable as it will be left to how this is interpreted by FOS which will inevitably set a high-level bar for all firms to follow, create inconsistency, drive customer behaviour and give rise to reputational impacts for sending firms, as seen with the CRM.

**5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We have embedded the vulnerability aspects of the APP CRM and believe these should be retained as you have detailed. It is critical that guidance is provided as to the point at which PSPs are to assess vulnerability. We are of the view that vulnerability should be assessed at the point the fraud is committed, rather than any alternative date. In addition, PSR should consider whether in line with FCA Guidance issued on vulnerability, examples and further guidance can be provided in the context of APP fraud.

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

We have no specific comments on this point and agree this is a logical definition to apply. We repeat our comments above, and have implemented an approach aligned to the definitions within the APP CRM Code, which we would wish to retain.

**7. Do you have comments on our proposals that:**

- sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- any 'excess' should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?



We support the provision in terms of an excess and have no further comments. We agree that any excess should not apply to vulnerable customers.

**8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

We support the proposal that a minimum claim threshold would be allowed. However, we believe more granular information and specific guidance should be provided as to what the threshold means in practice for the parties involved, and what expectations should be met, i.e., where reimbursement is not required, is reporting, and managing of recovery and mule account blocking, as per the existing APP CRM. We would suggest there are clear rules and thresholds by fraud type and approach should a threshold be used.

**9. Do you have comments on our proposal not to have a maximum threshold?**

An upper threshold should be in place. This is no different to other consumer protection measures (such as the Consumer Credit Act) where an upper limit or threshold is in place, representing a level at which the value in question is perceived to be outside of the boundary or scope of discussion. Without an upper threshold in place, not limiting a PSP liability increases the moral hazard risk and could encourage PSPs (indeed, we believe it would require PSPs) to restrict payments to reduce this risk as per our earlier points.

We have not here suggested what a maximum threshold could be in place as it would, at this stage, be speculative.

Analysis should be undertaken within the payment systems which could inform a threshold.

**10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

These feel logical and aligned to the existing protocols for unauthorised payment fraud within PSRs.

**11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

The sending bank responsibility is logical, it is much easier for the refund to be provided to the customer this way. However, we would like to see specific measures (potentially financial sanctions) introduced to ensure receiving firms

that do not meet their obligations (and repatriate and recompense their share) are appropriately penalised. To manage this, we believe an interbank reporting system, using infrastructure provided via the PSO would be the best way to both report a fraud, ensure liability is agreed and shared, and then centrally monitor performance metrics on all levels. This has worked well in card schemes, with many more parties involved for many decades.

On the 48hr timescale, we cannot agree, given the complexity of some cases that arise in APP fraud, the need to assess cases to identify gross negligence, and the likely problems arising from recipient bank reviews and judgement. Whilst PSPs should be required to reimburse as soon as possible, imposing such a tight timescale will be setting PSPs up to fail and create complexities in terms of ex post recovery of reimbursement payments from payment service users who were subsequently found to not be eligible for reimbursement. It will be impossible for PSPs to operationalise the review of cases to form an accurate view of gross negligence or otherwise within this timescale. Further, whilst it is accepted that a lot of customers will require their funds returned as soon as possible, in the immediate aftermath of a fraud (which is the period in which PSPs would need to be probing / evidence gathering) some customers may find it distressing to relive the circumstances surrounding the fraud with their PSP. In that context, further time would be beneficial and we see no reason not to retain the current timeframes under the CRM Code.

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Our comments above at Q11 re. the overall timescales are repeated. If those comments are taken on board the discussion as to which cases take longer to investigate will develop organically and will, to an extent, need to be at the PSPs discretion.

We have commented above on the element of gross negligence and have stated that examples of the actions which would be deemed to be gross negligence should be covered explicitly (even at a high level) to avoid confusion. First party fraud assessments should already be taking place for unauthorised fraud protocols, and we would expect firms to apply the same controls and logic.

On this point, there are significant issues across card fraud globally relating to 'friendly fraud' and as such learning should be taken as to how these could be combatted, for example using centralised data to review claim and fraud rates.

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

We agree that this is a suitable default, however we do believe that there are a number of specific situations where liability should fall directly and wholly on one party.

In addition, not all firms have equal controls and therefore the 50:50 measure can only apply where that is the case.

For example, we would like to ensure that where a receiving bank has failed in their KYC requirements and opened an account in a false identity or as part of an impersonation / social engineering situation, the responsibility of failure is weighted appropriately.

Given the regulatory position here we do not believe this should be problematic to include from the outset. Similarly, and linked to the intelligence sharing requirements in place across PSPs to help prevent APP scams (as set out at

paragraph 2.9 of the consultation paper), PSPs who fail to use that intelligence to shape their fraud practices should hold greater responsibility in instances where such intelligence could have prevented the scam.

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria? a**

We agree that this should be part of the design of the protocol. How this is achieved must be clearly defined and must not be unduly onerous to ensure engagement from PSPs (without clear rules, we predict that any form of discretionary dispute resolution scheme is destined to fail). Our position remains that what is required is a clear scheme structure, which could be influenced by specific sending or receiving bank 'risk indicators', as has been done historically in card payment schemes.

We repeat the examples set out in the answer to Q13 above (which are not exhaustive).

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

In the introduction to the consultation, the phrase '*APP scams happen when fraudsters trick someone into sending a payment to a bank account controlled by the fraudster*' is used. Our view is that the rules should be positioned directly around this point and be limited to cover payments from an account directly to the *recipient account* and reflect how that is controlled by the fraudster.

In the example used of a crypto wallet (in section 5.1), based on the complexity of the fraud we experience today, some examples for consideration are below:

- A) Victim's bank account to 'Wallet' – in customer's own name, controlled by customer, opened by customer before the fraud, or at the request of the criminal
- B) Victim's bank account to 'Wallet' – not held in customer name
- C) Victim's bank account to 'Wallet' – opened in customer's own name *by customer*, but then only / later controlled by the fraudster

**Case A** – the original account PSP did not make a payment to an account controlled by a fraudster; it undertook a customer-to-customer transfer. Absent any anomalies (based on prior customer behaviour) which would alert the original account PSP to the potential for a fraud it is not possible to understand how in such a situation, a 50:50 split between that original PSP and the recipient PSP could be applied as the original transaction would likely be deemed an inherently low risk transaction on the initial sending PSP's part. This transaction should not be covered by the proposals.

**Case B** – assuming the wallet is controlled by the fraudster, the 50/50 rules should apply. Relevant checks could reveal this as higher risk.

**Case C** – the recipient firm already have requirements to manage impersonation fraud, unauthorised payment fraud and KYC, and as such, there are other obligations already in place that should provide consumer protection here. In such cases, 100% liability on the recipient firm should be in place

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

No comments at this time, this seems like the most simple and logical approach. However, if the allocation of liability between the sending firm and recipient firm is not 50:50, the allocation of repatriated funds should follow the allocation of liability between the two firms and, if relevant, the customer.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We agree that the incentive is clear and the statistics in the consultation support this. However, as to our earlier comments on 50:50 splits, there are several specific situations (some detailed below) where liability could be deemed to fall on either side 100%, where specific considerations have not been met:

- Usage of Confirmation of Payee by either of the firms
- KYC failures (account opened with false details or as an impersonation)
- Prevention Capabilities – i.e. no evidence of either inbound or outbound payment profiling, APP Fraud warnings etc.
- Recipient account opened in an unauthorised fashion (i.e. victim socially engineered to open account in their own name)
- Previous payments to an account reported to the PSP as fraudulent and not acted upon by that PSP
- Overall mule fraud rate over a set threshold

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

A liability model that protects consumers and creates the correct risk prevention culture must be required for all PSPs.

There must be a driving central force defining future measures on fraud prevention as well as leading the thinking on the correct consumer protection model that is needed for real-time payment systems; at the heart of this must be thinking that revolves around the reason for the payment, the intent of the payee, risk assessment of the recipient and processing rules for different payment reasons. It is our view that APP fraud could be a significant driver for payment system changes, innovation and to find different 'ways' of making payments.

To enable APP fraud to be 'designed' out of the system the anatomy of those frauds must be assessed, and then solutions and design features be introduced to significantly reduce the occurrences.

The direction of travel here is the suggestion that Pay.UK should develop significant new capabilities, obligations, data standards and overlay services (as part of the NPA); there is clearly a need for the activity being described but given the existing ask on Pay.UK as an organisation, and that this process may take several years and the urgency of mitigating fraud losses in the short term, an appropriate plan detailing the strategic and tactical workstreams is needed, and an agreement as to whether a new body could be created to form and develop the structures needed. Should the PSO have a direct role in the reimbursement framework, including liability models between firms and customers / between PSP's, this is a significant role that we do not believe will be swift to implement, and is not a role the existing PSO could perform.

It would be important to ensure that Pay.UK has the relevant capacity and capability to conduct the administration and enforcement of the reimbursement rule as outlined by the PSR. As Pay.UK may not be able to support this scale of change; with the focus on delivery of the NPA and prevention solutions such as the Enhanced Fraud Data solution / Fraud Overlay, extra requirements to become a centralised risk oversight body essentially also, a dispute scheme governing body, provide tech solutions that do not exist today for Faster Payments may be a significant problem.

We feel very strongly about the need for a centralised, transaction level, scheme provided fraud reporting service. This has been a gap for many years in the UK payments system. The PSR should, through their powers direct the PSO to create such a service, which would mandate each PSP to report all their unauthorised and authorised frauds at transaction level to the scheme, and route messages (as a core part of that reporting) from the victim bank to the mule bank, to ensure full transparency. Such protocols are a key part of card schemes (for example SAFE reporting in MasterCard) and enable universal feedback and centralised fraud rate calculations to be achieved.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

The minimum set of rules seems sensible based on your proposals, covering timing, allocations, and dispute resolution. Given there will be a significant number of firms (especially recipients) being covered and taking liability for fraud cases for the first time we would also recommend some further steps. Most importantly of these is that the rules must be extended to include scheme reporting of fraud at transaction level by all firms in scope of the rules, as that would be the key precursor to the rest of the requirements you have defined.

We would suggest the minimum set of rules would benefit from the inclusion of the below:

- A worked definition of gross negligence – we recognise that there may be certain instances specific to a particular fraud, but many fraud types are known and so would benefit from examples of what could include gross negligence. Importantly, the PSR should clarify that repeated frauds can demonstrate gross negligence.
- PSR directions and scheme rules should include requirements on banks to complete data sharing on fraud types (Measure 2 in the PSR Consultation). This will support data sharing on the grounds of legal/regulatory requirements (rather than needing to rely upon consent).
- Liability should be included within the scheme rules and importantly the interaction with Confirmation of Payee and the CoP rulebook should be considered closely.
- Mandatory scheme fraud reporting, at transaction level into a central repository, including relevant information to APP fraud such as CoP utilisation.

Our experience of the nature of this area is that many firms have significant administration functions linked to fraud admin, chargeback, refund and dispute services. We believe the effort to create these should not be underestimated, especially for firms not currently part of the CRM / UK Finance BPS.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We would suggest that use of Section 55 FSBRA is probably the most appropriate mechanism for the PSR to direct the Faster Payments Scheme. We would however expect that any direction under Section 55 recognises that Pay.UK should be undertaking a full consultation process with bank's given the nature of the change. However, we would suggest that guidance (for example on what will constitute "gross negligence") as well as changes to the PSR 2017 should completely any change to the scheme rules.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

We agree that a centralised and universal approach is required and refer to our points above in relation to the impacts on Pay.UK and their specific experience in this field as an organisation.

A likely outcome could be a separate body is set up, resourced appropriately with skilled persons in the fields of fraud management in payment schemes, legal frameworks and technology, to design an appropriate model that could be operationalised by Pay,UK.

We also believe that the 50:50 position is not appropriate in some situations, especially where failures by the PSP who manage the recipient account occur. We have detailed this in our earlier section on reimbursement.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

Introducing new roles to the PSO such as monitoring compliance and dispute resolution does not fit within Pay.UK's current role and we would suggest that such significant changes are not likely to happen quickly and would require significant organisational change and investment. We refer to our comments in the above sections.

**23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We do not have enough information about the requirements on Pay.UK to meaningfully comment on this point. However, we would like to ensure that the alignment with the key central needs of the PSO are aligned with the NPA as well. We see the following as key requirements:

- Systemised reporting of fraud at transactional level, mandated and a system provided to all PSP's for this purpose.
- A requirement on a central body to analyse, monitor and set thresholds to put firms into special measures based on suitable KPI's.
- A technical model that supported the automated allocation of liability and the recovery of funds remaining at the recipient firm.
- A clearly defined role and mandate for oversight and accountability, and detailed measures that could be applied by to firms that are not performing.

We would also suggest it is important that Pay.UK (and PSPs) are given clarity on how their compliance monitoring will interact with other monitoring regimes (for example FCA, CMA and indeed even the PSR's own monitoring).

**24. Do you have views on the best option for short-term enforcement arrangements?**

Of the suggested arrangements (C) *Pay.UK applies its own enforcement regime, but with escalation to the PSR* is the most appropriate in our view. It is pertinent to return here to our concerns as to the capability of Pay.UK in this regard and note the uncertainty around any timescales for such a change given the lack of experience in such a fraud / liability enforcement regime.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

We would suggest that Pay.UK should give thought to applying the reimbursement rules to indirect participants and would suggest this is best served by the direct participant sponsoring bank standing behind the reimbursement obligations of indirect participants (as they would the settlement obligations under the UK Payment Schemes today). We expect this would require update to the legal architecture of the FPS Scheme rules to include liability accrued by Indirect Participants for APP Fraud and will require consultation.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

Our view would be that a firm capable of operating accounts in such a way that could enable them to be included in any APP Fraud liability framework should be appropriately regulated, controlled, and managed. As such, the PSR should give a direction to all indirect PSPs to comply with the reimbursement rules in Faster Payments.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

The cost benefit analysis appears to have been carried out in a detailed fashion, and we agree with much of the detail. We agree that requiring receiving PSPs to share 50% of the costs of reimbursement provides a strong incentive to reduce their exposure in various ways.

This is an established model in other payment schemes and is a logical step, universal application of this is welcomed.

**28. Do you have any other comments on the proposals in this consultation?**

As outlined above, we would suggest that the PSR work with the HMT/FCA to updates to the PSR 2017 and Approach Document to allow PSPs to delay payments (beyond D+1) in certain higher risk payment typologies. For clarity, in addition to submitting this response to the consultation, we have fed into the UKF response. Where the UKF response adequately covers Santander UK's position we have taken the view that it is not necessary to repeat those points in any detail below.

# Stafford Railway Building Society



- 1) Smaller Societies who operate passbook savings accounts only and use reference numbers as opposed to sort codes and have implemented a “closed loop” for funds withdrawals, recent updates confirm the need for a “respond” functionality under COP is not required. For the “send” requirement, if the Societies clearing bank provides a COP response for payments in, taking proportionality into account, would this satisfy the “phase 2” criteria or is there still the requirement to have a dedicated COP solution in place that may involve considerable cost to the Society.
  
- 2) The consultation seems very much “one size fits all” when it comes to reimbursement of funds with no proposed upper limit to the amount of reimbursement. This could have a detrimental impact on smaller Societies. The paper is silent on proportionality when it comes to the size of the firm and turnover. Further clarity is required on responsibility, if the account holder is transferring money from a “closed loop” savings account to a nominated bank account, it would seem unjust to penalise the sending firm when the purpose of implementing a nominated bank account is to mitigate risk and fraud.

# Starling

## [CP22/4: Authorised push payment \(APP\) scams: Requiring reimbursement](#)

### **Starling Bank response**

**Response date:** 9th December 2022

**Sent to:** appscams@psr.org.uk

### **Introduction**

Starling Bank welcomes the opportunity to respond to the PSR's Consultation Paper ("CP22/4") regarding the mandated reimbursement of Authorised Push Payment ("APP") scams. We fully support the PSR's intended aims of preventing APP scams from taking place, and ensuring victims are best protected. We support the PSR's aim of providing a fair level of protection to consumers, and so welcome the introduction of a consistent approach to consumer protection across the industry. However, as detailed in the response below, we do not consider mandatory reimbursement to be the only avenue, and hope to offer alternatives to provide an element of balance as regards to consumer responsibility.

### **Key Considerations**

Starling's number one priority when considering APP scams is prevention, and a significant amount of time and effort is devoted to this cause. The Bank supports the PSR's endeavours to see improvements in this area across the industry, however a reimbursement model in isolation does not constitute consumer protection. This is likely to lead to a number of unintended consequences which need consideration.

Firstly, the inclusion of mandatory reimbursement of victims removes any responsibility on the customer, and it's this moral hazard which we believe is likely to have a negative impact on the volume of APP scams recorded. In order to prevent scams from happening, there needs to be a balanced approach, including customers taking some responsibility. Creating an uncapped, near strict-liability regime is likely to increase APP fraud volumes by creating moral hazard and even provides an incentive for first-party fraud.

To reduce APPs it is also vital the whole ecosystem is taken into consideration. Starling reviewed some recent data and found in cases raised April - September 2022, where known, social media firms were the recognised 'enabler' for the scam in 60% of cases. Similarly, telcos were the 'enabler' for 30% of the total value of claims (with social media accounting for 23% of the total claim value). Both of these statistics highlight the importance of engaging with these industries to really make an impact on the prevention of scams. Starling acknowledges that the PSR are engaging with other government and regulatory bodies to address this, however there is the risk that putting full financial responsibility for scams on to PSP's removes any burden on the wider ecosystem, reducing their incentive to intervene. Starling encourage the PSR to continue to work with government and other regulators, such as Ofcom, to develop a cross-sector approach to tackling scams.

Another key consequence is the adverse effect these measures could have on the faster payments system. Working alone, PSP's only have a small time period to detect high risk transactions and interact with customers to understand whether it's a payment resulting from a scam or a genuine payment. With this in mind, there is a significant risk that genuine payment journeys are slowed down, as PSP's implement more friction in an attempt to prevent APPs. This cost of implementation will ultimately be passed onto consumers who are not victims, but individuals trying to make genuine payments.

Ultimately, focus has to be on what more can be done to prevent scams, both as an industry and across the wider ecosystem. The key to this is data. Authorised push payments capture very little data within the transaction, so there needs to be improvements to the way PSPs capture information from a customer, and send this to the receiving bank. Changes are on the horizon (such as the New Payments Architecture and ISO20022) which provide opportunities for change. Starling Bank has been working alongside the industry to help develop new data sharing standards and fully support this process. However it requires support from the regulator, government and scheme operators to ensure any changes are properly designed and implemented across all PSPs. With this in mind, the proposals to define an operating model and code of conduct that all faster payment participants must comply with is welcome. However, as aforementioned, reimbursement alone is not a solution, and the industry wide approach required should be one of technical innovation and data sharing, to design APP fraud out of the payment system.

## Chapter 3 - Outline and impact of proposals

### Potential impact of our proposals on consumers

#### Question 1: Do you have views on the impact of our proposals on consumers?

Starling Bank is in agreement with the PSR's statement that "preventing more APP scams in the first place will reduce the emotional distress caused to victims". Prevention is a priority focus for the Bank when considering APP scams, and a significant amount of time and effort is devoted to this cause. Whilst it is understood the PSR also aims to achieve this, we don't think the proposals go far enough with this regard with too much focus on providing reimbursement. As a result, this is likely to lead to a number of unintended consequences, which are detailed below.

#### Payment friction

As acknowledged by the PSR, the introduction of mandatory reimbursement of APP scams is likely to increase the amount of friction PSPs apply to the faster payment journey, in an attempt to prevent scam payments. The PSR note they expect "additional friction for a small proportion of payments is proportionate to preventing APP scams", however this is at risk of severely underestimating the impact, which is particularly important when considering the highest volume scam type, purchase scams. The nature of these scams, the majority of which are low value, means it is extremely challenging for PSPs to differentiate the scam payments from genuine, day-to-day transactions. In line with industry figures, a review of data from March - November found 73% of all scams reported were purchase scams, of which 91% are under £500. Any measures a PSP undertakes to

prevent these will naturally increase friction across the payment journey, and ultimately begin to diminish the benefits of the faster payment system.

Starling notes the PSR also places great confidence on the future data sharing initiatives minimising the number of payments which are stopped unnecessarily. Starling is fully in support of data sharing initiatives, and is engaged in industry wide workstreams to this effect. There is no doubt that better data sharing is key to having a positive impact on the reduction of APP scams, however this assumption that it will not slow down payments is not yet proven. In fact, there is the risk it might actually have an adverse effect. With more information to hand, there might be cause to slow down more payments as PSPs wish to verify payments and information at hand, and it's likely to be especially true at the outset of any new process.

#### Vulnerable customers

Without great care, there is a risk these measures will have a detrimental impact on this cohort of the population. The PSR have acknowledged this in relation to older customers, however this risk extends to all customers considered vulnerable to scams. PSP's will not and should not refuse or deny banking to this cohort of customers, however with these proposals in mind it does put considerable pressure on how best to mitigate the additional risk. It's likely to lead to more payment refusals as PSP's have limited options to take. Not only does this juxtapose regulations set out in the Payment Services Regulations 2017 (PSRs 17), but it's also going to result in an increase in dissatisfied customers. PSP's are increasingly seeing disgruntled customers migrate to different PSP's until they get the outcome they want, however this is increasingly at risk of creating an 'unbanked' cohort of society. It is likely to also put pressure on law enforcement, through increased use of the Banking Protocol. What would be beneficial, is the creation of an official channel for PSPs to report concerns that a customer may attempt to send funds related to a scam to another bank account. This might be an extension of the UK Finance BPS platform. This will enable PSPs to alert each other of concerns, so applicable protection measures can be put in place.

#### Complaints

All of the above will likely contribute to an increase in customer complaints reported to PSP's. As CRM code signatories, and with a strong focus on prevention, Starling has already introduced a sophisticated payment monitoring system with customer facing warnings to detect unusual payments. A priority with this was to make it user friendly and to have as little impact as possible. However despite this, there are already complaints received regarding new friction created, with customer's high expectations of faster payments. It's expected this will only be exacerbated by the changes which might have to be made, which are likely to impact more genuine payment journeys.

### **Potential impact of our proposals on PSPs**

#### **Question 2: Do you have views on the impact of our proposals on PSPs?**

These proposals are going to have significant consequences for PSPs. It goes without saying that financially, the impact will be great. However the proposals are also posing significant operational challenges which require much thought and are all discussed in more detail throughout the rest of this response.

### Financial impact

Whilst we are supportive of the PSR's proposal that the cost of reimbursement is shared across all faster payment participants, there is no doubt the biggest impact on these proposals will be financial for PSPs. Mandating the reimbursement of all claims (with the exception of 'gross negligence'), and introducing a 50:50 reimbursement model will unquestionably cost PSPs more. There is also the increased operational resource which needs to be taken into account. The increased focus on prevention, balanced with a requirement to limit impact on genuine customer payment journeys, will require increased operational overheads to ensure this balance is struck correctly. More generally, the PSR should consider the wider implications of this across the financial services industry. This cost might be absorbed in other areas, such as the introduction of fees. This might have a longer term impact which should be taken into consideration.

### Operational challenge

There are numerous operational challenges to consider. Firstly, and as previously mentioned, these proposals will naturally result in an increase in monitoring both inbound and outbound payments, including conversations with customers to truly understand the purpose of the payments. Not only does this need to be considered from an operational perspective as part of the initial payment journey, but also after the payment has been completed, with the potential for increased complaints received from customers who see more friction across genuine payment journeys.

Next, adhering to the specific proposals in the paper come with significant impact on operational teams:

- The 48 hour timeframe is extremely tight, given the investigation which is required to establish first party fraud, or whether a claim is a scam. It's often reliant on communication with the customer or the other Bank, which makes completion of this process in 48 hours impractical and not without consequence (this is discussed in more depth in question 5).
- The 50:50 reimbursement split (as well as the repatriation proposals) are going to have significant operational implications which must be considered. There is currently no streamlined process to move or track money around different PSPs, and introducing a 50:50 split across all faster payment participants is going to be increasingly challenging, given the vast array of PSPs this might involve. This is exacerbated when considering some cases involving payments to multiple firms, so tracking these refunds will become extremely complex (this is discussed in more depth in question 13).

### Legal challenge

As already mentioned, the additional friction the proposals will create on payment journeys is a reality to be expected if PSPs are to increase their efforts to prevent all scams, regardless of type or value. This brings additional legal challenges for PSPs, as there is currently no legislation which supports holding payments over 24 hours ('D+1') in order to be satisfied they are part of a genuine transaction. Increased regulatory comfort in this space is required should these proposals become reality, to ensure PSPs can do all they can to protect customers from scams. We recommend the PSR consider changes to the Payment Services Regulations (PSRs) 2017, specifically clause 86, to allow PSPs to pause the execution of a payment past D+1, where there is believed to be a very high risk of fraud. There is a similar situation for receiving firms. In our ambition to put prevention at the forefront, the Bank has built sophisticated tools for identifying unusual or suspicious

inbound payments. With these proposals in mind, the scope of this monitoring might be widened. However regulatory comfort and protections are required to allow PSPs to freeze and release funds back to the sending firm following an assessment of fraud. The PSR should engage with the FCA on how the relevant sections of PSR 2017 operate in this context. Clarity is required on what constitutes “exceptional circumstances” and the grounds where these payments can be held or even refused.

## Chapter 4 - Mandatory reimbursement for consumers

### Potential impact of our proposals on PSPs

#### **Question 3: Do you have views on the scope we propose for our requirements on reimbursement?**

Generally, there needs to be more clarity from the PSR on what payment and/or scam types are in scope. To assist with this, Starling Bank has considered the following.

##### Purchase scams

Generally speaking, purchase scams pose a very different problem for PSP’s, and have a fundamentally different impact on victims. As aforementioned, the nature of purchase scams, of which the majority are low value, means it is difficult for PSPs to differentiate the scam payments from genuine transactions without the introduction of a significant amount of payment friction.

From a customer perspective, Starling strongly believes low value purchase scams need to be treated very differently to scam types such as impersonation or romance scams. These are the life-changing APP scam types that PSP’s should be striving to prevent, but instead these proposals are leading to the financial services industry underwriting online purchases conducted with little or no care taken by the consumer. Purchase scam claims also pose difficulties when it comes to assessing whether they should be considered a scam or a civil dispute. A review of Starling claim data from H1 2022 found that of the cases which were identified as civil disputes, 61% were purchase scam claims. Further, of this cohort, 52% were for purchases under £100. For claims of this type, there is often limited evidence, and it can take time to investigate. This is contrary to the 48 hour SLA which is later proposed, causing an operational burden on the teams.

Taking these risks into consideration, the fact purchase scams are fundamentally different to all other scam types, and the high proportion of purchase scams which originate due to enablers such as online auction sites and social media platforms, Starling recommends this scam type be excluded from scope of the proposed mandatory reimbursement model.

##### Cryptocurrencies

Cryptocurrencies are a complex area which require more thought and clarity with reimbursement in mind. Not only because the industry is already seeing scam payments increasingly migrate to this sector (in particular with investment scams), but also because the number of crypto exchanges in the market is growing on a daily basis. There are also often differing interpretations between PSPs, the regulator, and the Financial Ombudsman

Service as to what point in the payment chain a scam has occurred, so clarity in this area is required. Due to the increase in scam payments in this space, Starling thinks crypto payments should be considered in scope, however the PSR need to consider how they can loop in what is predominantly an unregulated landscape.

#### Open Banking

The PSR have proposed mandatory reimbursement covers all scam payments over faster payments, including PISP-initiated payments. It is not clear where the PSR expects the responsibility to lie here, and there is an assumption the PSR considers it to be with the Account Servicing Payment Service Providers (ASPSP), but this should be made clearer.

#### Other areas for consideration

- Lack of supporting evidence - There must be exceptions for occasions where the consumer has not provided sufficient evidence to the PSP to enable the investigation to move forward. Customer cooperation is fundamental to ensuring genuine scam claims are fully investigated.
- Ponzi/pyramid schemes - these schemes are often high in case volume and escalate quickly over multiple different PSPs, creating a certain degree of complexity. However there needs to be consideration of whether these are deemed within or outside of scope for reimbursement. At present, it's been agreed that these cases will be considered in scope whereby the 'investor' is aware that the success of their financial return is dependent on recruiting others. However to get to this point of understanding requires coordination across PSP's and communication with the customer (both of which will likely take these cases over the 48 hours threshold).
- Hybrid scam payments - as might be expected with the increased friction within the faster payment journey, PSPs are already seeing a migration of scams away from this channel and into the card space. Often, one scam case might involve both authorised card and faster payments, so consideration should be taken as to potential inconsistencies in this space, where the faster payments are refunded under this mandate, but perhaps the card payments aren't.
- Law enforcement involvement - the PSR need to allow for certain (typically complex) cases which, due to their law enforcement involvement, are deemed out of scope (at least for a time period) until the relevant investigation is completed.

<b>Exceptions for first party fraud and gross negligence</b>
--

#### **Question 4: Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

Starling Bank believes that through guaranteeing the refund, it removes the risk from the customer's decision making process, and actually consumer caution is key to fighting fraud. Rather than driving a reduction in APP scams, this high bar proposed may instead enable consumers to take risks which would previously have been out of character. This warrants any warnings PSP's provide though the payment journey largely redundant, and it also makes any additional conversations with customers about specific payments more



challenging. With this in mind, Starling recommends a ‘consumer caution’ exception is applied to mandatory reimbursement. This should include:

- Where customers have ignored relevant safety advice or recommendations which their PSP have provided them with throughout the payment journey (this should include instances where law enforcement, via the Banking Protocol, is engaged);
- Where customers have been dishonest to their PSP, or provided misleading information as part of the payment review process;
- Where the customer and their PSP have agreed the payment is a scam, however the customer later resumes payments to the same payee/payments are made as part of the same scam;
- Where the PSP has advised the customer it’s a scam payment, but the customer wishes to continue with the payment regardless.

The PSR has not defined gross negligence. The terminology “adequate caution” and [gross negligence as a] “high bar” is used within the consultation paper, but it’s not articulated what this means from a liability perspective. Without clarity, this will lead to inconsistencies across the financial services landscape, especially given the lack of legal definition. Most importantly, PSPs, customers and 3rd parties such as the Financial Ombudsman Service (FOS) need to be on the same page. Guidance and examples will help considerably in reducing the ambiguity of this issue and will ultimately provide better customer outcomes.

**Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

Starling Bank is in agreement that where there is evidence that the nature of a customers’ vulnerability is such that it would not have been reasonable for the customer to have protected themselves from falling victim to a scam, PSPs should be required to reimburse, although as per the following question, we do not align with the PSR’s proposal on the definition of vulnerable in this context.

**Question 6: Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?**

The definition of a vulnerable customer used by the FCA lacks the specificity required in the APP scam landscape. Generally speaking, whilst Starling Bank considers all customers under the FCA definition of vulnerable customers, in the context of scams Starling considers the current definition of vulnerability used within the CRM Code to be the definition which should be used going forward. Vulnerabilities are both dynamic and wide reaching, and so this should be considered on a case by case basis.

A customer who has certain vulnerabilities is not necessarily susceptible to all scams, and it depends on when the payment is made and the customer’s susceptibility at the time. For example, just because a customer is hard of hearing, does not necessarily make them more susceptible to a purchase of a new pair of trainers from social media. There is no evidence that the decision to make the purchase has been altered by the customers’ physical vulnerability, and it is unlikely that a PSP is able to act with “appropriate levels of care” which do not include severely restricting the customers payment abilities on their account.

Equally, a customer may in ‘everyday’ circumstances not be deemed ‘vulnerable’, but the timing and nature of the scam might suggest they are vulnerable at the time the payment was made (influenced by factors such as life events, mental health conditions or caring responsibilities). We would therefore recommend continuing with the existing definition of vulnerability as outlined within the CRM Code.

### **An allowed fixed ‘excess’**

#### **Question 7: Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement**
- **any ‘excess’ should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?**

Applying an ‘excess’ threshold of £35 is considered too low to have any meaningful impact on consumer behaviour, and it’s also likely to create confusion amongst customers who may hold accounts with multiple PSPs across where the thresholds differ.

Starling understands why the excess has been proposed, however in reality this amount would have no impact on incentivising customers to take care when making a higher value payment. For example, taking a payment of £500, it is reasonable that customers would still take the risk of a payment being a scam, to secure a reimbursement of £465. To drive better customer behaviours and reduce the risk of morale hazard, we recommend the PSR consider an alternative option, such as making the excess a percentage of the total claim (with potential to be capped to reduce impact on high value cases).

As well as confusion for customers, allowing for optional application of this excess, of “no more” than £35, creates operational complications for PSP’s. When considering the 50:50 reimbursement, where the application of an excess varies between firms this will create ambiguity when determining the amount to be refunded. Competition also needs to be taken into consideration. If one PSP utilises an excess for each case, but another firm doesn’t, that sets a benchmark which the PSR should consider the impact of.

Starling is in agreement that for vulnerable customers, any excess applied should be discounted at the PSPs discretion.

### **Allowed minimum and maximum thresholds**

#### **Question 8: Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

Starling Bank agrees that PSPs should be allowed to set a minimum threshold for the reimbursement of low value cases. However, there are challenges which need greater consideration.

If this proposal is to encourage customers to take an appropriate level of caution, the minimum claim threshold needs to be higher than £100, and having reviewed internal data, Starling would recommend the PSR consider increasing this to £250 at a minimum. It also needs to be mandated - allowing PSP's to choose their minimum threshold for reimbursement is not only going to result in inconsistencies across the industry, it might also lead to increased competition risk.

Scam type needs to be taken into consideration with this proposal, as again categorising each together does not work within these proposals. There is a significant difference between someone who's lost £100 because they were trying to purchase a new iPhone through social media, and someone who paid £100 to obtain a loan they need to pay bills. Whilst the amount lost is the same, the 'loss' here is fundamentally different, and will have differing impacts on individuals. This is another reason lower value purchase scams should be exempt from this proposal altogether. The risk should sit with the customer and they should bear some liability for their decision to buy goods / services online. PSP's will continue to have difficulty in confirming the 'intent' of a customer's actions (for example when a builder has not completed work to a customer's satisfaction), and it's near impossible for a PSP to confirm with 100% accuracy whether goods purchased through an online marketplace were or were not received.

Starling Bank agrees vulnerable customers should be exempt from any minimum threshold set.

**Question 9: Do you have comments on our proposal not to have a maximum threshold?**

Starling Bank strongly recommends implementing a maximum threshold within these proposals. The lack of an upper threshold would bring unlimited risk for PSPs, and firms might respond by lowering transaction limits on specific payments. The Financial Ombudsman Service (FOS) implements a maximum award limit of £375,000, and it makes sense to mirror these thresholds. Starling recommends this should also be on a per claim basis (rather than transaction).

<b>A time limit for making claims for reimbursement</b>
---

**Question 10: Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

Starling Bank is in agreement with the proposal to set a time-limit for claims to be considered for mandatory reimbursement, although it needs to be mandatory and alongside this there also needs to be consideration of a date set whereby this comes into force i.e. claims for reimbursement can only be made from any date on or after the PSR's liability model enters into effect.

There is clarity required with the proposed 13 month time-limit, which includes the following:

- In a case with multiple payments, would the 13 month time-limit be from the first or last payment? More clarity is required here.

- It is stated within the paper - “We think the vast majority of consumers would become aware that they were the victim of a scam, and be able to make a claim, well within 13 months.” Starling believes this statement to be incorrect however, as it isn’t taking into consideration romance and investment scams which typically occur over a longer period of time, often well over 13 months.

## Chapter 5 - Allocation of reimbursement costs

### Responsibility for reimbursing the consumer

#### Question 11: Do you have comments on our proposals that:

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

Starling Bank is in agreement with the PSR that to ensure best customer outcomes, the sending PSP should reimburse the customer in the first instance. However the 48 hour timeframe is unrealistic when taking into consideration the steps which need to be taken before any reimbursement can be made.

The sending PSP needs to conduct a thorough investigation to assess the potential for gross negligence or first party claims, which is not always a simple process. It is likely to include further communication with the customer, or perhaps with the receiving PSP to understand the nature of their customer's account (the beneficiary) and the relationship between the payer and payee. With this in mind, the PSR should take into consideration the difficulties different operational models will cause - not all PSP's work on a 24/7 basis and will naturally create delays to this process.

PSP's also need appropriate time to assess whether claims should be raised as scams, or treated as civil disputes. A review of the data from the claims received by Starling Bank customers in H1 2022, found 21% of these were civil disputes (36% by value). This demonstrates the high number of civil dispute cases which are received and which require additional review and insight from other parties before any reimbursement decision can be made. Both contacting the customer or the beneficiary bank are elements outside the sending PSP control and it is likely in many cases to take longer than 48 hours to come to a conclusion. A rushed decision whether a case is a scam or civil dispute might also have unintended detriment for potential mule accounts. Without a proper investigation, beneficiaries of the payment in question might unfairly and incorrectly end up with closed bank accounts and an inability to access financial services.

Starling recommends the PSR consider keeping time frames in line with the current SLA's dedicated by the CRM Code. This is a model which has been proven, and ultimately, it's crucial to ensure that the industry manages customer expectations. To apply an SLA which is unlikely to be met is only going to result in overall customer dissatisfaction and goes against the core principles of this paper.

Lastly, Starling wishes to highlight the need for exceptions to be built into the reimbursement timeline. Complex cases, which may be subject to law enforcement and/or

FCA investigation, often involve the complex and layered movement of funds across many different firms. These cases cannot be resolved within a set timeframe.

**Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Any standards of evidence needed will need to be adapted per scam type. If a time frame is to be established, this needs to be communicated to customers from the outset, to encourage them to respond quickly or risk their claim not being investigated, and a lack of cooperation leading to exceptions applied as per our response in Question 11. Only through investigating the evidence in question can an investigator identify the customer is being dishonest (although it might also be noted that at times, it is a lack of evidence which is also cause for concern). This has its challenges however, and with these proposals the PSR needs to acknowledge that there is likely to be a high proportion of first party fraud which goes undetected.

<b>Allocation of reimbursement costs</b>
--

**Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

In order to improve protections across all faster payment participants, Starling largely supports the introduction of a 50:50 split between the sending and receiving firm. The liability is currently only with CRM signatories, which has resulted in a migration of fraud funds away from the more established firms to smaller PSP's.

However, this proposal does ignore 'no blame' scenarios, and further, puts the entire financial burden onto the financial services further removing responsibility from the wider ecosystem. To truly have an impact on scam volumes, this burden should also be placed on others outside the sector, such as social media firms and telcos. Having a more sustainable funding model for no-blame scenarios would add incentive for these sectors to ultimately improve protection, and we might then see the reduction in scam volumes which is required.

Naturally, the 50:50 split is going to have a significant impact on receiving firms, and as a result is likely to see an increase in the number of inbound payments being held for further investigation. Whilst this is not strictly negative, and Starling supports the idea of increasing prevention effort in this space, this additional friction is going to have consequences for customers and might result in an increase in complaints as a result. Further, unwitting money mules need to be taken into account here. Unwitting mules are more likely to be vulnerable customers, who aren't aware of the process they are being asked to undertake. Again, this might drive an increase in customers who have severely low thresholds on their accounts, or even unbanked customers, who PSP's might be reluctant to take the risk on.

Aside from that, one of the main challenges with the introduction of a 50:50 split is the operational burden it places on PSP's. Moving and tracing money around different PSPs is going to be increasingly operationally challenging without a set process for doing so,

especially given this mandate covers the entire faster payment ecosystem. It becomes more complex, with some cases spanning many different PSP's, including smaller PSP's who might not have the functionality to respond quickly to cases in a timely manner. As a minimum, the PSR should stipulate an SLA for the receiving firm to refund the sending firm, and this needs to be monitored closely to ensure compliance.

The PSR also needs to consider the development of one method of communication. Starling would advocate the use of the UK Finance BPS portal, a system which the majority of PSPs use today. Should all PSP's be on-boarded to this system, it would enable a streamlined process for communication and ultimately, better customer outcomes. This system could also be developed to manage the payment process. Instead of funds being moved on a per payment basis, which will result in 100's of payments a day, Starling Bank recommends reimbursements are sent to a central account, managed by an independent 3rd party, and are then distributed on a regular basis (e.g. weekly, monthly). This would reduce operational overheads, likelihood for error, and provide oversight when receiving firms are reimbursing the required amounts.

**Question 14: Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

Starling holds concerns that this would be a costly exercise in terms of operational burden, and could result in a backlog of claims. As a result, Starling recommended the option to dispute the 50:50 allocation, however there should be a strict set of criteria for this, such as SLAs and the inclusion of a minimum threshold (£250k). This would ensure resources which could be focused on prevention aren't wasted on the processing of claims, and only the claims which involve significant, life changing sums of money would be reviewed in this way.

**Question 15: Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

Starling Bank identifies multi-generation scams where 'victim A' is contacted by the fraudster, but is socially engineered to send funds to a known payee ('victim B') (and potentially further subsequent payees) before it is transferred to the fraudster's bank account.

Due to the complexity of these cases and to simplify the issue, Starling believes the 'scam' should only be considered when the funds move into the criminal's bank account, (as it is currently stipulated under the CRM Code), and in essence, means these scam types are not considered in scope of this reimbursement model. This is because within the current legislative framework there is neither the ability to share the necessary data concerning multiple parties across PSPs, nor is there a framework for repatriation of funds across multiple payment generations.

This would mean it is victim B (or C or D etc. should many generations of payments be involved) who receive the 50:50 allocation of funds, and the subsequent movement of funds to victim A would have to occur as a separate process (although it is acknowledged this process also has its limitations). To truly rectify this issue and allow the beneficiary

firm to send funds to the original victim (both reimbursed or repatriated), a more sophisticated framework is required to allow PSPs to transfer funds across multiple other PSPs, regardless of the payment journey. However this does not currently exist and would need due consideration before implementation.

#### **Allocation of repatriated funds**

##### **Question 16: Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

Starling Bank supports the proposal for a 50:50 default allocation of repatriated funds, however it comes with operational difficulties. Tracing these funds through the system is already very difficult, especially given it can at times take months, without the additional consideration of splitting the funds 50:50. Reconciliation is also an issue, and puts operational constraints on understanding what money is coming back from what scam case. Lastly, it should be considered that some receiving firms might be incentivised to retain these funds to offset their own losses - there is not yet a systematic way to trace these funds so no one would be any the wiser should funds be recovered to be repatriated.

As such, and as referenced in Question 13, Starling recommends the development of the UK Finance BPS Portal to allow for a more streamlined process with an inbuilt audit function to provide the ability for PSP's to monitor and trace funds through the system.

#### **Scope of rules for allocating reimbursement costs**

##### **Question 17: Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

Starling Bank largely agrees with the proposal that the costs of reimbursement apply to all directly and indirectly connected PSP participants sending and receiving payments over Faster Payments. Since the introduction of the CRM Code, the Bank has seen a shift of scam payments to smaller PSPs where it is implied there are weaker prevention tools at play. If they were to be excluded from this proposal, this shift would be exacerbated. Moving forwards, it is imperative that the PSR establish clear mechanisms to ensure that within the payment landscape, every player is incentivised to develop strong anti-fraud controls, including unregulated firms such as the cryptocurrency exchanges.

However, it does need to be taken into consideration that fraud and scams will not cease to exist, and these proposals do not future proof for the inevitable shift of scam payments from the faster payment platform to alternative payment methods. The industry is already seeing evidence of this with a rise in authorised scams across the card landscape, a direct consequence of the introduction of friction to the faster payment journey over recent months and years. Within the paper, the PSR suggests the card schemes already have consumer protection in place, which is true for disputes and chargebacks, however authorised scam payments are generally not covered by these protections. The PSR should be cognisant of this and be considerate of the steps which might be required post implementation.



## Chapter 6 - Our long-term vision for Pay.UK's role

### Our long-term vision

#### **Question 18: Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

Starling Bank is in agreement that Pay.UK, as payment system operator (PSO) of the Faster Payments system, should be responsible for this process so that consumers are protected, and fraud is prevented from entering the system.

## Chapter 7 - Short-term implementation of our requirements

### A minimum initial set of Faster Payments scheme rules

#### **Question 19: Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

For ultimate prevention of APP scams, if these proposals are to come to fruition then they must be implemented across all participants from the outset. The clearest operationalisation of this is for Pay.UK to implement the initial suggested set of proposals into scheme rules. Taking into consideration the time taken to change or amend regulation, this would also allow for more agility to adapt rules to new scam types and trends seen. The PSO are better placed to engage with PSPs on an ongoing basis, and reflect any changes as required.

As already mentioned throughout the response, Starling recommends exploring the use of UK Finances' BPS platform to act as the mechanism for PSPs to share information. With a few amendments, this could be adapted to work in real-time, from the point of the victim's PSP raising the scam to the receiving PSP, through to repatriation and the reimbursement of funds across PSPs.

#### **Question 20: Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

Starling Bank is in agreement the most effective way to achieve the necessary changes to Faster Payment scheme rules is for the PSR to exercise their powers under section 55 of the FSBRA.

### Dispute resolution arrangements

#### **Question 21: Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**



Starling Bank is in agreement that should these proposals be implemented, there needs to be the ability for disputes to be raised and sequentially resolved between the two parties. However, given the scale of this proposal with the volume of PSP's included, it needs to be a process that is automated, so it's as cost and time efficient as possible. Taking into consideration the development of this, this might be a costly and timely exercise, Starling suggests the PSR recommend the dispute process as is currently outlined within the CRM Code. It should be a rare occasion that firms may want to dispute the allocation of a claim (to date, since the inception of CRM there has not been a dispute raised), the PSP may choose to do so through the appointment of an independent dispute resolution firm.

### **Monitoring compliance**

**Question 22: Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

**Question 23: Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

In order to ensure consistency across such a wide set of PSPs, Starling would support the development of a real-time compliance monitoring system. This system would be best integrated with a system such as the UK Finance BPS platform (should all PSPs be mandated to use this system) as it will allow for automated monitoring of reimbursement and repatriation of funds throughout the faster payment system. As aforementioned, at present the reconciliation of these funds and tracking through the system poses significant challenges. Manual reporting to Pay.UK would be another operational burden on PSP's, and there is no guarantee of accuracy. The introduction of a real time monitoring system (especially the development of one already in existence) would be beneficial to all PSP's and would enable straightforward and accurate monitoring for Pay.UK.

A real-time compliance monitoring system should be introduced in line with the introduction of any new measures. Introducing a manual work around before a more automated solution is implemented is not only likely to create inaccuracies, but it will also be time costly and resource heavy - especially if just envisaged as a short-term solution, this is an unnecessary step to take.

**Question 24: Do you have views on the best option for short-term enforcement arrangements?**

Starling Bank's preference would be for Pay.UK to develop and implement its own enforcement regime in the short-term.

### **Applying reimbursement rules to indirect participants**

**Question 25: Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

**Question 26: If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

Starling Bank considers option C to be the most realistic and sustainable option. With the high number of PSP's who would be included in these proposals, there is benefit to making the service as streamlined as possible. The Indirect Access Provider (IAP) is best placed to receive, manage and respond to claims within quick timelines. It creates a leaner model and scope for many of the previously mentioned improvements to be implemented (such as the advancement of the BPS Portal). It will require the IAP to lean on the indirect clients to ensure prevention remains a key focus, and whilst it will likely require operational change, this approach might also have its advantages.

However, there are challenges which the PSR should be aware of. Placing the responsibility on the IAP would have an additional operational impact which is unlikely to be currently considered as part of that relationship. With a requirement for increased oversight on indirect PSPs processes, as well as the actual processing of claims and reimbursements, an increase in operational costs is guaranteed. Contract reviews are likely to be required, and there needs to be consideration for what happens if a smaller PSP doesn't pay/can't afford to pay, and who should then cover this cost. Considering the scope of the proposals, a realistic consequence is that the financial burden might be too great for some PSPs.

If it were necessary, the direction should be applied to Indirect Access Providers, who would then need to ensure their indirect clients adhere to rule changes. However as previously referenced, Starling Bank recommends the changes are applied within the scheme rules by Pay.UK, opposed to a direction.

<b>Proportionality and cost benefit analysis</b>
--

**Question 27: Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

Starling understands that the PSR's expectation that the the costs associated with these proposals will incentivise firms to invest in their fraud systems and controls. Whilst this might be true for some PSPs, what is evident through a real focus in this space for Starling particularly throughout the past 3 years of being CRM Code signatories, is that PSPs cannot solve the issue in isolation. It is imperative that data sharing leverages data from across the financial services, telco and tech sectors. An obligation on the wider ecosystem to actively manage fraud risk should be an important part of the public-private sector approach to tackling fraud, and cannot be ignored.

**Question 28. Do you have any other comments on the proposals in this consultation?**

All comments on the consultation proposals are detailed in the above question responses.

# Steven Murdoch (Individual)

# Authorised push payment (APP) scams: Requiring reimbursement

Consultation Response to CP22/4, November 2022

*Professor Steven Murdoch, University College London*

Thank you for the opportunity to contribute to this consultation. My response is not confidential and may be published and shared in full.

*4. Do you have comments on our proposals:*

- that there should be a consumer caution exception to mandatory reimbursement*
- to use gross negligence as the consumer caution exception*
- not to provide additional guidance on gross negligence?*

I welcome the proposal to enhance the level of consumer protection through broadening the range of circumstances in which a victim of fraud is reimbursed. I agree that there is little evidence that unconditional reimbursement for fraud would result in customers acting without due caution. On the contrary the experience of TSB shows that customer will act to avoid being the victim of fraud even when an almost unconditional guarantee of fraud exists and is advertised to customers. Similarly, the US has had unconditional reimbursement of unauthorised fraud through regulations E and Z, and has a successful and profitable financial system. I also note that the proposed measures in the US for APP fraud mitigation include unconditional reimbursement for victims.<sup>1</sup>

I therefore think that unconditional reimbursement is a reasonable approach to APP fraud mitigation, and may be the best approach if it becomes infeasible to define and enforce a fair and transparent consumer caution exception. I would welcome more research in this area, including on whether a consumer caution exemption is necessary to encourage customers to act with due care. I would suggest that the PSR or other regulator commission such research, since financial institutions would benefit from the creation of a consumer caution exemption and therefore have a conflict of interest in conducting or funding research on this question.

If gross negligence is taken to be the appropriate level of a consumer caution exception then we can draw on experience of fraud reimbursement under PSD2 which also uses this test. In my experience this has not resulted in the fair treatment of fraud victims. Firstly the level of care that is required for customers to be reasonably certain of reimbursement is higher than just avoiding gross negligence. Secondly it is in many cases practically impossible for customers to show that they have not acted with gross negligence.

On the first point, a common approach of financial institutions denying a refund is to assert that any failure to follow bank terms and conditions is gross negligence. My research has shown that few customers do comply fully with all bank terms and conditions, and in many

---

<sup>1</sup> Steven Murdoch, US proposes to protect bank customers from Authorised Push Payment fraud (April 2022) <https://www.benthamsgaze.org/2022/04/29/us-proposes-to-protect-bank-customers-from-authorized-push-payment-fraud/>

cases it is practically infeasible to do so.<sup>2</sup> Therefore this interpretation of gross negligence would result in refusal to reimburse fraud victims becoming commonplace, rather than the rare exception set out in the consultation.

On the second point, when a reimbursement of fraud is refused by a financial institution due to an accusation of gross negligence, it is common for there to be no direct evidence of gross negligence. Instead the argument made by the financial institution is that computer evidence of the transaction shows that the customer's credential were used to authenticate the transaction and therefore it must have been that the customer acted with gross negligence. There is no evidence presented to exclude the possibility that the financial institution's computer systems were not acting properly or that there was a design flaw in the authentication system. The Horizon Post Office scandal has demonstrated the harm that can be caused by treating computer evidence as inherently more reliable than testimony of people affected by that computer system.

If gross negligence is to be used for a consumer caution exception then these two limitations must be addressed in order for the reimbursement scheme to be fair, transparent, and effective.

While I support the PSR's plan of not giving a detailed definition of what security measures financial institutions must have, I believe that the PSR should state how financial institutions should demonstrate why particular behaviour meets the high bar of gross negligence. For example, experiments could be conducted showing that in realistic circumstances a negligible proportion of experimental subjects would fall victim to fraud when using the financial institution's payment system, despite being targeted by a simulation of a sophisticated criminal. For such experiments to be realistic they should be designed following the principles of valid behaviour security research.<sup>3</sup> Experiments should be performed with a wide range of customers, including those who are vulnerable, and in a wide range of contexts.

To avoid the risk of reliance on computer evidence I would recommend that in order to refuse the reimbursement of fraud there should be positive evidence of gross negligence. It should not be the case that computer evidence that the transaction was performed with customer credentials is sufficient to discharge the burden of proof. If there is a dispute between computer evidence and customer testimony, and this is relevant to whether reimbursement is granted, the financial institution should give an expert witness acting on behalf of the victim access to all information available to the financial institution concerning the reliability of the computer system in question. Specific recommendations on this can be found on the briefing note "Briefing Note: The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences".<sup>4</sup>

5. Do you have comments on our proposal to require reimbursement of vulnerable

---

<sup>2</sup> Steven Murdoch et al. Are Payment Card Contracts Unfair? Financial Cryptography and Data Security, February 2016. <https://murdoch.is/papers/fc16cardcontracts.pdf>

<sup>3</sup> Krol et al. Towards robust experimental design for user studies in security and privacy. LASER 2016. [https://discovery.ucl.ac.uk/id/eprint/1503240/1/LASER\\_2016.pdf](https://discovery.ucl.ac.uk/id/eprint/1503240/1/LASER_2016.pdf)

<sup>4</sup> Bohm et al. Briefing Note: The legal rule that computers are presumed to be operating correctly – unforeseen and unjust consequences. Digital Evidence and Electronic Signature Law Review, Volume 19, pages 123–127. <https://doi.org/10.14296/deeslr.v19i0.5476>

consumers even if they acted with gross negligence?

The test for gross negligence should take in account the full context of the situation in which the fraud took place, including characteristics of the fraud and characteristics of the victim. Therefore a case could be made that in practice additional checks for vulnerability are not needed. However in practice reliably establishing the acceptable range of behaviour for a vulnerable individual could be infeasible so I would support unconditional reimbursement where a victim is vulnerable.

7. Do you have comments on our proposals that:

- sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- any 'excess' should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

8. Do you have comments on our proposals that:

- sending PSPs should be allowed to set a minimum claim threshold
- any threshold should be set at no more than £100
- PSPs should be able to exempt vulnerable consumers from any threshold they set?

Limits to the full reimbursement of fraud victims are in my opinion not appropriate because the fraud is a result of the payment system design and this is under the control of the customers. As stated in the Royal Society report on cybersecurity:<sup>5</sup>

“To improve security, responsibilities should be assigned to parties that could effectively discharge them, and could afford to do so. Consumers typically have the least capacity to mitigate risks, while service providers can improve security through system design and implementation, and by taking careful account of real-world use of their products. In most cases this means liability regimes should protect consumers, and prevent system operators from shifting liability to individuals where it is not reasonable to do so.”

There is no clear evidence that an excess is needed to cause customers to act with due care, though I would encourage the PSR to commission research on this question. While there is a cost in investigating reimbursement claims if the fraud amount is low, the depth and consequent cost of a proportionate investigation would be similarly low.

If an excess or minimum claim threshold is set, financial institutions should be required to waive this in cases of financial hardship. There is evidence that banks treat less well off customers worse than others, so it is not sufficient to leave this to the discretion of financial institutions, although I have no objection to them also being able to waive these limits in other circumstances too.<sup>6</sup>

---

<sup>5</sup> Progress and research in cybersecurity Supporting a resilient and trustworthy system for the UK, Royal Society, July 2016. <https://royalsociety.org/~media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf>

<sup>6</sup> Ellson, 'Banks Biased against Black Fraud Victims'. The Times (12 January 2017)

# Stop Scams

**Stop Scams UK's submission to the PSR's consultation on mandatory reimbursement for authorised push payment (APP) scams: 'CP22/4: Authorised push payment (APP) scams: Requiring reimbursement'**

Stop Scams UK welcomes the opportunity to contribute to the PSR's consultation and wider work on APP scams reimbursement. Our submission introduces the work of Stop Scams UK and sets out our thinking on APP scams reimbursement, including specific areas of concern in relation to timelines and the technical implementation of the rule changes. We have also provided answers to the specific questions set by the PSR where appropriate. These are at **Annex A**.

This response complements those submitted by our members and should be read in conjunction with those responses. It also sits alongside responses submitted by other organisations and bodies that also represent the views of our financial services members. This includes the response of UK Finance with which this response aligns.

Stop Scams UK notes that our PSP members are regulated entities and will have specific views on the rule changes and questions in this consultation, especially where they relate to technical proposals and their implementation. We have not provided answers to these questions or in those areas where SSUK has no locus.

**An introduction to Stop Scams UK**

Stop Scams UK is an industry-led collaboration of responsible businesses from across the banking, technology and telecoms sectors who have come together to stop scams at source. We currently have 18 members.<sup>1</sup> Together they cover over 95% of all UK online searches, 90% of the UK home email market, 80% of online advertising and 70% of online messaging services used in the UK, as well as significant mobile and fixed broadband connectivity.

For a scam to be successful it will touch on at least two if not all of the banking, telecoms and technology sectors. The only way to effectively tackle this harm is for businesses across each of the banking, technology and telecoms sectors to work together on the development of technical solutions to scams and for that action to be backed by appropriate and proportionate regulation. This is why collaboration of the sort fostered by Stop Scams UK is so essential.

Although a young organisation, Stop Scams UK is already helping to turn the tide against fraud and scams through several collaborative initiatives. These include:

**159:** is a memorable short-code phone service that has the capability of connecting most UK banking customers safely and securely with their bank if they receive an unexpected or suspicious call about a financial matter. In this way, the scam journey is broken at a critical moment when the consumer is at most risk of being socially engineered to make a payment. So even if scammers make contact with potential victims, that link will be broken before any information is shared, any payment is made, or any harm is done. Over 250,000 calls have now been made to 159.

---

<sup>1</sup> SSUK members are: Barclays, BT, the Co-operative Bank, Gamma, Google, HSBC, KCOM, Lloyds Banking Group, Meta, Metro Bank, Microsoft, Nationwide, NatWest, Santander, Starling, TalkTalk, Three and TSB.



**URL blocking:** Through our Alliance Partners led by BT, Stop Scams UK has enabled the implementation of an additional layer of protection to help prevent customers from inadvertently accessing phishing domains. Over 41,000 malicious and fraudulent URLs have now been blocked in a process that is far faster (taking as little as 15 minutes), than through other existing systems. We intend to extend this to more Stop Scams UK members.

**Data Sharing:** We are also undertaking an ambitious programme of work together with the Royal United Services Institute (RUSI) around data sharing between Stop Scams UK members. This work has already made recommendations for changes to policy as well as industry practice to help enable the effective sharing of data to prevent scams and will underpin the data sharing initiatives that Stop Scams UK is bringing forward with its members. Ultimately, the insight and intelligence that emerge from this work will help provide solutions to an issue that has been identified by both regulators and business.

### **An overview of Stop Scams UK's position on mandatory reimbursement**

Stop Scams UK fully supports the PSR's intention of better protecting consumers by ensuring they are compensated in the event of losing money to a scam. The PSR proposals will ensure a more certain and consistent consumer experience, which we welcome. The rule changes will also end the current patchwork of consumer remedies that lead to unsatisfactory outcomes, e.g. for customers of those banks and institutions that are not signatory to the voluntary CRM code. Stop Scams UK notes that our members have been clear that they support proportionate and appropriate regulation in the payment services space.

It is the view of Stop Scams UK that the status quo is neither satisfactory nor sustainable. The voluntary CRM code has delivered only partial success despite best intentions. The largest Tier 1 institutions are signatories to the code and already reimburse over half of those customers who experience a scam. However, many smaller institutions and fintech businesses offer consumer banking services but are not signatories of the CRM code; they reimburse the victims of scams less often. This is unfair both to consumers and to those responsible institutions that reimburse their customers when they are scammed.

The differing interpretation of the code across institutions has also led to unsatisfactory outcomes for some consumers. The proposed rule changes will bring a welcome uniformity of approach to this issue that will help alleviate the financial harm that some consumers experience. Measures to extend liability for the cost of reimbursement to recipient banks are also to be welcomed and will help ensure that all parts of the banking sector value chain are responsible for the cost of the harm caused by scams, while at the same time incentivising them to take action.

Our PSP members already dedicate significant time and resource to the development of highly effective security systems to help detect and prevent scams. Through these efforts, the industry currently stops more unauthorised fraud than it misses - £583.9 million in the first 6 months of 2022. We believe that the PSR must be mindful of the consequences of placing significant further economic and logistical responsibilities on PSPs, particularly when they are unlikely to stop a greater number of scams. Measures could also compromise this security infrastructure, by incentivising scammers (see below), and lead to an increase in scams by both volume and value.

In particular, we share our members' concerns that the proposed rule changes could incentivise 1st party fraud. The requirements for PSPs, including the 48-hour deadline for reimbursement, the leniency of the consumer caution exemption and the absence of a maximum threshold for

reimbursement, mean it will be very challenging for PSPs confidently to rule out 1st party fraud or gross negligence, leaving the system vulnerable to abuse by scammers.

Further consultation on the overall implementation timeline but also the technical implementation of these rules will be critical to ensure that unintended consequences are mitigated and where possible avoided. Additional consultation will also be needed on the 48 hour timeline for reimbursement which will pose significant challenges to some PSPs (see below). More long term, we urge the PSR to consider how it can deploy its influence and resource more effectively, to give industry the right tools to tackle this issue at source. This begins with more effective and consistent dialogue between the public and private sectors on solutions that address the root causes of scams.

While the principle of better protecting consumers and people who are scammed is to be welcomed, we strongly believe that scamming will only be stopped through the development of proactive and collaborative technical solutions that target scams at source. Mandatory reimbursement, while a significant benefit to consumers, is in contrast a reactive, potentially high-risk and short-term solution to an endemic problem. It does little to stop, slow down, or disrupt scamming in the short- or long-term.

The rule changes that the PSR proposes must also not be seen as an end point to regulatory action in relation to scams. Further legislative and regulatory changes are needed; this includes the PSR working closely and in cohort with other regulators to look at the policy and regulatory framework for data sharing, including amending and re-working guidelines to make clear that data sharing is not just allowed but encouraged. Government, for its part, needs to look at data protection law more broadly, including the forthcoming Data Protection and Digital Information Bill to make clear that data sharing by private companies for the purposes of stopping scams is not just consistent with the law but desirable. Input from the PSR will be critical to this.

Much greater coordination is needed to bring greater urgency and action to the policy response to scams. While the PSR's remit only applies to PSPs, we would strongly encourage them to come together with their counterparts in HM Treasury, the Home Office, DCMS, the FCA, Ofcom, and others, to come up with and pursue a comprehensive strategy for tackling scams that includes requirements for all relevant actors.

Lastly, if the fight against scams is to be effective, it is imperative that Government leads a coordinated effort to develop a comprehensive approach. While some progress has been made and is to be welcomed, more must be done and the PSR has a key role to play. A key step in achieving this would be the appointment of a single scams authority to lead the policy response to scams, designing and delivering a comprehensive framework that spans Government, regulators and industry. It would align existing activities, identify gaps and set clear targets and ambitions for action. We urge the PSR to work with industry on communicating to Government the importance of moving forward on this critical initiative. We note that this is a call that has been made by policy makers and industry, including most recently in the report of the House of Lords Committee looking at the Fraud Act 2006 and Digital Fraud.<sup>2</sup>

---

<sup>2</sup> <https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/8702.htm>

## **Technical implementation and timeline**

Our industry members have expressed concerns in relation to the compacted timings for implementation, given what will be significant changes to the existing rules, as well as the mechanics of how these changes will be implemented.

If the changes are implemented as proposed, the time constraints placed upon PSPs would be likely to necessitate the introduction of considerable friction to the UK's Faster Payments infrastructure. The rationale given by the PSR for giving PSPs economic responsibility for APP scams is that it will force them to introduce back-end solutions to combat fraud. However, such systems already exist. Furthermore, our banking members have attested that once an APP scam has entered the payments environment, the only effective solutions come from adding friction to the front end, which would compromise the purpose of Britain's unique faster payments environment.

SSUK is concerned that the timeline of the PSR's proposals is unrealistic given the scale of the change, and could interfere with critical PSP security apparatus that detects and rejects fraudulent payments, as well as adding significant friction to the UK's Faster Payments infrastructure. The PSR will need to take a proportionate evidence-based approach to amending these rules, considering carefully how they will affect PSPs existing security systems, and the UK's wider payments processing environment, and ensuring that unintended consequences are minimised.

## **Unintended long-term consequences**

We share the concerns of our industry members at the potential unintended long-term consequences of the proposed rule changes. We worry that the new rules offer an immediate fix for a limited number of scam victims, without incentivising consumers to adopt more effective steps to protect themselves from potential scams, or indeed to bring other sectors into work to prevent scams. In doing so, the rule changes could reward scammers without leading to the action necessary to stop scams at their source.

While alleviating the immediate loss experienced by consumers is welcome, the proposed rule changes do not address the wider harm scamming inflicts on the UK economy as a whole. Regardless of whether it is consumers or PSPs that meet the cost of fraud, if anti-scam initiatives do not tackle the root causes, the loss will still be felt, sooner or later, by business and consumers.

## **Conclusion**

SSUK recognises and fully supports the PSR's ambition to protect consumers and provide for a more consistent experience, particularly for those consumers who are vulnerable. SSUK also welcomes the levelling of the playing field that will come from requiring reimbursement from all PSPs, including those not currently covered through the voluntary CRM code. However, we ask the PSR to look again at the timelines for implementation and to work with the industry to mitigate the risks that will come with a reactive solution unlikely to encourage consumer care or caution. As we note above, scamming will only be curtailed through the development of proactive and collaborative technical solutions.

## **Annex A**

### **Answers to specific questions.**

#### **1. Do you have views on the impact of our proposals on consumers?**

Stop Scams UK is gravely concerned at the harm that APP scams are causing consumers and businesses across the UK. As a cross sector organisation of responsible businesses dedicated to stopping the harm and loss caused by fraud and scams, we know how fast APP scams are growing and how complex a problem they are to overcome.

We fully support the intention behind the rule changes, protecting consumers is an essential part of our collective mission. However, we worry the proposals do not focus adequately enough on stopping scams at source or disrupting scammers or scam journeys. We are concerned that the reimbursement proposals as presented will create a risk that consumers are disincentivised from exercising caution when engaging with potentially fraudulent content.

We believe the best way to protect consumers is through preventing scams from happening in the first place. This requires a greater effort from industry, regulators and government, particularly in enabling cross sector, technical solutions that stop scams at source. The PSR should look at what it can additionally do through its proposed rule changes to incentivise public/ private collaboration and data exchange to stop scams.

#### **2. Do you have views on the impact of our proposals on PSPs?**

The proposed changes will place significant new obligations on PSPs, that will make considerable financial and resource requirements of both sending and recipient PSPs. We are concerned that the changes could increase the value and volume of scamming and their impact on the UK economy, as under the proposed changes banks would be required to finance not just the victims of scams but also potential scammers. This will only incentivise their criminal activity. We provide some further thinking on the potential impacts of the proposal in our response to question 4.

We are also concerned that the changes will weaken the incentives consumers have to remain vigilant to scams. Consumer education around scamming is regarded by some parts of the industry (albeit not all) as a core component of helping protect people from scams. Stop Scams UK is concerned that the current proposals do not include any measures that will increase consumer caution when making payments or engaging with people online.

#### **3. Do you have views on the scope we propose for our requirements on reimbursement?**

If the process of assessing a reimbursement claim is too rushed, the ability of PSPs to accurately identify fraudulent reimbursement claims will be undermined. Stop Scams UK believes that in the absence of further consultation on timings, the timeline and requirements for implementing the reimbursement model are not only unrealistic but come with risks.

Under the proposed rules, PSPs will have only 48 hours to decide whether a scam claim meets the criteria for reimbursement. This is not enough time for PSPs to confidently rule out either 1st party fraud or gross negligence. If these checks are not reliable, the rules risk creating a surge in fraudulent requests for reimbursement. We therefore ask the PSR to look again and extend the

timeframe for reimbursement, and ensure that the rule changes do not unintentionally create a new scam type.

**4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

Stop Scams UK supports a consumer caution exemption to mandatory reimbursement. But, by using 'gross negligence' as the bar for reimbursement, the PSR has set it too high. In chapter 4.24, the consultation describes 'gross negligence' as a "higher standard than the standard of negligence under common law." But it also states that 'gross negligence' does not have a precise meaning in common law and its application would be different from case to case.

This ambiguity will make it very difficult for PSPs to challenge claims they suspect to be fraudulent. APP scams are increasingly ingenious and have been consistently fooling PSPs advanced security systems without the added burden of mandatory reimbursement. If PSPs have 48 hours to find proof of 'gross negligence', in order to refuse reimbursement on a loss that has no upper financial limit, scammers will be handed a considerable advantage over security systems that will have one hand tied behind their backs.

We believe further consultation will be needed to create sensible and reliable guidance. We urge the PSR to provide detailed guidance on the meaning and implementation of 'gross negligence', and consider lowering the bar for reimbursement to avoid scammers taking advantage of its ambiguity.

Additionally, we note that to effectively stop scams will require a consistent and collaborative approach from all links in the scam value chain. This includes measures to encourage responsible consumer behaviour. As consumers interact with scammers in the earliest and arguably most important part of the APP scam journey, there needs to be an appropriate level of focus and responsibility from consumers for any approach to stopping scamming to be truly successful.

**5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

N/A

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

N/A

**7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement • any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

N/A

**8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**

- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

N/A

**9. Do you have comments on our proposal not to have a maximum threshold?**

Stop Scams UK believes a maximum threshold is sensible as it would help curtail some of the economic impact these changes will have on PSPs. However, this should not preclude further action at all stages of the scam journey if we are to stop scams at source. This means all actors involved in a scam need to shoulder an appropriate and proportionate level of accountability by working together to prevent scams. Implementing a maximum threshold would go some way to balancing this accountability and would provide consumers with an incentive to stay alert to potential scams.

**10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

N/A

**11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

Stop Scams UK has no view on the sending PSPs share of the reimbursement. We do, however, believe that allowing PSPs only 48 hours to reimburse the customer comes with unnecessary risk. It doesn't allow PSPs adequate time to confidently rule out 1st party fraud or gross negligence. Without the time to properly assess each claim, the rule changes run the real risk of fuelling a surge in fraudulent reimbursement claims.

**12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

N/A

**13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

N/A

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

N/A

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

N/A

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

N/A

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

N/A

**18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

Stop Scams UK agrees that building a safer Faster Payments System is crucial for building greater consumer confidence in the digital economy, something that the extent and volume of scams has eroded. We also understand the rationale behind the PSR's belief that the PSO is an appropriate body to "undertake the role of making, maintaining, refining, monitoring, and enforcing compliance with, comprehensive scheme rules that address fraud risks in the system."

However, we believe this long-term vision is not ambitious enough, and places too great an emphasis on the capacity of the PSO to undertake the tasks of creating, maintaining, monitoring, and enforcing rules on fraud and scams. We believe that any long-term vision involving fraud needs to focus on collaboration. Scams are a uniquely cross sectoral criminal activity that require a uniquely cross sectoral response. This should include regulatory support for cross sectoral initiatives intended to combat scams, such as 159 and the work of SSUK to enable data sharing.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

N/A

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

N/A

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

N/A

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

N/A

**23. Do you have views on the costs and benefits of Pay.UK implementing a real time compliance monitoring system and when it could be introduced?**

N/A

**24. Do you have views on the best option for short-term enforcement arrangements?**

N/A

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

N/A

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

N/A

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

N/A

**28. Do you have any other comments on the proposals in this consultation?**

N/A



# The Money Charity



# The Money Charity Response – Authorised push payment scams: Requiring Reimbursement (November 2022)

The Money Charity is a financial wellbeing charity whose vision is to empower people across the UK to build the skills, knowledge, attitudes and behaviours to make the most of their money throughout their lives, helping them achieve their goals and live a happier, more positive life as a result.<sup>1</sup>

We welcome the opportunity to respond to the Payment Systems Regulator’s consultation on Authorised push payment (APP) scams: Requiring Reimbursement.

In this response, we make some overall comments on the issue then answer the questions posed in the Consultation Paper.

---

<sup>1</sup> See box on back page.

## Overall Comments

As the UK's financial wellbeing charity, The Money Charity are delighted to see the introduction of a set of radical new proposals that will have a wide-reaching positive impact on the financial wellbeing of consumers across the UK. The proposals for mandatory reimbursement set out in this consultation mean that a much greater number, in fact the vast majority, of APP (authorised push payment) scam victims will be entitled to a significant level of reimbursement. This in turn will incentivise PSPs to act to prevent more scams from happening in the first place. The beneficial impact that these measures will have upon consumer financial wellbeing cannot be understated and come at a time when critically needed; in the first half of 2021, £4 million per day was stolen from people in the UK via scams, with less than half of this money being refunded by banks<sup>2</sup>. In our responses to the consultation questions, in some instances we suggest that the proposals don't go far enough, for example, we suggest that there could be further measures to protect specific groups of consumers who are more likely to fall victim to scams. However, we are well aware that these proposals will face considerable opposition from banks and PSPs, so we are keen to support the proposals in their current form if necessary.

## Answers to consultation questions

### Question 1: Do you have views on the impact of our proposals on consumers?

We warmly welcome the proposals outlined in this consultation, as we believe that they will have an extremely positive impact on consumers. The proposals mean that the vast majority of APP scam victims will be entitled to a significant level of reimbursement. We celebrate these measures not only from a financial wellbeing perspective, but also in the interests of consumer emotional wellbeing. Falling victim to a scam can be a distressing experience. Incentives that work to prevent more scams from happening in the first place will also help to protect consumers from the negative emotional impact that is associated with scams.

We are satisfied that due to the Equality Act 2010, PSPs will be unable to restrict services to certain groups who may be more likely to fall victim to scams, such as elderly people. However, we think that more could be done to address the underlying reasons that cause groups such as elderly people to be more likely to become victims of scams. A reliance on anti-discrimination laws in this instance presents only a symptomatic solution; while it is illegal for banks to discriminate against elderly customers and prevent them from making payments, there is no evidence that any thought has been given as to why elderly customers are more likely to become victims of scams. Elderly consumers may be equally entitled to reimbursement, but they will continue to become victims of scams at a higher rate until the root causes are addressed. This

---

<sup>2</sup> UK Finance, September 2021 [https://www.bbc.co.uk/news/business-58649698?mc\\_cid=97ef893b22&mc\\_eid=4c7424401b](https://www.bbc.co.uk/news/business-58649698?mc_cid=97ef893b22&mc_eid=4c7424401b)

also means that they will continue to experience the emotional distress that is associated with scams at a higher rate than other groups. In the spirit of incentivising PSPs to stop scams from happening in the first place, it makes sense for there to be further measures to protect groups who are more likely to fall victim to scams, as these groups surely represent a significant proportion of the overall losses caused by scams. Preventative protections could perhaps come in the form an education initiative on money safety, targeted at these specific groups. The Money Charity has a depth of experience in delivering money safety workshops to a wide range of audiences. PSPs may find a solution such as this to be more attractive and cost-effective than simply continuing to reimburse these groups.

**Question 2: Do you have views on the impact of our proposals on PSPs?**

The costs that PSPs may expect to incur as a result of the proposals, while likely to be unpopular with PSPs are a necessary part of protecting the financial and emotional wellbeing of consumers. Ultimately, if the proposals are effective, PSPs will be incentivised to prevent a larger number of scams than are currently being prevented, and therefore incur less reimbursement costs than are currently being paid.

**Question 3: Do you have views on the scope we propose for our requirements on reimbursement?**

We agree that the proposed scope is appropriately inclusive. PSPs should not be expected to reimburse large businesses for losses caused by scams. All directly connected PSP participants sending payments over Faster Payments, as well as PSPs indirectly connected via an indirect access provider, should be obliged to reimburse consumers under the scheme. No category of APP scam should be excluded from mandatory reimbursement.

**Question 4: Do you have comments on our proposals:**

- **That there should be a consumer caution exception to mandatory reimbursement.**
- **To use gross negligence as the consumer caution exception.**
- **Not to provide additional guidance on gross negligence?**

It has been argued that in making reimbursement mandatory, the scheme may cause some consumers to be less cautious in making payments. Therefore, a consumer caution exception may be necessary. We would like to make two objections to this argument. Firstly, and as highlighted in the consultation, the PSR has seen no evidence that when faced with the prospect of guaranteed reimbursement, consumers are likely to act more recklessly when making online purchases. Even more, the prospect of reimbursement cannot completely offset the emotional distress that is often experienced by scam victims. Consumers may want to avoid falling victim to scams altogether, rather than go through the perhaps humiliating process of realising that they've been targeted and then having to make a claim for reimbursement. Secondly, the consultation rightly argues that it is difficult to pin down what kind of actions should count as

‘gross negligence’, and therefore does not offer any additional guidance on how PSPs should define what kind of consumer behavior could be defined as grossly negligent, other than as having behaved with a very high degree of carelessness. This means that PSPs will be able to decide if consumers have acted with gross negligence, in turn opening the possibility of PSPs setting the bar low in order to reimburse as few consumers as possible. There are good proposals for monitoring and enforcing compliance of PSPs, such as requiring PSPs to publish data on APP scams. If it seems that a PSP has reported a very low number of reimbursements, it may be because they have rejected too many claims as being grossly negligent. However, this is a solution that is not an infallible one, and risks allowing claims to be rejected before data can be analyzed and acted upon. We suggest that the practice of ‘gross negligence’ as a consumer caution exception be kept under review, as it is crucial to understand whether the caution is having the intended effect. After this review, at which point PSPs may have clear examples of claims they have rejected as being grossly negligent, the PSR may be expected to publish some guidance on what kind of actions can be defined as grossly negligent.

**Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We strongly support the proposal that PSPs should be required to reimburse vulnerable customers, even if they have acted with gross negligence.

**Question 6: Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?**

We accept the proposal to use the FCA’s definition of a vulnerable customer, as this will ensure that all firms are working to a single definition of vulnerability. However, we would like to make a small amendment, as detailed in our response to questions seven and eight.

**Question 7: Do you have any comments on our proposals that:**

- **Sending PSP’s should be allowed to apply a modest fixed ‘excess’ to reimbursement.**
- **Any ‘excess’ should be set at no more than £35.**
- **PSP’s should be able to exempt vulnerable consumers from any ‘excess’ they apply?**

Please see below, included with answer to question eight.

**Question 8: Do you have comments on our proposals that:**

- **Sending PSPs should be allowed to set a minimum claim threshold.**
- **Any threshold should be set at no more than £100.**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

We understand that there are good reasons for allowing PSPs to set an ‘excess’ of £35 and/or a minimum claim threshold of £100, mainly that are beneficial to PSPs, such as helping to ensure

that the administrative costs of the proposals to PSPs are proportionate. Despite these reasons, we strongly suggest that both the excess and minimum claim threshold are dropped as proposals. The reality remains that £100, or even £35, is an unaffordable loss for many people, and particularly vulnerable consumers. Indeed, having fixed thresholds means that those who can afford to lose the least are worst affected. If dropping these proposals altogether is unrealistic, at the very least PSPs should introduce an excess that is instead a percentage of the losses and be obliged to exempt vulnerable consumers from any excesses or thresholds that are set. Additionally, the definition of vulnerability should be adjusted to include people who are less financially secure, as scam losses have a disproportionately negative impact on people who have less money and with lower levels of financial resilience. On the other hand, if consumers are more financially secure and able to afford any losses caused by scams, they should not be viewed as being somehow more liable for these losses. Such a view risks slipping into ‘victim blaming’ territory. The moral responsibility of scam prevention should primarily fall on criminals not to commit scams, as consumers have a right not to be scammed. Obviously, this goal is neither likely nor realistic. PSPs must therefore be entirely responsible for scam prevention, which is of course argued in the consultation – however this should not include measures such as setting an excess or minimum threshold, which not only appear to defer blame to the consumer, but also have a disproportionately negative impact on vulnerable consumers.

**Question 9: Do you have comments on our proposal not to have a maximum threshold?**

We agree with the proposal not to introduce a maximum threshold, as there are usually already strong protections in place for very large payments. We recognise that most payments made using Faster Payments are typically well below £1 million, making a maximum threshold redundant.

**Question 10: Do you have comments on our proposals that:**

- **Sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement.**
- **Any time limit should be set at no less than 13 months?**

We agree that 13 months is a reasonable timeframe for which consumers should be expected to submit reimbursement claims.

**Question 11: Do you have comments on our proposals that:**

- **The sending PSP is responsible for reimbursing the consumer.**
- **Reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We agree that the sending PSP should be responsible for reimbursing the consumer, and that reimbursement should happen no later than 48 hours after a claim is made, unless the PSP can provide evidence that the consumer acted with gross negligence.

**Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The standard of evidence needs to be sufficiently high to disallow PSRs from unnecessarily delaying payment or playing the consumer in any way.

**Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

We agree that at 50:50 default allocation of reimbursement costs between sending and receiving PSPs mean that the overall losses should balance out, and so is an appropriate default distribution.

**Question 14: Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We agree that PSPs should be able to depart from the default allocation to a more tailored allocation if they so choose.

**Question 15: Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

No comments.

**Question 16: Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

No comments.

**Question 17: Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We agree that the rules on allocating costs of reimbursements should apply to all directly connected PSP participants sending and receiving payments over Faster Payments, as well as PSPs indirectly sending and receiving payments.

**Question 18: Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

We agree that the PSO should be the rule setter responsible for mitigating fraud.

**Question 19: Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

No comments.

**Question 20: Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

No comments.

**Question 21: Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

No comments.

**Question 22: Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

We agree that the short-term implementation approach is the most appropriate option, as it is important that a monitoring regime is implemented as soon as possible after the reimbursement requirements start. However, as detailed earlier in our response, the process of monitoring how many claims are being rejected by PSPs as grossly negligent must be kept under review to ensure that PSPs are not setting the bar too low.

**Question 23: Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?**

We support the introduction of Pay.UK implementing a real-time compliance monitoring system, and agree that this should be implemented as soon as possible, as this will be crucial in ensuring that an acceptable proportion of claims are being investigated as grossly negligent.

**Question 24: Do you have views on the best option for short term enforcement arrangements?**

No comments.

**Question 25: Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

No comments.

**Question 26: If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

No comments.



**Question 27: Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

No comments.

**The Money Charity** is the UK's financial wellbeing charity providing education, information, advice and guidance to all.

We believe that everyone achieves financial wellbeing by managing money well. We empower people across the UK to build the skills, knowledge, attitudes and behaviours to make the most of their money throughout their lives, helping them achieve their goals and live a happier, more positive life as a result.

We do this by developing and delivering products and services which provide education, information and advice on money matters for those in the workplace, in our communities, and in education, as well as through influencing and supporting others to promote financial capability and financial wellbeing through consultancy, policy, research and media work.

We have a 'can-do' attitude, finding solutions to meet the needs of our clients, partners, funders and stakeholders.

Tel: 020 7062 8933

hello@themoneycharity.org.uk

<https://themoneycharity.org.uk/>

# The Payments Association



connecting the future

**Authorised Pushed Payment (APP) Scams:  
Requiring reimbursement**

**PSR**

**September 2022**

*Response from The Payments Association*

## Introduction

The Payments Association welcomes the opportunity to contribute to the PSR Consultation Paper “*Authorised Pushed Payment (APP) Scams: Requiring Reimbursement*”.

The community’s response contained in this paper reflects views expressed by our members and industry experts recommended by them who have been interviewed and who are referenced below. As The Payment Association’s membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to fully represent the views of all members.

We are grateful to the contributors to this response, which has been drafted by Riccardo Tordera, our Head of Policy & Government Relations. We would also like to express our thanks to the PSR for their continuing openness in these discussions. We hope it advances our collective efforts to ensure that the UK’s payments industry continues to be progressive, world-leading and secure, and effective at serving the needs of everyone who pays and gets paid.

With special thanks to:

- [REDACTED], Chief Strategy and Partnership Officer, PPS
- [REDACTED], CTO, Okay
- [REDACTED], CEO, Okay
- [REDACTED], UK General Counsel, LHV
- [REDACTED], Regulatory and Trade Association Lead – Payments, NatWest Group
- [REDACTED], Regulatory Change Manager, Modulr
- [REDACTED], Chief Lead and Compliance Officer, PPS
- [REDACTED], Senior Product Manager, Form3
- [REDACTED] Head of Data Services, Form3
- Other members who have preferred not to be listed, as their companies have decided not to respond to this consultation, but have expressed personal views on this topic.

[REDACTED]  
*Director General*  
**The Payments Association**

## Contents

The section numbering below corresponds to the numbering of the 'questions for respondents' in this paper.

### 1. Do you have views on the impact of our proposals on consumers?

APP Scams continue to grow, and we appreciate the PSR is committed to doing more to protect consumers. Nonetheless, we do not believe that measures such as requiring mandatory reimbursement will effectively prevent fraudsters from acting, rather we believe this could create the opposite effect. Whilst the implementation of these measures do provide additional protection for consumers, we highlight four main areas of concern:

- **Friction:** the proposals will slow down the Faster Payment Scheme (FPS) for some payments and this could cause customers to stop using it. Instead, they could revert to using cheques and cash; further, whereas the current EU proposals on the widespread adoption of instant payments are likely to be adopted soon, these proposals take the customer experience in the opposite direction – towards slower or delayed payments.
- **Education of payment users:** educating customers to be careful should be at the core of this approach rather than adjacent to it.
- **Increase in first party fraud:** because most people will be reimbursed from what are claimed to be fraudulent transfers, fraudsters will target consumers and reward them for claiming reimbursement of a transaction that can then be claimed as being fraudulent. This is fraud by both the payer and the fraudster. This could have the unintended consequence of indirectly incentivising consumers to be party to the fraud.
- **Reduced competition:** if all firms will have to reimburse consumers for all APP fraud, the relative burden on smaller firms will be greater. This runs contrary to PSD2 and the goal of opening up the market.

In addition, we observe that the system is still based on the victims' claim to be victims, but there is no mention about the starting point of the claim, and whether PSPs have a responsibility into identifying the fraud and initiating the process on behalf of the client.

### 2. Do you have views on the impact of our proposals on PSPs?

Most of our members do not believe that requiring mandatory reimbursement is the way to go and that these proposals will be detrimental to PSPs.

We believe that the most immediate impact on PSPs will be the cost of implementation, and the practicalities related to the 48-hour window for reimbursement, as this allows insufficient time to investigate each claim thoroughly and fairly.

In addition, we believe that there is still no focus on inbound transactions screening. At the moment this happens only for outbound transactions.

### 3. Do you have views on the scope we propose for our requirements on reimbursement?

Most of our members do not agree with mandatory reimbursement. Many believe that the scope should not include micro-enterprises and small charities.

We would like to see a framework of how you plan to operationalise the reimbursement process, because the current system via emails poses concerns.

**4. Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**
- **to use gross negligence as the consumer caution exception**
- **not to provide additional guidance on gross negligence?**

Most of our members would welcome a consumer caution exception rather than just gross negligence. We think customers will be able to make mistakes, which is our main concern. Because of the definition of gross negligence being extremely broad, we believe no one would be effectively considered negligent and this would result in PSPs having to fund consumers' naivety. We would like the definition of gross negligence be narrowed and tighter.

**5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

Our concern here is that this may cause the unintended consequence of creating more fraud, by malicious people pretending to be "vulnerable" according to the definition of vulnerability, and thus automatically entitled to reimbursement even when they have been acting intentionally and with gross negligence.

**6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

Our general view is that every potential victim is potentially vulnerable, given the techniques that fraudsters are able to deploy. Nonetheless, it is not fair to suggest that everybody who is considered vulnerable by the definition of vulnerability, is in a vulnerable situation that makes him/her/them unable to make a transfer, hence not to be held responsible. We would like to highlight that, according to the most recent FCA assessment, the proportion of UK adults with characteristics of vulnerability was 53% in October 2020, and the cost of living crisis is likely to make this proportion even larger.

**7. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement**
- **any 'excess' should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?**

Provided the excess is applied to recovered funds then we generally believe this is acceptable. Some members have suggested that we should apply the same mechanism here that operates for credit card chargebacks, where the charge is paid by the merchant. However, the view of the majority is that the current figures would not make much difference even though they are not enough to force consumers to take care in the way they should.

**8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

Most of our members believe that a £100 threshold would still not be enough to make consumers more careful about their transfers.

## **9. Do you have comments on our proposal not to have a maximum threshold?**

Whilst most members disagree with the view that requiring mandatory reimbursement is the appropriate way to beat the fraudsters, they agree with the general principle that, if there has to be a reimbursement, there should not be a maximum threshold.

## **10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

We agree with a limit, but we would appreciate the PSR to set standards on this, not the PSPs.

## **11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

The 48-hour window is really difficult to implement, and it leaves insufficient time for proper investigation. Further, there is no clarity of what should happen in case of suspicion. Also, more guidance on when and how PSPs can turn the 48-hour timer off would be appreciated. A consistent and balanced technical standardised framework should be provided to avoid further unintended consequences.

## **12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

The type of evidence should be dependent upon what information is shown to the payer when approving a transaction. If PSPs show the wrong name for an IBAN, then the liability should be on the PSP. But if PSPs show the correct owner of an IBAN, and the payer still approves the transaction, an argument can be made that the payer should have verified the recipient more closely.

Further, we believe that investigations are likely to require the involvement of multiple institutions and significant bureaucracy, so 15 days (or 30 days in most complex cases) should be allowed. Our members believe that standards for gross negligence or first party fraud must at least consider:

- Ignoring warning during the payment journey;
- Misleading controls when questioned i.e. advising they are happy with the payment.

## **13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

It is our view that, if this has to happen, then we agree with the proposal.

Nonetheless, some members have pointed out – as an addition to our answer to question 12 – that if the receiving PSP is unable to provide an API for verifying the IBAN, more of the responsibility of the reimbursement should be on the receiving PSP because:

- Having the allocation dependent upon what the user sees will help educate users and motivate PSPs to implement user interfaces that better informs end users;



- Having verification of IBANs as part of the reimbursement allocation calculation will motivate PSPs to provide APIs so that their IBANs can be verified, and for more competition in the IBAN verification space.

Also, a remitting bank can do absolutely nothing wrong, and act on the instruction of their customer (as it is an authorised payment) and then still be punished. If this takes place, then there will be an increased level of friction and delay in payments as banks will seek to do something to mitigate their losses. For example they may:

- a) Raise the amount of due diligence undertaken on new current account customers;  
and
- b) Monitor these accounts more vigilantly

While these may be seen to be appealing changes, this will increase the cost of opening and running current accounts and reduce the ease with which accounts can be opened. The first of these will reduce the profitability of current accounts and therefore reduce competition in the current account market. The second of these outcomes does not bode well for solving the problem of access to current accounts, which has been a persistent challenge for our industry in recent years.

Finally, if issuers are more cautious about opening marginal accounts because they are concerned that they may have to accept 50% of the costs of any APP scams, they will be less likely to open accounts for low income, disadvantaged, technologically challenged, older or vulnerable consumers. This goes counter to our society's objectives of including more vulnerable consumers into our financial system.

Note:

*Some members have suggested that it may not be easy to find the right balance of loss distribution. Their suggestion is a PSP rate/indicator based on a previous period of activity. (i.e. a receive side PSP with a strong protection and a high level of scrutiny would have a lower proportion of the loss if the send side PSP had a more relaxed approach to their responsibility and vice versa).*

**14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We envision that departing from the 50:50 default allocation would add an extra layer of complication, but we would need to evaluate the possible set of rules regarding the negotiations before making a final judgment.

**15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

Applying the same logic, there should be no difference, because the intermediaries should be responsible for the refund.

**16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

We agree with the proposal.

**17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We do not wish to comment.

**18. Do you have views on our long-term vision, and our rationale for the PSR being the rule-setter responsible for mitigating fraud?**

We are supportive of rules being set for all to adhere to as long as the process is consultative and we are able to consider the practical application and timelines effectively with differing business models.

**19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

Some of our bank members are supportive of the Faster Payments scheme rules being used to incorporate the PSR's plans to ensure scammed customer reimbursement, and they would like direct and indirect firms to go live at the same time, which may mean that this is late 2023. Time will be needed to allow smaller firms to familiarise themselves with what is required.

However, EMIs tend to be critical of this way forward, as they believe that Faster Payments Scheme rules cannot be applied to those indirectly using the scheme and all rules should be applicable to anyone accessing the Faster Payments Scheme.

**20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We do not wish to comment.

**21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

Standardisation of the type of information required to generate a dispute and protect the rights of the consumer needs to be made clearer. This must be done in consultation with all key members and operators in the sector and ensure an understanding of the impacts to different business models.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

Whilst most of our members are not supportive of mandatory reimbursement in first place, they have made clear that, if this has to happen, they would be supportive of allowing a compliance monitoring regime on the requirements and scheme rules that sets out clear guidelines to help detect and prevent fraud.

**23. Do you have views on the costs and benefits of Pay.UK implementing a real time compliance monitoring system and when it could be introduced?**

Overall, our comment is that this must be considered against the different business models and capacities to ensure that timelines are realistic and do not put undue pressure on a business.

Some members have expressed the view that they do not see Pay.UK implementing such a system in the short term. Others have considered not just when this could happen but on the fact that once it happens it may see it direct and indirect firms needing to adhere to the scheme rule. To ensure these firms are not bound to all scheme rules, we are aware that some members (who have responded individually to this consultation) have proposed that

Pay.UK adopts a similar approach to Credit Payment Recovery, where the rule/procedures are set out in a document which can be made available to indirect participants. It is their belief that this would also allow Pay.UK to work with/consult firms on its proposals in order to produce procedures which reflect firms' different business models.

**24. Do you have views on the best option for short-term enforcement arrangements?**

We believe that it is not clear how enforcement should be achieved.

Some of our members have clearly stated that they are unable to support short-term enforcement arrangements for those that are now meeting the scheme rules for reimbursement.

**25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

We have taken the view that this should be the responsibility of the direct participant providing access to the scheme.

**26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

We believe that the liability should be direct via PSP and not via clearing bank – otherwise this will result in the clearing banks restricting access.

**27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

Most of our members have encouraged us to express their unhappiness with this model. They believe the logic of this analysis is flawed and has no basis for real time application of the scheme. It is their view that it will have the unintended consequence of effectively acting as funding fraud, increasing costs for PSPs and undermining their ability to allocate and invest in the relevant prevention tooling. It is their strong belief that this model will also make the payments market unattractive for many of them and reduce competition and innovation. They also believe that the additional costs of implementing and maintaining such a scheme, and providing the reimbursement of what is likely to be an increased level of fraud, will ultimately be borne by consumers who will have to pay for the operation of an intrinsically inefficient system.

Rather than filling the holes in the bucket, this system rewards those who make the holes, rewards them for making them bigger and encourages consumers to join them in the task.

**28. Do you have any other comments on the proposals in this consultation?**

We welcome the comment in the Consultation Paper introduction, which says the PSR wants to solve problems through PSPs. But our view is that the PSR should go beyond this proposed system and focus on a much broader arena: the source of the scam (social media, advertisers, social selling, and big tech). Many of our members believe it is simplistic to think that we can resolve this problem by just mandating refunds for scammed victims. While consumers may become protected, the PSPs will become the victims.

We fully support any activities on data sharing within the payment flow which allows for better decision making, as long as this is supported and applied universally. There are a large number of consumer payments which will be impacted by the proposals in this consultation and they have not actively been considered.

A further consideration that some of our members have raised is about the scope of the proposed measures. In particular, they focus on the fact that whilst the consultation does explain that both direct and indirect members of FPS should be covered, it does not look at authorised e-money institutions (EMIs) and authorised payment institutions (PIs) that are neither direct nor indirect members of FPS. Is the position that the obligation to reimburse the clients of these PSPs would fall on safeguarding institutions that handle the payments for these PSPs – even while the safeguarding institutions have no direct contact with and no ability to directly contact the potential victim, who is a client of the authorised EMI/PI? More clarity on the proposed liability for the EMIs/PIs and the safeguarding institutions would be appreciated.

## About The Payments Association

The Payments Association (previously the Emerging Payments Association or EPA) is for payments institutions, big & small. We help our members navigate a complex regulatory environment and facilitate profitable business partnerships.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector in order to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA, HM Treasury, the Payment Systems Regulator, Pay.UK, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of leading payments CEOs, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of monthly digital and face-to-face events including our annual conference PAY360 and awards dinner, CEO round tables and training activities.

We run 5 stakeholder working Project groups: Inclusion, Regulator, Financial Crime, International Trade and Open Banking. The volunteers within these groups represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

We also conduct exclusive industry research which is made available to our members through our Insights knowledge base. These include monthly whitepapers, insightful interviews and tips from the industry's most successful CEOs.

See [www.thepaymentsassociation.org](http://www.thepaymentsassociation.org) for more information.

Contact [REDACTED] for assistance.

Tink

## **Response to Payment Systems Regulator Call for Views on Authorised Push Payment (APP) Scams: Requiring reimbursement (CP22/4)**

**Date:** 24<sup>th</sup> of November 2022

**Sent to:** [appscams@psr.org.uk](mailto:appscams@psr.org.uk)

We welcome PSR's call for views on APP fraud. Protecting customers from the emotional stress it means being a victim of fraud as well as their funds is of utmost importance for the financial market.

The consultation's proposed requirement on mandatory reimbursement covers all APP scam payments over Faster Payments, including PISP-initiated payments. We have no objection to the proposed scope. We want to stress the importance of keeping the providers of PIS (PISPs) outside of the model for allocation of reimbursement costs, which is proposed to be equally divided between sending and receiving PSPs by default.

We believe that the definition of a PISP and the PIS itself explains why this is important. A PISP is a provider of a software tool that enables an account holder, PSU, to place a payment order with its ASPSP in other channels than the ASPSP's own customer facing channels. This enables the PSU to a greater extent choose in which environment he or she wishes to place a payment order. After the PISP has placed the payment order with the ASPSP, the payment is subject to the exact same controls and processes as a payment order placed within the ASPSP's own customer facing channels.

A PISP does not hold or come in contact with any funds and does not execute the transaction. It is also the ASPSP that issues the personalised security credentials and performs the strong customer authentication (SCA) on the PSU. Further, it is the ASPSP that has the complete payment transaction history of the payer and the knowledge of what is considered a normal use and behaviour for the specific PSU, factors that usually are a vital part in assessing the risks with a transaction and if it is a potential fraud. The PISP usually only has the payment information of that single payment order.

Today, the Payment Services Regulation 2017 specifies that if '*a payment transaction was initiated through a PISP, it is for the PISP to prove that, within its sphere of competence, the payment transaction was authenticated, accurately recorded and not affected by a technical breakdown or other deficiency linked to the payment initiation service*'. If the PISP can prove this, it is not liable to compensate the ASPSP. If the PISP cannot prove this, then it is liable to compensate the ASPSP for losses incurred or sums paid by the ASPSP, which according to our interpretation would include possible reimbursement costs the ASPSP has had as an effect of

this proposal. There's no justification for extending the PISPs' liability beyond matters that are within its sphere of competence, which is why the current scope, which does not include the PISP, shall remain.

# Token



# Token response to PSR consultation "Authorised push payment (APP) scams - Requiring reimbursement (CP22/4)"

December 2022

# TOKEN

## About Token

Token is a leading Open Banking enabler for the UK's payments industry. Our mission is to power the success of its customers through best-in-class Open Banking payments infrastructure and expertise. We are driving the shift from traditional payment methods to faster, fairer, frictionless payments by helping payment providers successfully launch Open Banking payment capabilities. Payment providers and gateways partner with Token to plug-and-play, white-label, or use our technology to build their own open banking payments propositions.

Token welcomes the opportunity to respond to the Payment System Regulator's (PSR) consultation "Authorised push payment (APP) scams – Requiring reimbursement (CP22/4)".

APP scams have a terrible and lasting impact on victims, who are more often than not consumers. We fully support the PSR's ambitions of reducing consumer harm caused by APP scams. Without doubt, there's an urgent need to adopt a cross-sectoral approach to protecting consumers and reducing harm from APP scams in the future.

### The PSR's proposals

The PSR has proposed making reimbursement of APP scam victims mandatory and splitting the funding of that reimbursement 50/50 between the sending bank and the receiving bank. The PSR states that payments initiated via Open Banking will be included in these proposals, although no detail is provided about how this would work in practice.

Alongside its work on APP scams, the PSR also has a policy programme aimed at driving Open Banking-enabled A2A payments to compete with cards for retail payment use cases. We're concerned there is a fundamental tension between the PSR's ambitions for A2A retail payments and its latest proposals to address APP scams.

For Open Banking-enabled A2A retail payments to compete effectively with cards, it's key that A2A payments are fast, low friction, and low cost. Unfortunately, the PSR's APP scam proposals have the potential to adversely impact all of these characteristics. Further, we think this is unlikely to be for any material benefit, given that most Open Banking-enabled A2A payments to merchants are already at significantly lower risk of APP scams.

The PSR's proposals will likely result in banks introducing more warning screens and steps to A2A payment consent and authentication journeys. More broadly, there's a risk of banks slowing down payments as a result of these proposals. For example, by introducing a lower threshold for payments that are escalated for enhanced fraud checks. While more friction and slower speed may be an appropriate response for A2A payments at genuine higher risk of APP scams, it's not appropriate for Open Banking-enabled A2A retail

payments to merchants.

For these payments, merchants partner with a payment provider to immutably pre-populate the merchant's payment account details for the consumer. This means the consumer is unable to be convinced to change these details by an APP scammer. Furthermore, a merchant using Open Banking A2A payments in this way is also at much lower risk of themselves being a scammer, given the merchant is subject to additional due diligence by their Open Banking payments partner. This is on top of the detailed vetting already done by the merchant's own bank when providing them with a business bank account.

These factors explain why a report by the Open Banking Implementation Entity (OBIE) called out that the risk of APP fraud in merchant initiation via PISP as "**exceptionally low**",<sup>1</sup> and that the inclusion of Confirmation of Payee and other warnings in these payments was "inappropriate" and would introduce more friction and costs disproportionate to any benefits.

Finally, we also believe broader liability for reimbursement could negatively impact the economics of instant payments. At present, instant payments are typically free to consumers on the send side, with businesses paying to receive them. To claw back some of what they would spend on victim reimbursements, banks may pass higher costs on to businesses — which could sway a business' decision on whether to accept retail transactions using Open Banking. Banks may even begin charging consumers for making instant payments, as is common in other banking markets (including Europe). This would place Open Banking payments at a significant disadvantage to other payment methods that are free to the consumer.

### **Our suggestions**

Before implementing its APP scam proposals we think the PSR should first consider in more detail their potential impact on the ability of Open Banking-enabled A2A payments to effectively compete as a retail payment method. Reference to PISP-initiated payments only features in a single footnote in the PSR's current consultation and does not feature at all in the PSR's cost-benefit analysis. We think the PSR should conduct a separate cost benefit analysis of its APP scam proposals in light of the impact they could have on open banking payments, and the detrimental downstream impact this could have on the PSR's work to promote competition from A2ART for card payments.

Further, the PSR should support the burgeoning Open Banking ecosystem to enable richer sharing of data between Open Banking providers and banks. This will help support banks in making more targeted and informed decisions around the vulnerability of a specific A2A scenario to APP scams. Finally, industry-level data around fraud and Open Banking payments is currently extremely limited. We think this is something that the PSR and industry can help to collate to inform collaborative, targeted measures across the industry. Discussions on both of these points have been taking place in the Strategic Working Group (SWG) and should feature in the Joint Regulatory Oversight Committee's (JROC) thinking for the future roadmap of Open Banking.

---

<sup>1</sup> Open Banking Implementation Entity, [A2\(d\) – Open Banking Standards Relating to Confirmation of Payee and Contingent Reimbursement Model Code: Consultation Document](#), 2021

# Transpact

### Paragraph 3.5 states:

*'Stakeholders' concerns relating to the validation process were centred around receiving PSPs not having access to the fraud data held by sending PSPs. Data on fraud is held by the sending PSP, as they are the first point of data capture when a victim reports an APP scam. We were told that unless the sending PSP notifies the receiving PSP at the time of the fraud being reported, the receiving PSP may be unaware of this and may not have access to this data.'*

This paragraph encapsulates why failure of both the PSR and the FCA has allowed APP scams to continue in epidemic proportion in the UK.

In January 2019, the FCA introduced important new mandatory rules to make payee banks (receiving PSPs) liable for APP fraud. But neither the FCA nor the PSR has informed consumers and small businesses of these rules.

Therefore, when APP scams occur, consumers and businesses are not making claims against payee banks (they make claims only against their own bank, the payer's bank). In the majority of cases, any claim against the payee bank would lead to reimbursement to the consumer or small business making claim. But no such claim arises, as the claimant is unaware that they are in a situation that they are able to make a good, simple and winning claim (when indeed they are).

Due to lack of publicisation, consumers and small businesses are not making claims they are entitled to against payee banks.

So payee banks are not aware when APP scams occur.

Here is the crux of the problem, demonstrated in paragraph 3.5 of the PSR's consultation.

If the PSR publicised the rights available to small businesses and consumers - that they have (unbeknown to them) a very good claim against the payee bank in an APP scam case, the level of APP scam would be greatly reduced (and payee banks would be fully aware of all APP scams through their accounts).

But the PSR is not doing so !

### Giving final say to Sending Bank

The consultation seems to imply that after representation has been made by a receiving PSP back to a sending PSP, the sending PSP will have the opportunity to reconsider its data and where it deems appropriate make changes.

This strongly implies that the final decision about which PSP will be included within receiving PSP data will be up to the sending PSP.

But this ignores the fact that the sending PSP and receiving PSPs are in competition with each other. It is not fair nor appropriate to leave the final say up to the sending PSP – they may have commercial reasons to unfairly and/or wrongly attribute a receiving PSP as the receiving PSP, and damage that competitor thereby.

If a receiving PSP can provide evidence that they have been wrongly named as a receiving PSP, a mechanism must be introduced where the PSP can clear their name (and not simply leave it up to their competitor – the sending PSP – to do so).

### Indirect PSPs – late notice

We do not understand the PSR's proposals in the case of a sending PSP identifying a sponsor PSP as the receiving PSP, but the sponsor PSP within 2 months then provides evidence to the sending PSP that an indirect PSP was the true recipient.

Under the PSPs proposals, there does not seem enough time for the sending PSP to then provide evidence to the indirect PSP, and for the indirect PSP to be able to refute the allegation from the sending PSP (and prove to the sending PSP that they were mistaken).

If the proposals are left as written in the consultation, a number of indirect PSPs could end up getting falsely and wrongly attributed as receiving PSPs when they were not – and they will not get ample time to correct.

**Direction Order 4.1:**

The following definition is made in the PSR's order, as currently drafted:

*b. 'APP scam payment' means a payment that is executed by the sending PSP in accordance with an authorisation given by its customer, where the customer has been deceived into granting that authorisation as part of an APP scam.*

*This includes scams where:*

- 1. the payer intends to transfer the funds to a person other than the recipient, but is deceived into transferring the funds to the recipient; or*
- 2. the payer intends to transfer the funds to the recipient, but is deceived as to the purposes for which they are transferring the funds*

However, the existing definition of APP Fraud in the FCA Handbook states:

*a transfer of funds by person A to person B, other than a transfer initiated by or through person B, where:*

- (1) A intended to transfer the funds to a person other than B but was instead deceived into transferring the funds to B; or*
- (2) A transferred funds to B for what they believed were legitimate purposes but which were in fact fraudulent.*

There is a huge and glaring difference between the second parts of these two definitions.

In the currently operating (since 2019) FCA definition, an APP scam takes place where the payment reaches the intended beneficiary, but the purpose of the payment turns out to be fraudulent.

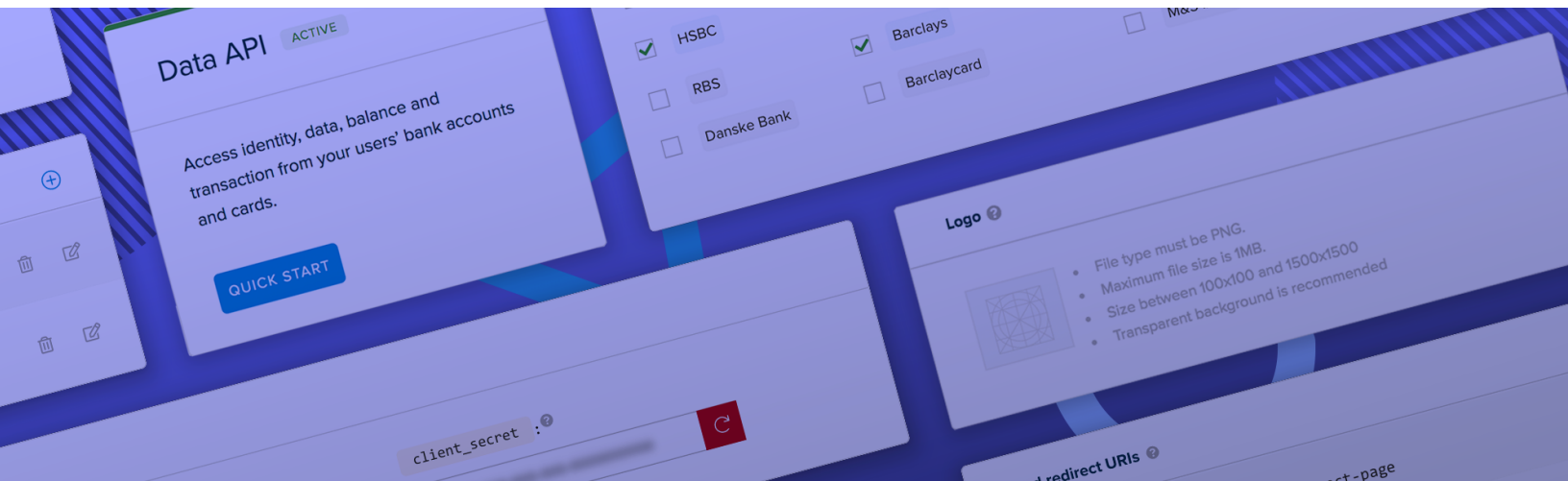
Under the PSR's proposals, a different measure for APP scams is used – fraud is not mentioned in the definition, and APP fraud is decided to have taken place whenever there is a deception of purpose for which the payment was made. This 'deception' is a much broader measure than 'fraud', and will include many, many more cases.

There is a strong material difference between the two definitions, with many real-world differences.

We strongly suggest that the PSR does not introduce a new definition of APP scam, which will confuse the regulatory perimeter by introducing two conflicting definitions, and instead sticks to using the existing FCA definition.

# Truelayer

TrueLayer consultation response to PSR CP22/4: Authorised Push Payment  
(APP) scams: Requiring Reimbursement



25 November 2022





## Authorised push payment (APP) scams: Requiring reimbursement

### TrueLayer response

#### About TrueLayer

TrueLayer is a UK and EU authorised payment service provider. We provide payments using open banking technology under permissions as an account information service provider (AISP) and payment initiation service provider (PISP).

#### Summary

We welcome the opportunity to respond to the PSR's consultation on APP scams. APP scams can have a devastating impact on victims' lives and we recognise the urgent need to tackle the issue.

We believe that the adoption of open banking payments by business and consumers will itself be an effective countermeasure to APP scams because open banking payments tackle the root causes of APP scams inherent in manual bank transfers.

However, we also believe the PSR's APP scam proposals, as they are currently formulated, put the viability of open banking at risk for the following reasons:

- **De-risking:** Open banking companies already struggle with banks limiting and blocking legitimate open banking payments. Imposing further liability on banks will reduce banks' risk appetites, leading to further limiting and blocking of legitimate open banking payments, and make open banking untenable as a payment option (removing a potential competitor to cards).
- **User experience** - even where banks don't block open banking payments, the current proposals are likely to incentivise banks to introduce additional friction in instant payment journeys (including those initiated by open banking), such as more screens, 'pop up' warnings and/or verification steps for consumers when authenticating payments.
- **Cost of faster payments** - It is likely that the proposed APP scam measures will increase costs for sending and receiving banks (e.g. costs of managing



disputes and FOS escalations). These will be passed onto merchants in the form of charges for receiving faster payments. This will make open banking an unattractive option for merchants, because the costs to receive faster payments via open banking will be greater than the cost to receive card payments.

We do not think that there has been sufficient consideration of these impacts of the APP scam proposals on open banking payments, evidenced by the fact that the only reference to payment initiation services in the consultation is a single footnote at section 4.6.

The PSR has rightly recognised that open banking has "the clear potential to facilitate account-to-account payments for retail transactions and compete with card systems."<sup>1</sup> Without further consideration, for the reasons set out above, TrueLayer are concerned the PSR's APP scam proposals present a significant risk to this potential and to the PSR realising its objectives in this space.

We would note that PISPs are only legally responsible for initiating payments, not executing them (which remains the bank's responsibility). PISPs are not direct or indirect participants in payments systems. There needs to be more clarity from the PSR that PISPs are not expected to take on liability for payments that they do not execute.

### **Proposals:**

#### **TrueLayer would ask the PSR, before it implements any final rules to:**

- Conduct a separate cost benefit analysis of its APP scam proposals in light of the impact they could have on open banking payments, and the detrimental downstream impact this could have on the PSR's work to promote competition from A2ART for card payments.
- Explicitly recognise the security benefits of open banking payments and consider how to support the **adoption** of open banking payments as an alternative to manual bank transfers as a **countermeasure** to APP fraud.
- Delay the implementation of any changes to liability until more data has been collected on whether existing APP scam measures (CoP and CRM) are working - We note that the latest UK Finance half-year APP fraud statistics (H1'22) showed — for the first time — a significant year-on-year reduction in APP fraud in both volume (-6%) and value (-17%) terms. Although undoubtedly

---

<sup>1</sup> <https://www.psr.org.uk/our-work/account-to-account-payments/>



still high in absolute terms, directionally this suggests that existing measures are beginning to have an impact on APP fraud and more time is required to assess their full impact.

We also note the proposal at section 6.7 indicating the PSR's expectation that Pay.UK will 'establish, maintain and enforce crossmarket arrangements on PSPs' conduct in a number of areas, including as part of its role in assessing and enabling use cases for the NPA, **such as open banking account-to-account retail transactions.**

- More clarity is needed from the PSR on what is meant by this, and how this interplays with discussions under JROC to develop a future entity to oversee open banking standards. **The TrueLayer strongly believes that standards relating to open banking providers should be the responsibility of the future open banking entity, not Pay.uk.**

### **Further detail**

#### **Why open banking payments can counteract APP fraud**

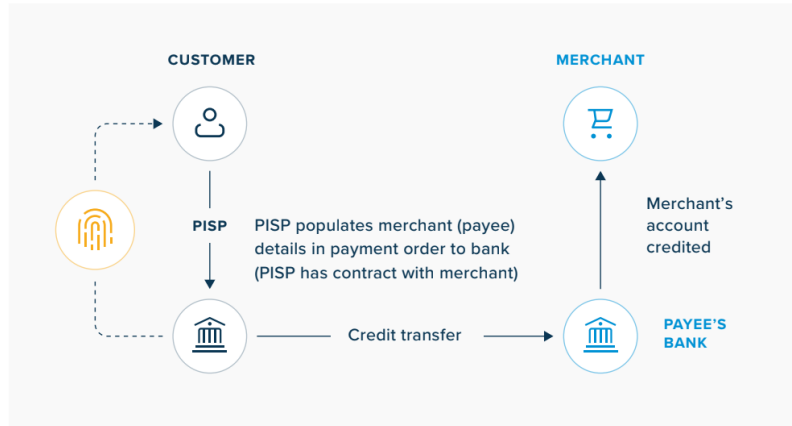
Open Banking payments to merchants are an inherently safer way to pay than other forms of payment, especially manual bank transfers, which are the main vector for APP scams. The way open banking payments are set-up addresses the risks of APP fraud because:

- **Open banking providers onboard and carry out due diligence with the payee** - When an open banking provider enables payments for a business, they enter into an ongoing commercial contract with that business, and undertake due diligence on the business as part of that. This reduces the likelihood that the beneficiary of an open banking payments will be used for fraud. In the unlikely event that fraud occurs - the open banking provider can immediately raise this with their client (the beneficiary).
- **Payee details (sort code and account number) are pre-populated by the open banking provider, removing the possibility of human error** when typing payee details or customers being tricked into sending money to an account controlled by a fraudster. The beneficiary's name is also presented back to the payer by the payer's banks in the authentication journey.

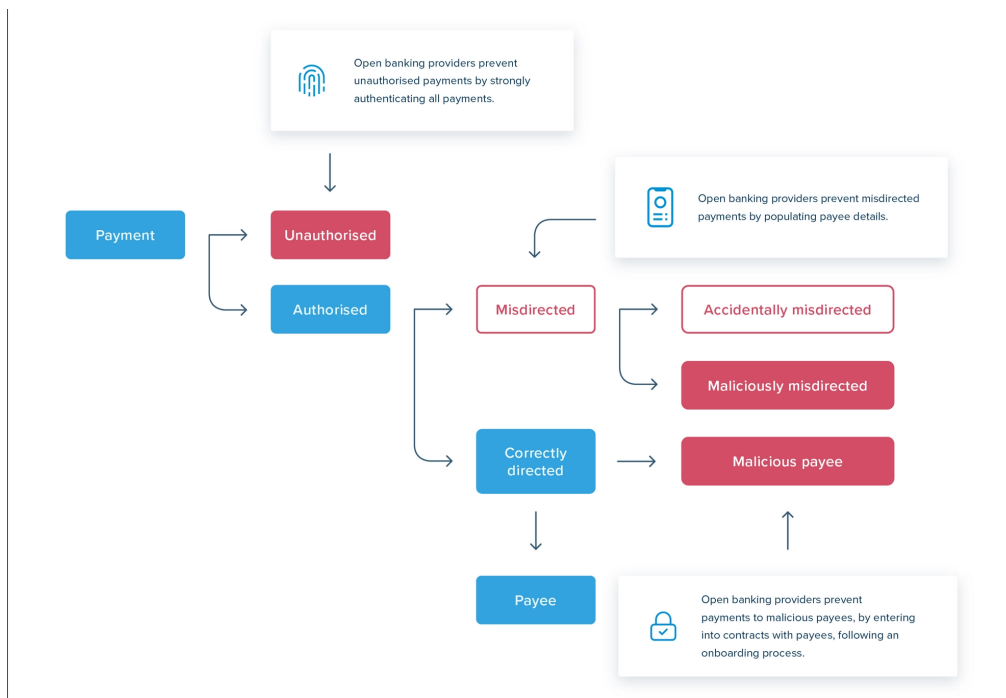


Fig. 3

Open banking payment to merchant: open banking provider populates the merchant's account details



How open banking prevents fraud (including APP fraud):





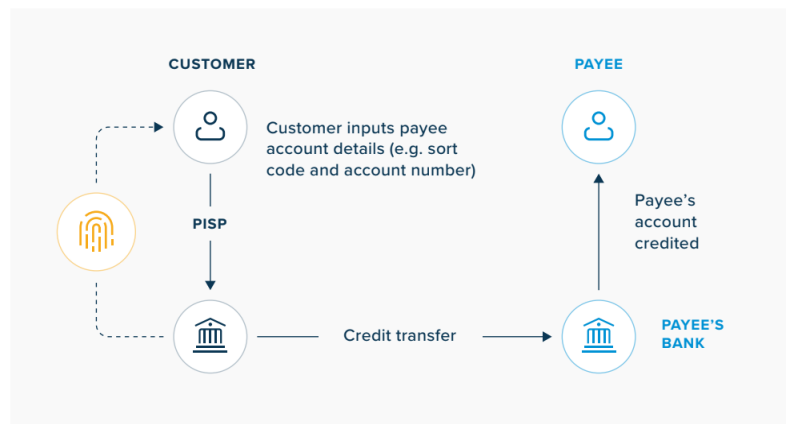
This is why the Open Banking Implementation Entity (OBIE) noted last year that, “the risk of APP fraud in Merchant Initiation via PISP is **exceptionally low**.”<sup>2</sup> (emphasis added).

Indeed, TrueLayer believes that as open banking payments replace manual bank transfers in day-to-day life - not only will APP fraud continue to decrease, but customers will start to see manual bank transfers as less convenient and less secure, and this will further reduce the risk of customers being involved in APP scams.

### Do all open banking payments reduce the risk of APP fraud?

Open banking payments can be used in a similar way to manual bank transfers in what are known as ‘party-to-party’ use cases. In this use case, the consumer (rather than the PISP) populates the payee details, and so therefore could potentially be manipulated into entering the wrong details. However, this use case is increasingly rare ([Yolt Pay](#) enabled this, with Yolt Pay, but has since closed down).

Fig. 2  
Open banking payment  
where consumer inputs  
recipient details



### How does a bank know if an open banking payment is low risk of APP fraud or not?

Parties across the open banking ecosystem already apply a risk-based approach to open banking payments. For example, banks in monitoring transactions for high risk factors, and TPPs conducting due diligence on the businesses they offer services to.

<sup>2</sup> Open Banking, [A2\(d\) - Open Banking Standards Relating to Confirmation of Payee and Contingent Reimbursement Model Code: Consultation Document](#), 2021



There are, however, changes in open banking standards that could be made that would enhance and assist the risk-based approaches applied by open banking ecosystem players.

Current OBIE standards enable PISPs to send ‘payment context codes’ to banks, which allows them to understand the risk profile of a payment. For example, a PISP can tag a payment with an ‘Ecommerce’ code, if the payment is to a merchant, or ‘party-to-party’ if the consumer is using the PISP to make a payment to another account of their choosing e.g. paying a friend.

The latest version of the OBIE standard - 3.1.10 - has introduced more detailed transaction risk indicators, which are supposed to give banks further information about the risk profile of payments, e.g.

- **ContractPresentIndicator** - Indicates if Payee has a contractual relationship with the PISP (the thinking being that if a PISP has a contract with the beneficiary, they will have undertaken due diligence, lowering the risk of any payments to the beneficiary).
- **BeneficiaryPrepopulatedIndicator** - Indicates if a PISP has immutably pre-populated payment details in for the PSU (the thinking being that if a PISP has populated the payee details (as opposed to the consumer), the payment will not be vulnerable to APP fraud).

However, the implementation of these TRIs and PCCs is voluntary and is not being coordinated by the OBIE. This risks inconsistent and patchy implementation by both PISPs and banks. It risks the benefits of payment risk information not being realised - and a continuation of arbitrary risk management by banks, leading to more PISP transactions being limited or blocked.

We recommend that the OBIE or future entity coordinate the implementation of TRIs to better transaction risk information sharing.

### **De-risking**

It is important to highlight the implications the PSR’s proposals for APP reimbursement may have on the development and adoption of Account to Account (A2A) Retail Transactions.

The PSR believes that A2A payments will increase choice for merchants and consumers and give an additional option for both POS and e-commerce transactions,



however if the proposals for APP reimbursement were to set the benchmark for A2A this could significantly damage this proposed new payment option.

A 'reimburse first, investigate later' culture applied to A2A payments may mean that banks build such a robust and defensive economic model around them that they are unlikely to be economically appealing as a payment method.

In open banking this could manifest in banks blocking and limiting transactions initiated by PISPs to payees they perceive to be in higher risk sectors.

There is already evidence that banks are de-risking in the way that they are blocking payments for entire sectors like crypto ([Santander](#) is blocking payments to crypto exchanges in 2023 and Starling bank has already [cut off crypto payments entirely](#)).

### **User friction**

We believe that the current proposals are likely to incentivise banks to introduce additional friction in instant payment journeys, such as more screens, 'pop up' warnings and/or verification steps for consumers when authenticating payments. This will damage the payer experience and reduce trust in Open Banking overall, and is despite the fact that the OBIE concluded that for PISP-initiated payments, *"[Confirmation of Payee and Contingent Reimbursement Model pop up] warning messages are of limited utility and that the resultant additional friction together with the incremental costs of deployment are not justified. Indeed, emerging evidence from our consumer research suggests that there would be positive benefits from eliminating the overuse of warning interventions; customer fatigue erodes their effectiveness."*<sup>3</sup>

TrueLayer also believe there will be an increased propensity for banks to suspend payments for fraud checks and look to generally slow down the payment process. One approach for achieving this we are aware is being discussed, is to introduce delays in faster payments transactions so that banks have more time to scrutinise payments. This could have a significant negative impact on open banking payment propositions.

### **Cost of faster payments**

Changing the liability model for reimbursing APP scam losses may prompt ASPSPs to revisit the economic model they use for instant payments and e.g. increase charges to

---

<sup>3</sup> Ibid



businesses for instant payments, or even consider introducing charges to consumers for sending or receiving Faster Payments.

Businesses are typically charged by their banks to receive Faster Payments into their bank account, with fees varying significantly and typically being lower for larger businesses (for example, one CMA9 bank offers tariffs charging £0.35 per incoming payment for businesses <£5m turnover and £0.15 for larger businesses). By comparison, when using Card payments, low value transactions are typically charged on an ad valorem basis (i.e. percentage of transaction value). The BRC recently reported that merchants on average pay 26bps of turnover to accept debit cards (small merchants can pay significantly more than this). On an absolute basis this amounts to ~3p for a £10 sale.

This means that open banking payments are already uncompetitive with card payments at low values. The APP liability shifts could further exacerbate this problem and prevent open banking A2A payments from being a competitive constraint on card payments.



TSB



TSB Bank plc  
20 Gresham Street  
London  
EC2V 7JE

## TSB Bank response to Payment Systems Regulator Call for Views on Authorised Push Payment (APP) scams

9<sup>th</sup> December 2022

**Sent to:** appscams@psr.org.uk

We introduced the TSB Fraud Refund Guarantee (FRG) in April 2019, and it remains the gold standard of fraud protection.

Over this period TSB has proven that refunding victims is the right thing to do – for consumers and as a commercial proposition.

TSB supports the PSR's efforts to significantly improve the protections that fraud victims have when seeking a refund from their bank and a move to mandating reimbursement.

While we support the key elements of the PSR's proposals we do not support the proposals to allow a £100 minimum threshold and the £35 excess for claims. We feel that this approach could discourage the reporting of low-value fraud and also have a disproportionate impact on poorer fraud victims.

TSB has conducted research which shows that losing up to £100 can have a huge impact on people's lives. 16% of people in the UK would struggle to afford to buy food if they lost this much, 12% said they would struggle to pay their rent/mortgage and 15% said their mental health would be affected.<sup>1</sup>

On the topic of fraud, the priority for regulators and policy makers should be to protect fraud victims from the devastating financial harm that results from becoming the victim of fraud. However, that is not to say that TSB believes that the entire cost of refunding the victims of fraud should be borne by PSPs.

Over the past three years, TSB data on the incidence of fraud proves that the "moral hazard argument" that reimbursing fraud victims will lead to them acting recklessly is unfounded. However, there is little discussion of the moral hazard created by shielding large tech firms, telcos and social media companies from the true costs of the harm they enable. While the sectors that enable fraud are insulated from the costs of fraud the UK will be fighting fraud with one arm tied behind its back. Ultimately it is the fraudsters and organised crime who will continue to benefit if the focus is only on victim compensation by the banking industry and not also on fraud prevention. The 'polluter pays' approach is an important incentive to ensure those best able to prevent the harm in the first instance are held to account and incentivised to put effective controls in place.

Over the course of 2022 Facebook has accounted for 58% of all social media purchase scams reported by TSB customers. TSB cannot prevent fraudsters operating on Facebook Marketplace however we are currently bearing the cost for each one that does and where the victim happens to be a TSB customer. Facebook could choose to take steps to reduce the fraud that their platform facilitates. However, they have no financial incentive to do so while TSB – and other banks if the PSR's proposals are implemented - underwrite the cost of the fraud they enable. If Facebook is not able to prevent fraudsters operating on their platform it does not follow that PSPs should be held financially liable for the damage done by their business. To use the environmental analogy again, polluters should pay for the pollution they emit.


---

<sup>1</sup> TSB Fraud survey prepared by Savanta, Fieldwork Conducted 12th - 13th August 2022 (sample size 2236)

TSB supports the PSR's work to strengthen the protections that all consumers receive if they fall victim to fraud. We have led on this issue, and we are pleased to see regulators and policy makers have responded by moving to an approach much closer to our own.

However, mandatory reimbursement treats the symptoms not the disease. Once mandatory reimbursement is in place regulators and policy makers must move rapidly to establish a mechanism to allow PSPs to recover costs from social media firms, telcos and other businesses that enable fraud.

Without this approach, we will not be able to tackle the overall incidence of fraud and it is likely to remain the number one crime in the UK.

  
**Director of Fraud and Financial Crime,**  
**TSB Bank plc**

## Q1 – Do you have views on the impact of our proposals on consumers?

TSB is proud to have offered what we believe to be the gold standard of fraud protection in the industry to our customers for over three and a half years as a result of our unique Fraud Refund Guarantee (FRG). Over this period, we have been a lone voice challenging prevailing orthodoxy and leading by example by proving that refunding victims is the right thing to do – for consumers and as a commercial proposition.

Many of the proposals outlined by the Payment Systems Regulator (PSR) in their consultation document align with the design of our FRG and we believe they will represent a significant step forward for consumer protection in the UK.

The methods used by fraudsters evolve all the time, as do products and services offered by banks, building societies and payment service providers (PSPs). However, consumer protections relating to fraud have not kept pace with this change and they still draw a simplistic distinction between payments which are unauthorised (where consumers are provided with high levels of protection) and those which are not (where there are very few consumer protections).

Most fraud which happens in the UK today is either on payments which were fully authorised by consumers or is on payments which sit in a grey area between being authorised and unauthorised (for example, where payments were instigated by a fraudster but partly approved by the genuine customer). Without action from regulators, UK consumers are fast approaching the point where existing statutory protections are insufficient against the majority of scams which they are likely to fall victim to.

Previous attempts to address this issue have so far fallen short. The development of the Contingent Reimbursement Model (CRM) had good intent but many banks and PSPs have still not signed up to this voluntary scheme. For those who have, data shows that the code is applied inconsistently. Refund rates have increased recently but still sit at just over 50%, on average, as against 97% of claims refunded by TSB. In short, consumers who fall victim to the most common frauds in the UK face a lottery as to whether they will be reimbursed – with the notable exception of those who bank with TSB.

Overall, we believe that the proposals outlined by the PSR will offer consumers improved and more consistent protection against Authorised Push Payments (APP) scams, with a greater proportion of consumers' APP losses being reimbursed than they are today, resulting in peace of mind and a higher degree of trust by consumers in the faster payments scheme.

Much has been made of the fact that the PSR's proposals will drive up fraud by increasing moral hazard. And indeed, these proposals may result in increased 1<sup>st</sup> party fraud attempts. However, TSB's experience over the last 3½ years offering the Fraud Refund Guarantee has demonstrated that increased customer protection does not reduce their motivation to protect themselves to falling victim of fraud. At TSB, we regularly use data provided by our trade body, UK Finance, to compare our customer fraud losses to the industry as a whole. This analysis has consistently shown that our losses are below our normal market share of accounts. Indeed, our share of losses has generally declined since we introduced our Fraud Refund Guarantee.

In summary, we believe that this point is mere conjecture. Whilst it sounds plausible, it is not borne out by our data. Scams don't happen to our customers because they make reckless decisions safe in the knowledge they will be protected by our FRG. Rather, they happen because these are sophisticated crimes carried out by ruthless criminals enabled by technology firms, social media companies and telcos who have little incentive to prevent fraud while the costs of fraud fall to consumers and PSPs. As an example, Facebook accounted for 58% of all social media purchase scams reported by TSB customers so far in 2022. Whilst we have borne the cost for each customer who fell victim to a scam on Facebook Marketplace, Facebook ought to take steps to reduce scams facilitated via their platforms but they currently have no incentive to do so. If Facebook is not able to prevent fraudsters operating on their platform, it does not follow that PSPs should be held financially liable.

That said, we do believe that consumers will see changes being made to payment processes across the industry as a result of these changes proposed by the PSR. Banks don't need extra incentives to invest in systems and controls to prevent fraud from occurring: fraud already impacts their bottom line and existing UK regulations (e.g. the Financial Conduct Authority's SYSC sourcebook) already creates an obligation on all firms to prevent fraud

from occurring. However, as a result of these changes, banks and PSPs are likely to add additional friction into the payments journeys as an additional line of defence to reduce the harm caused by fraud and the additional financial liability that will be placed on banks as a result of these new reimbursement rules. Consumers can expect payments to be slowed down, and some payments will be refused as PSPs focus on providing 'safer payments'. It is our view that delays and cooling off periods are the most effective way of delivering interventions where fraud is suspected, and this additional friction, on the whole, will be beneficial for UK consumers. However, it will reflect a significant change in the payments landscape and, from the perspective of the recent focus of payments innovation (i.e. speed), a retrograde step.

As an example, in the final quarter of last year, TSB implemented blanket restrictions on bank transfers and card payments to known crypto currency platforms in response to seeing very high rates of reported fraud for such payments. This decision was taken in part by the existence of our FRG and the fact that we were ultimately the point of refund for all losses which arose, as well as the need to protect our customers. Similar examples of additional friction can be expected across other banks as a result of the changes proposed by the PSR.

## Q2 – Do you have views on the impact of our proposals on PSPs?

We agree with the summary of the impacts on PSPs set out in the consultation, namely that proposals will increase the cost of APP scams reimbursement for most PSPs – even if the costs are redistributed between sending and receiving PSPs.

In our experience of offering our Fraud Refund Guarantee, however, this cost increase is more than offset by reductions elsewhere. For example, our claim and complaint handling costs are lower than they would otherwise be and all of our fraud risk management activity can be focussed on prevention rather than resolving disputes with individual customers on the merits of their request to be reimbursed.

We believe that the proposals may impact the amount of competition in the industry on the basis that smaller or newer PSPs may see their business models impacted by the aggregate impact of refunds to victims. Individual high value cases could create prudential impacts. However, on balance our view is that this would be positive overall if it improves standards of consumer protection across the industry. PSPs whose business models today are not impacted by the financial impact of fraud are really only being insulated from the cost rather than truly avoiding it.

More widely, the proposals outlined by the PSR will place all of the costs of reimbursing victims onto PSPs even though the vast majority of these frauds are facilitated by other sectors. Whilst it may be outside the remit of the PSR, we believe that a mechanism needs to be developed to allocate these costs onto other sectors that enable fraud, including telecommunication and social media companies. Without this, the root causes that enable fraudsters to operate at scale and with virtual impunity will not be addressed.

### **BOX 1: Cost Recovery and fraud enabling sectors**

We note that this view is supported by the House of Lords Fraud Act 2006 and Digital Fraud Committee who recently recommended the creation of a mechanism whereby fraud enabling sectors share the cost of refunding fraud victims.<sup>2</sup>

*“To incentivise companies to act on fraud and more accurately reflect the balance of responsibility for fraud, the Government must establish a mechanism by which fraud-enabling sectors—in addition to the outgoing and recipient PSP—are required to contribute to the costs of reimbursement in cases where their platforms and services helped to facilitate the fraud. In making these changes, the Government must ensure that these reforms do not complicate the victims’ experience of reimbursement; they should retain a single point of contact.” - House of Lords Fraud Act 2006 and Digital Fraud Committee, Fighting Fraud: Breaking the Chain’*

TSB was also pleased to hear similar views expressed by Chris Hemsley, Managing Director, Payment Systems Regulator during an evidence session with the Treasury Select Committee on 25 May 2022.

<sup>2</sup> Paragraph 401: [The UK has retreated from the fight against fraud, says Lords Committee - Committees - UK Parliament](#)

TSB Bank plc. Registered Office: Henry Duncan House, 120 George Street, Edinburgh EH2 4LH. Registered in Scotland No. SC95237. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Registration No. 191240).

*"It is possible. One thing that is worth exploring, as we go forward, is that, if it can be demonstrated clearly that the fault lies with a social media firm, it is then a bit difficult to look the payment firms in the eye and say, 'You are responsible for refunding'. It is important that people get that refund, but it is a legitimate question as to whether they can recover those costs from those who have ultimately caused the problem."*<sup>3</sup> - **Chris Hemsley, Managing Director, Payment Systems Regulator** (In response to a question on social media firms compensating fraud victims. TSC PSR session)

Finally, the proposals only focus on faster payments and will not cover "on us", CHAPS or authorised frauds on cards. The latter in particular is a growing threat for consumers and banks.

### Q3 – Do you have views on the scope we propose for our requirements on reimbursement?

As stated previously, the proposals outlined by the PSR would not extend to 'on us' and 'CHAPS' which we believe is far from satisfactory. All payment types are covered by our Fraud Refund Guarantee and even the Contingent Reimbursement Model includes these two payment types. We do not believe that voluntary coverage of these payment types would be an appropriate solution.

We also do not support the proposals to allow PSPs to set a 'fixed excess' of up to £35 and a minimum threshold claim for reimbursement of up to £100. Research previously conducted by TSB showed that a fraud loss of up to £100 would result in the following:

- 16% of customers surveyed would struggle to afford food for themselves/their family for more than one week;
- 12% of customers surveyed would not be able to afford their rent/mortgage;
- The mental health of 15% of those surveyed would be badly affected.

Furthermore, this aspect of the proposed scheme is intended to act as a mitigant to prevent first party fraud and to reduce moral hazard. Our view is that it will do neither of these things. As such, our recommendation is that no such excesses are applied. In practice, we suspect that very few firms would apply these excesses anyway.

One area that we do believe requires further clarification in the reimbursement rules relates to the definition of an Authorised Push Payment fraud and the definitions to be used for sending and receiving banks. Whilst they might seem straightforward they are anything but.

- Many claims raised by customers fall into a grey area between a scam and a civil dispute. For example, purchase scams often share similar characteristics with civil disputes between a buyer and a seller. Investments which do not pay out the promised rate of return often do not clearly segment into case of fraud or reckless investment management. Insufficient thought given to this area could result in banks underwriting the performance of all other industry sectors, when realistically they cannot police the integrity of legitimate trades and service providers.
- Many scams often involve monies being moved between different accounts. Some of these accounts may be in the name of the customer and some may have been opened as part of the scam. We see some cases where the customer has no knowledge of accounts opened in their name, others where they were involved in part in opening them and others where both the customer and the fraudster have access to the account via security credentials. It is not clear in such cases which bank was the point of exit for the funds and therefore which ones should be classed as the "sending account" and "receiving account".

Greater clarity needs to be given on both of these points for the PSR's proposals to be workable.

<sup>3</sup> <https://committees.parliament.uk/oralevidence/10320/html/>

#### **Q4 – Do you have comments on our proposals:**

- **That there should be a consumer caution exception to mandatory reimbursement**
- **To use gross negligence as the consumer caution exception**
- **Not to provide additional guidance on gross negligence?**

We support the proposals made by the PSR. TSB has utilised different exemptions in our Fraud Refund Guarantee although we believe that they would, in practice, amount to the same standard as that of “gross negligence”.

Whilst guidance additional to that provided by the FCA would be welcome, we understand that it can be challenging in practice. Authorised Push Payment frauds tend to be very case-specific and documenting what a “gross negligence” standard would look like would be incredibly challenging. It would also need to vary based on scam type and any document which contained such a definition would become very unwieldy and most likely of limited benefit in practice.

The only exception we would recommend is one based on the concept of ‘good faith’; in other words where the payer has manifestly failed to act in good faith, particularly where they may obtain some financial gain from their actions. This would clearly include any involvement by way of first party fraud (eg obtaining a ‘backhander’ payment from the fraudster) but also where the payer has known there is a very high likelihood of the transaction being fraudulent but nonetheless cynically proceeded in the slim hope of making high returns and on the basis their paying bank would pick up the cost. This seems entirely fair in the very rare exception where bad faith can be proven, on the civil law test of the balance of probabilities and will also go some way towards further mitigating against moral hazard.

Our Fraud Refund Guarantee takes into account a negligence standard, albeit against a very high bar, effectively amounting to bad faith. The basis on which we believe that our FRG does not increase moral hazard is only because this negligence/bad faith standard exists.

#### **Q5 – Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We do not support this proposal.

FCA guidance on customer vulnerability makes clear that vulnerabilities can come in many different types. These can range in impact, severity and duration. The idea that all customers meeting any vulnerable customer definition need take no care at all with payments will almost certainly increase moral hazard and 1<sup>st</sup> party fraud.

Our recommendation would be to require PSPs to take customer vulnerability into account as part of assessing any fraud claim.

#### **Q6 – Do you have comments on our proposal to use the FCA’s definition of a vulnerable customer?**

We support this proposal and have no further comments.

#### **Q7 – Do you have comments on our proposals that:**

- **Sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement**
- **Any ‘excess’ should be set at no more than £35**
- **PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?**

Please see our response to question 3.

**Q8 – Do you have comments on our proposals that:**

- **Sending PSPs should be allowed to set a minimum claim threshold**
- **Any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

Please see our response to question 3.

**Q9 – Do you have comments on our proposal not to have a maximum threshold?**

We do not agree with the proposal not to have a maximum threshold.

The TSB Fraud Refund Guarantee (FRG) has operated with a £1m claim limit since launch. In practice, very few claims have got close to this figure and a much lower maximum claim limit would still have achieved exactly the same outcomes for virtually all our customers.

In our experience higher value cases tend to be the most complex. Simple approaches to reimbursement models tend not to provide a helpful framework for assessing refunds on such cases.

Maximum thresholds more closely aligned with that for the Financial Services Compensation Scheme (£85k) or the Financial Ombudsman Scheme redress limit (£375k) are more likely to achieve the stated aims of the PSR.

In addition, if the PSR is concerned about the impact of competition and continuing to encourage innovation in the payments market then a useful tool would be to implement a maximum claim value. This would cap liability on exceptional cases and limit the extent of any prudential risk which may arise on new or small firms from time to time.

The absence of a maximum threshold would also sit in stark contrast to the existence of a £100 minimum threshold to make a claim – offering greater protections for wealthier fraud victims while potentially excluding poorer fraud victims from the same protections.

**Q10 – Do you have comments on our proposals that:**

- **Sending PSPs should be allowed to set a time limit for claims for mandatory reimbursement**
- **Any time limit should be set at no less than 13 months?**

Since its launch the TSB Fraud Refund Guarantee has operated with only one condition relating to the timings of claims being raised – namely that the guarantee only covers payments made on or after the launch of the scheme (14<sup>th</sup> April 2019). There is otherwise no time limit for customers raising fraud claims.

We would strongly recommend that, at the very least, the PSR introduce a start date for any new protections introduced as a result of their proposals. Not taking this step would be tantamount to retrospective regulation which we do not believe would be an appropriate step.

In terms of the proposal to set a claim time limit, on balance we believe that including such a limit in the design of the scheme is appropriate even though it would differ slightly from our current Fraud Refund Guarantee. Investigating historic claims can be challenging, not least because many rely on obtaining testimony from the customer or bank staff involved. It is also important from a fraud prevention perspective that victims do have some sort of appropriate incentive to raise claims as quickly as possible so that steps can be taken to prevent others falling victim to the same scam.



In terms of what the actual time limit should be, there is merit in the 13 month proposal in that it would align with protections for unauthorised payments and therefore avoid confusion in the minds of consumers.

In practice, we believe that a 13 month upper limit is likely to make little difference to victims. In our experience of having offered our guarantee for over three years, almost all victims of fraud raise their claim relatively quickly. For example, of all the claims made in 2022 only in around 0.3% of cases did the customer take more than a year to contact us after the payments in question had been made.

#### **Q11 – Do you have comments on our proposals that:**

- **The sending PSP is responsible for reimbursing the consumer**
- **Reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of 1<sup>st</sup> party fraud or gross negligence?**

We support the proposal that the sending PSP is responsible for reimbursing consumers.

We also agree that reimbursement should be made as soon as possible, however we disagree with the requirement to do this within 48 hours.

TSB have taken an industry-leading approach to fraud refunds and the treatment of victims for three and a half years through our Fraud Refund Guarantee. In operating this guarantee, we have refunded around 80% of claims within 5 days.

Fraud claims on authorised payments tend to be complex and investigations into cases tend to take longer than for unauthorised fraud. Scams can be elaborate and involved several counterparties. Concerns of first party fraud are also more prevalent given the broader spectrum of payment recipients (compared, for example, to vetted payment card merchants), but evidence is unlikely to be available within such a short timeframe which would meet the standard proposed by the PSR.

Tasks which typically take several days to complete can include obtaining evidence from customers, obtaining testimony from bank staff involved in making payments, obtaining information from the receiving banks and, in some cases, validating some information with law enforcement.

Allowing for more rigour in the validation of claims by the remitting bank would also be a more effective tool to deter first party fraud claims than the recommended £100 minimum claim value.

Furthermore, APP fraud scam victims could be placed under excessive pressure to provide relevant supporting evidence to their bank in order to enable them to meet this timeframe. This could create a poor customer experience and would be emotionally stressful for victims of scams.

We therefore propose a period of no less than 7 days as a minimum, in itself an improvement on the current Contingency Reimbursement Model timescales of 15 business days or 35 days for extraordinary cases.

We also propose that PSPs be expected to publish reimbursement rates and timescales.

#### **Q12 – What standard of evidence for gross negligence or 1<sup>st</sup> party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Standards of evidence for gross negligence/bad faith (see answer to Q4 above) and first party fraud should align to those defined by the PSR for unauthorised transactions which are in place today.

We acknowledge the risk that a broad adoption of protections of this nature could see a rise in 1<sup>st</sup> party fraud attempts however in offering these protections in isolation, TSB has not seen an increase in moral hazard and first party fraud since the Fraud Refund Guarantee was implemented. We have, however, experienced isolated cases of first party fraud which we mitigate via controls within our claims process.

It is not clear to us what benefit would be served by making notifications to Pay.UK and such a regime would run counter to the existing approach for unauthorised fraud. This arrangement is likely to provide limited benefit to consumers and only serve to increase costs across the industry.

At most, we agree that Pay.UK could be well placed to provide principles-based guidance.

**Q13 – Do you have comments on our proposals for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

We support the proposals for a 50:50 split in reimbursement costs on the basis that it is the most sensible and would avoid convoluted and time-consuming dispute resolution models. This model also ensures that all participants in the payments chain are suitably motivated to prevent and detect mule accounts, which is an area that currently (aside from CRM Code signatories) participants are only required to undertake best endeavours recoveries.

That said, we would recommend that this approach be closely monitored over time to measure its success and assess any unintended consequences.

We would also recommend that any settlements between receiving and sending PSPs be subject to appropriate timescales and that guidance is issued on the time limit for payments to be made between firms.

**Q14 – Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

We have two concerns with allowing for arbitration on individual cases:

- Firstly, in the long run, variation from 50:50 on individual cases is likely to make little or no difference to either costs or outcomes. Firms requesting to vary from 50:50 will win some cases and lose others but most likely end up back at 50:50 overall once the scheme has run its course over time.
- Secondly, that firms with most resources (i.e. larger banks with large legal teams) will stand to benefit most from the existence of any such scheme. Arbitration outcomes are more likely to be based on the resources expended by legal teams than the merits of each case.

Therefore, we believe that the 50:50 cost split should be fixed with no option for variation in individual cases (subject to close monitoring, as stated above).

Given that one of the benefits of such a mechanism would be to limit the impact on competition and payments innovation, as stated previously, a more effective tool would be to place a limit on the maximum claim value.

It is acknowledged that there may be 'regular offenders' in the payments chain, either acting as remitters or as beneficiaries, where there may be a desire to take cases to arbitration. We would suggest that such offenders will be more appropriately managed by (a) the publication of MI on fraud levels, and (b) the steps likely to be taken by other PSPs to insert greater friction into their customers payment journeys where they choose to send/receive payments from those offenders.

**Q15 – Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

Our response to question 3 outlined our view that greater clarity needs to be given to defining "sending bank" and "receiving bank" for the purpose of assessing fraud claims whilst reflecting the complexity of dealing with scam 'chains' that involve unwitting mules who may have moved funds onwards to 3<sup>rd</sup> party accounts under false pretences. Should this be done effectively, there is no need for a bespoke approach for multi-generational scams.

**Q16 – Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

We agree with the proposal.

It is also our view that clear expectations need to be set around the timeframes for returning any recovered funds.

**Q17 – Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We have no additional comments.

**Q18 – Do you have views on our long term vision, and our rationale for the PSO being the rule setter responsible for mitigating fraud?**

In general, we believe that rules around refunds for authorised fraud should adopt the same approach as for unauthorised fraud. That is, be specified in primary legislation.

We believe that any other approach is likely to only increase complexity and introduce additional costs into the system which would ultimately be passed onto consumers.

If this were not possible in the short term, then we believe a PSR-issued direction on all firms would be the best immediate option.

**Q19 – Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

We have nothing to add above and beyond our comments in response to question 18.

**Q20 – Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

We have nothing to add above and beyond our comments in response to question 18.

**Q21 – Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

We have nothing to add above and beyond our comments in response to question 18.

**Q22 – Do you have comments on our preferred short term implementation approach of requiring Pay.Uk to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

In line with our response to question 18, we do not believe this is an area where Pay.UK should play a role. We believe this will only increase complexity and introduce additional costs into the system which would ultimately be passed onto consumers.

Monitoring adherence to reimbursement rules would be best carried out via normal regulatory supervision with the Financial Ombudsman Service acting as an arbitrator on individual customer fraud claims as per the position today.

**Q23 – Do you have views on the costs and benefits of Pay.UK implementing a real time compliance monitoring system and when it could be introduced?**

TSB Bank plc. Registered Office: Henry Duncan House, 120 George Street, Edinburgh EH2 4LH. Registered in Scotland No. SC95237. Authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and the Prudential Regulation Authority (Registration No. 191240).

We have nothing to add above and beyond our comments in response to question 22.

#### **Q24 – Do you have views on the best option for short term enforcement arrangements?**

We have nothing to add above and beyond our comments in response to question 22.

#### **Q25 – Do you have views on the best way to apply the rules on reimbursement for indirect participants?**

We do not believe that any special arrangements are necessary in this regard. Application of the rules to direct participants will enable application to the indirect participants they support and ensure that the same standards are applied.

#### **Q26 – If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

Under this approach we would see no downside to directing all firms.

#### **Q27 – Do you have any comments on our cost benefit analysis at annex 2 or any additional evidence relevant to the analysis?**

We are broadly supportive of the cost benefit analysis, however:

- We believe it is unlikely that the incidence of scams will fall by £100-£150m.
- The proposals relating to victim reimbursement in themselves are unlikely to result in an uplift in investment from PSPs in respect of fraud prevention.

The proposals outlined by the PSR will improve the protections for victims, but banks already have strong incentives to prevent fraud from occurring (as mentioned previously). Such a significant reduction in the incidence of fraud could only be achieved through a step change in response from other sectors which facilitate fraud including social media, technology and telecommunication firms. Since these proposals will create no additional incentives for these firms to take action, the proposals in themselves will most likely make no difference to the amount of fraud which occurs.

PSPs are just one set of actors in the end-to-end fraud ecosystem. It is wishful thinking to believe that imposing additional costs onto PSPs (whilst the right thing to facilitate refunds for victims) will result in new opportunities being developed to prevent fraud which were not identified or progressed in the absence of that requirement.

That's not to say there will not be significant benefits to consumers and firms from the proposals being adopted. As stated in response to question 1, since we introduced our Fraud Refund Guarantee, 97% of claims have been refunded by TSB. Our own assessment of this scheme has confirmed that it is the best approach for our customers, is consistent with the severity of these crimes, reduces costs elsewhere in our business, does not increase moral hazard and does not create risks of first party fraud that we cannot mitigate via our normal controls. At the same time, our overall rate of fraud losses is below our proportionate share of overall industry losses. We would endorse the approach outlined by the PSR to any firm and believe this will be a significant step forward for consumer protections in the UK.

#### **Q28 – Do you have any comments on the proposals in this consultation?**

We do not have any additional comments.

# UK Finance

# UK Finance response to Payment Systems Regulator Call for Views on Authorised Push Payment (APP) Scams

**Date:** 9<sup>th</sup> December 2022

**Address:** APP Scams Team  
Payment Systems Regulator  
12 Endeavour Square  
London  
E20 1JN

**Sent to:** [appscams@psr.org.uk](mailto:appscams@psr.org.uk)

UK Finance is the collective voice for the banking and finance industry.

Representing around 300 firms across the industry, we act to enhance competitiveness, support customers, and facilitate innovation.

If you have any questions relating to this response, please contact:



## Introduction

Fraud is now the most prevalent crime in England and Wales, accounting for 41% of all crimes in the year to June 2022. More than £609.8 million was stolen through fraud and scams in the first half of 2022, with authorised push payment (APP) fraud losses comprising £249.1 million of the total. UK Finance therefore welcomes the Payment Service Regulator's (PSR) call for views on APP fraud.

However, UK Finance and its members feel strongly that while a necessary step, a reimbursement model alone will not slow the UK's growing epidemic of scams, nor prevent the non-financial impacts on customers and industry. Consumers are better protected when they are educated, responsible and alert to the threat and its consequences. Knowing that they will almost certainly be reimbursed – no matter their actions – removes the incentive for customers to take sensible steps to reduce their risk of being defrauded.

Moreover, we believe that the plans will encourage more complicit fraud and exacerbate the problem as fraudsters capitalise on the opportunity of near-100% reimbursement.

We strongly believe that there is much more that could be done to prevent fraud, including:

- Allowing firms to slow a small number of high value payments where fraud is suspected
- Allowing firms to trace funds after the first payment and legally enable repatriation of funds through the chain of subsequent payments. Effectively treating funds as proceeds of crime
- Enable data sharing across sectors to identify scammers and mules
- Bring all fraud-enabling sectors, including social media giants and the telecommunications sector, into the solution
- Increased law enforcement capacity and capabilities to capture and stop criminals

We are concerned that, if implemented as outlined, this model will have unintended consequences, negatively impacting most consumers, with the costs of reimbursement inevitably passed on through increased friction in payment journeys, reduced choice, and increased costs for payment services. This risk of pass through was clearly recognised by the FCA during a consultation on FSCS, another industry-funded customer protection scheme, with respondents invited to comment on the 'ability of firms to "pass through" costs to customers'<sup>1</sup>. The reimbursement of fraud victims will ultimately be financed by other customers and this model increases the burden on them.

The model, as proposed, would see uncapped liabilities for clearing banks which will threaten the sustainability of the indirect access provider banking market. If not carefully considered and delivered in an effective way, we may see many small and innovative PSPs lose access to payments services altogether. There will be a significant impact on the potential growth of open banking payments, as well as the development and adoption of account-to-account retail transactions, curtailing the opportunity for innovation in this market.

Generally, we do not see a way that the proposed approach can work without having an impact on competition and innovation.

The PSR's proposal for reimbursement places all liability – and therefore effectively responsibility – for fraud and scams onto PSPs. However, there is a much wider ecosystem of firms whose platforms and infrastructure are used by criminals to target and socially engineer victims. The PSR's proposals do not consider the liability of the technology sector controls and the sector's role in fraud enablement.

UK Finance data shows that 70% of reported APP scams originate through an online platform<sup>2</sup>. 96% of investment scams and romance scams originate online and that figure rises to 98% of all purchase scams. A means to ensure financial accountability on the part of platforms, internet service providers and telecommunications sectors is needed to create aligned incentives and shared accountability for fraud prevention and reduction.

The current legal timeframe for processing outbound payments – a day plus one after initiation of a payment – does not enable appropriate time for PSPs to engage with vulnerable customers to seek to dissuade them from making payments. This issue must be resolved.

In addition, there is currently no clear legislative framework to enable freezing and repatriation of funds to victims of fraud. The Payment Services Regulations 2017 do not expressly provide a means for Firm A to repatriate funds to Firm B to reimburse a victim. PSPs have been proceeding at legal risk in doing so and there is considerable inconsistency in approach and outcome as well as delays in reimbursement for victims.

### **What we propose:**

**A clear definition of a scam payment** supported by detailed scam specific guidance to ensure consistent views across PSPs, the regulator, and the FOS. The definition must:

- Be clear where a scam originates. The consultation uses the phrase 'APP scams happen when fraudsters trick someone into sending a payment to a bank account controlled by the fraudster'. The definition should be positioned directly around this point, limiting a scam payment specifically to one generation i.e., the singular payment which places the scam funds into the control of the criminal.
- Show how to distinguish between a private civil dispute and a purchase scam, or a poor investment and an investment scam. Otherwise, there is considerable risk that the

---

<sup>1</sup> Compensation framework review, DP21/5, FCA ([Link](#))

<sup>2</sup> <https://www.ukfinance.org.uk/press/press-releases/over-two-thirds-of-all-app-scams-start-online-new-uk-finance-analysis>



reimbursement framework would lead to the financial industry underwriting consumer purchases and high-risk investments and would fuel disputes between PSPs and the Ombudsman.

- Clearly define which scenarios are in scope. For example, payments to Ponzi schemes and pyramid schemes should be out of scope where it is made clear to the person at the outset that the basis of joining the scheme and ultimately making money is through the recruitment of others. In such a scenario, there is no dishonesty, it falls outside of section 2 of the Fraud Act 2006 and anyone who joins on the back of this does so at their own risk.

**Development of a simple Consumer Contributory Negligence exemption.** Gross negligence should not be the only exception for reimbursement. This sets the bar too high and risks moral hazard across customers. Our recommendation is that the consumer negligence determination be based on simple principles which are easily communicated and can evolve over time. If a customer's negligence facilitates the successful completion of the scam payment, the customer reimbursement would be proportionally reduced. The cost of the remaining reimbursement would then be shared 50:50 by the sending and receiving PSPs. This will still achieve the PSR's aims of incentivising PSP investment in scam prevention and markedly increase the level of reimbursement for customers.

**The inclusion of an industry-wide upper and lower threshold.** UK Finance and its members strongly advocate the inclusion of an upper limit. We see this as an essential tool to limit the emergence of moral hazard. While there is some divergence of views around the inclusion of a lower threshold, there is agreement that, were one to be included, it should be consistent across PSPs. The level should be determined through the analysis of industry data.

**Development of a practical timeline for reimbursement.** Our members cannot support the 48 hour reimbursement timeline proposed. Until there is evidence that the new reimbursement model can overcome several of the current operational challenges, we would recommend maintaining the existing 15 / 35 day timeline of the CRM Code, for a period following implementation. There will be a significant increase in number of PSPs who will be engaging in this reimbursement approach who have no experience in operating within an APP liability framework. The timelines may in the long term be shortened where there is evidence that they are achievable.

**Implementation through PSR Directions of all PSPs** to adhere to the mandatory reimbursement rule meaning consistency and clarity across all participants. A direction means the reimbursement rule can be implemented within an expedited timeframe. Scheme rules could be used in parallel to set minimum standards for participation. These may then evolve over time with the changing fraud landscape and the introduction of new prevention measures.

In the long term, we strongly believe **the reimbursement rule for authorised fraud must be placed on the same legislative footing as unauthorised within the PSRs 2017.** This will mitigate the risk of the authorised fraud threat migrating to other payments schemes. UK Finance and its members propose working with HMT and regulators to agree changes to PSRs 2017 to include a specific and detailed definition of an authorised payment scam, clarity regarding scope and the obligations and liability framework. It will be necessary to make clear in legislation who has responsibility for the monitoring and enforcement aspects of the reimbursement framework. We strongly believe that these roles should fall to the regulator, leveraging enforcement capability already available to them.

**We strongly advocate the PSR continuing to work with UK Finance, its members, and HM Treasury to develop an alternative model** to ensure that the ultimate model strikes a better balance between consumer protection and the commercial viability and competitiveness of the sector.



**We believe the following needs to take place before we can support implementation of a reimbursement framework:**

**An end-to-end strategy for tackling scams at source is developed.** While we recognise that the PSR's remit only applies to PSPs, we would strongly encourage them to urgently come together with their counterparts in HM Treasury, the Home Office, the Department for Digital, Culture, Media and Sport, the Financial Conduct Authority, Ofcom and others, to devise and implement a comprehensive strategy for tackling scams that includes requirements for all relevant actors and which apportions liability fairly.

**The Online Safety Bill is passed.** The Bill will deliver urgently-needed protection to shield consumers from becoming victims of fraud and prevent criminals from attaining stolen funds then used to perpetrate further criminality. Whilst the Bill is designed as a standalone measure, additional complementary work through the Online Advertising Programme will be needed to examine the role of the entire ecosystem in relation to fraud as well as other harms caused by online advertising.

**Legislation is passed to provide private sector information-sharing powers with the non-AML regulated sectors.** We suggest these powers should be limited in application to the scope of entities regulated by OFCOM. This data sharing capability is critical to enable the financial services sector to work directly with these sectors to inform threat assessments and proactive fraud prevention activity.

**Amendments are made to Regulations 86 and 89 of the Payment Services Regulations 2017 to allow the adoption of a risk-based approach to payments** to enable enhanced scrutiny of high-risk payments across the faster payments scheme allowing time for PSPs to engage with vulnerable customers to dissuade them from making payments.

**A statutory framework to prescribe minimum standards and processes to govern investigation, response, and repatriation of funds to victims has been created.** Providing PSPs with the comfort to repatriate where funds have been frozen within beneficiary accounts.

## Question 1: Do you have views on the impact of our proposals on consumers?

UK Finance and our members are supportive of the PSR's ambition to ensure victims of APP scams receive a consistent approach to reimbursement regardless of who they hold their account with. We support the PSR's proposal for reimbursement to be fairly shared between sending and receiving PSPs, but we remain of the opinion that it is important for consumers to take appropriate measures to protect themselves and for consumers' actions to be considered within the reimbursement model. We understand the PSR's desire to drive the incentives for financial services firms to invest in scam prevention, however we strongly believe that the proposals outlined by the PSR may have unintended and negative impacts on consumers – both directly, in terms of their payment experience and indirectly, through the impacts on the financial services ecosystem.

### **Reduced consumer caution and an increase in APP scams**

Some of our members have strong concerns that a mandatory reimbursement rule which does not have sufficient level of consumer caution included may reduce consumer incentives to take appropriate measures to protect themselves against APP scams. This will, in turn, make consumers more vulnerable to APP scams, and mean increased funds flow into the criminal economy, which will galvanise the focus of criminals on this type of fraud.

UK Finance has one member PSP which has operated a similar reimbursement model for over three years and does not believe that this has created moral hazard across its customer base. However, other members have called out significant concerns about the risk of an increase in moral hazard, noting an unvalidated assumption by the PSR that the experience of that PSP can be extrapolated for the whole industry without moral hazard emerging. This is a sentiment supported by the House of Lords report (Page 162, paragraph 57) which states, 'While we recognise the case for mandatory reimbursement of victims of APP fraud, we are concerned that a blanket reimbursement policy may lead to increased levels of moral hazard and fraud, and the perception that it is a 'victimless crime'. In some cases, it may even lead directly to new avenues for APP-reimbursement frauds.'

Before finalising the reimbursement approach, we urge the PSR to conduct detailed analysis on the potential unintended consequence of moral hazard across differing customer demographics and scam types. We would also recommend that the PSR review the approach to reimbursement being considered by regulators in other countries, which have explicitly considered moral hazard in the design of their systems.

Policy documents released by the Monetary Authority of Singapore suggest that consumers must contribute to losses they incur to create incentives for them to be vigilant against fraud. Evidence shows that moral hazard implications are being considered during the framework drafting: although the authority expects financial institutions to treat their customers fairly and bear an appropriate proportion of losses arising from scams, it made clear that care must be taken to ensure that compensation paid to customers does not weaken their incentives to be vigilant.

Whilst in the EU, following a period of consultation, in October 2022, the EU adopted the finalised '*Proposal for a Regulation of the European Parliament and of the Council amending Regulations (EU) No 260/2012 and (EU) 2021/1230 as regards instant credit transfers in euro*', whose Impact Assessment provides interesting indications of options rejected for the time being. One of which was a proposal which would give consumers the right to ask for a refund under certain circumstances, which included where that individual could satisfy that a payment was authorised under fraudulent circumstances. This request would need to be submitted within a certain timeframe and would require the payer to evidence that its intention was to send the payment to a different payee.

This option was not factored into the final proposal based on several considerations, the most relevant of which being moral hazard concerns. The document expressly provides that "more lenient

refund conditions may give rise to greater moral hazard in the form of unfounded refund claims". The EC expects that a mandatory reimbursement regime would amount to increased fraud rates (as victims who currently do not report would feel encouraged to seek reimbursement) and ongoing compliance costs, particularly if the moral hazard factor is not effectively contained.

### **Reduced incentives for action by other sectors**

The payment from victim to fraudster sits at the end of the scam journey, which is the last opportunity to identify and defend against a scammer. Most scams are perpetrated through criminals exploiting vulnerabilities in other sectors, such as the online platforms (e.g., social media, online sales, dating websites etc) and telecommunications sectors, to target, engage and scam victims. It is therefore critical that all sectors across this 'scams ecosystem' take the action necessary to prevent criminals targeting their infrastructure. The banking and finance sector has been at the forefront of cross-sector collaboration and data sharing in the recent years, and we have seen several successes where Financial Services intelligence and data can mitigate the attacks. We are concerned that the PSR's proposals to introduce PSP mandatory reimbursement spanning all scam types, will ease the mounting pressure in this space for other sectors to act appropriately to mitigate risk and subsequent consumer harm, ultimately leaving consumers vulnerable.

### **Increased friction in payment journeys**

If the reimbursement model is implemented, as outlined, it is almost inevitable that wide reaching, irreversible, changes will be applied to offset the potential increased moral hazard - impacting how consumers make payments through the Faster Payments Scheme.

In recent years industry has been striving to achieve the right balance in applying friction, through the introduction of dynamic warnings and the implementation of Confirmation of Payee, whilst still maintaining a simple, streamlined customer experience. With the proposed move to a two party liability model, almost entirely removing consumer responsibility, industry will introduce additional friction into certain payment journeys across the FPS rails. This friction will be designed to reduce moral hazard through incentivising the consumer to exert effort by increasing the perceived cost of fraud on them. Whilst the PSR acknowledge this within the consultation, their expectation is that friction only impact a small proportion of payments, believing that liability imposed by the reimbursement model will encourage firms to introduce back-end solutions to mitigate the APP risk. In contrast, industry— particularly those firms that already have sophisticated fraud detection capabilities - recognise that the most effective way to mitigate APP scams before they enter the payment system, is to add friction at the front end through the collection of information on the payment and conversations with the customer. This may mean that ultimately the existing instruction to make a payment may move towards an application for payment handling, supported by customer evidence. This will negatively impact genuine payments and customers and therefore growth of the economy,

Industry will require guidance for situations where the PSP and the consumer reach an impasse over the legitimacy of the payment. PSPs recognise the benefit of maintaining a relationship with their customer where they have identified the potential risk of susceptibility to scams. The increased liability risk to PSPs however may incentivise PSPs to take an earlier decision to provide notice to close in situations where they are unable to 'break the spell'. This will be to the detriment of the customer. The new PSP will not have access to the customers payment history or knowledge of the previous PSP scam concerns. This may leave the customer at greater risk of being scammed again.

We must also recognise the risk that additional friction may make payment journeys more challenging for some consumers, creating the unintended consequence of pushing consumers towards more traditional payment methods such as cash and cheques, neither of which are within

scope of reimbursement models and which, in the case of cash brings with it unique personal security risks.

We have outlined in detail the inevitable need for additional friction across FPS payments if the PSR move forward with their current proposals. For consumers accustomed to operating in a seamless payment environment, this may create irritation and potentially levels of stress. As such these changes must be communicated by a centrally coordinated HMT / Regulator led public announcement campaign, highlighting the reasons why additional questions will be asked and, in some circumstances, evidence required when making payments.

### **Emergence of a claim management market**

The PSR proposals are also likely to encourage a growth in claim management companies taking on APP scam cases for customers, taking fees of circa 25-50% from victims for successful reimbursements. This market is already emerging in response to the CRM Code. Noting the deductions made, this would result in a worse outcome for victims of APP scams compared with the position today.

### **Migration of scam payments to other payment channels**

There is a risk that authorised payment scams might migrate to other payment channels. For example, the PSR note this risk, specifically referencing card payments, but observing that 'Card systems have existing consumer protections in place'. Many issuers have reported an increase in authorised card scam payments in recent years. In October, UK Finance, working with issuers, conducted a pilot MI collation exercise which has supported members' anecdotal claims that this is a potential industry threat.

However, the precise scale of the issue is at present unclear and as a result there is some divergence in views. Issuers have indicated that they would benefit from further clarification and guidance around the reporting of this type of fraud. The Card schemes are working collaboratively with UK Finance and its members to develop additional guidance to help close the current gap.

The risk of migration is of course not just limited to card payment systems, but the current proposal to address authorised fraud in one system will encourage criminals to alter their approach, instead directing consumers towards other payment channels. Therefore, it will be important to keep this monitored and UK Finance will continue working with members to better understand the issue.

### **Impact on Service**

In the future, repeat victims of scams, may find it harder to access normal retail banking products. The PSR note that PSPs should treat current and prospective customers according to their obligations in the Equality Act 2010, however on the basis that PSPs may restrict access to full payment services, on a case by case basis, to protect individual consumer this can be evidenced as "objectively justified".

Our members also suggest there is a risk that the proposals will result in negative impacts on the market for banking and payment services in terms of pricing, investment in innovation or market choice as firms respond to the proposals to limit risk and cover costs, which in turn will impact on the services for consumers. PSPs may seek to recover the costs of mandatory reimbursement by increasing the charges levied to businesses for Faster Payments, or even to consider introduction of consumer charges for Faster Payments. The introduction of a mandatory reimbursement model in addition to Confirmation of Payee will bring significant costs for PSPs. Small PSPs or those with an international footprint may deem the UK market too expensive to remain a viable proposition. If the PSR pursue their preferred option for ensuring in-direct PSP participation, we would also expect

to see a decline in innovative products and services as Direct FPS participants seek to limit their risk exposure, declining to offer payment services to PSPs who may, initially at least, carry more risk.

We recognise the PSR's intentions in proposing a 48hr timeframe from claim to reimbursement is to reduce the period of uncertainty for consumers. However, we strongly suggest that this may not always be in the customer's best interest, potentially adding additional pressure to consumers who are already feeling vulnerable following the occurrence of the fraud / social engineering. The speed of the proposed reimbursement may also leave consumers at risk of further attempted exploitation if the criminal is still in contact.

The suggested lower threshold for eligibility will significantly reduce the incentive for consumers to report low value frauds to their PSP. This will limit the opportunity for PSPs to provide early education, potentially leaving consumers exposed to further exploitation.

The potential for PSPs to set their own thresholds, excesses, and time limits, will be confusing for consumers, even more so if they hold payment accounts across multiple PSPs. This is exacerbated further if, as part of the scam, the consumer has made payments across multiple PSPs and potentially payment schemes, with differing protections offered across schemes.

## **Question 2: Do you have views on the impact of our proposals on PSPs?**

UK Finance and its members agree with the PSR's view that the mandatory reimbursement proposals, as outlined, will increase the cost of APP scam reimbursement for most PSPs.

We clearly articulated throughout our response to CP 21 – 10 the need for receiving PSPs to play a greater role in the reimbursement of scam victims, which we believe will incentivise them to play a stronger role in prevention. We are therefore supportive of the PSR's proposal that the cost of reimbursement should be shared with receiving PSPs.

However, as with our previous consultation responses, we remain of the opinion that the proposal to incorporate the obligation to reimburse into scheme rules is neither an effective nor proportionate way to achieve a reduction in the volume and occurrence of APP scams. We recognise and support the PSR's position that reimbursement is an important component in addressing the APP scam problem but believe strongly that it is required as part of a wider approach covering education, legislative change, tech development and effective engagement and collaboration of the wider ecosystem.

As such, we question why the PSR is continuing to pursue delivery of the reimbursement model via FPS scheme rules, specifically considering the limitations, as outlined by the PSR concerning the incapability of Pay.UK to apply rules to on-us payments, indirect participants, and the limited ability to enforce these rules.

The proposals if delivered as outlined in full, create uncapped liabilities for clearing banks which may have unintended consequences for the sustainability of the indirect access provider banking market. If not carefully considered and delivered in an effective way, we may see many small and innovative PSPs lose access to payments services altogether. The PSR's preferred approach of reimbursement rules applying to all payments, creates an unnecessary complexity in interposing clearing banks between the ASPSPs that manage payment end user accounts, giving rise to disputes between clearing banks and clearing customers, as well as between the sending and receiving PSPs.

Generally, we do not see a way that the proposed approach can work without having an impact on competition and innovation. There is tangible evidence of firms moving away from the market following the introduction of cheque imaging. The introduction of a mandatory reimbursement model,



in addition to industry wide CoP may see some small firms decide that the costs of operating within the UK Market are too high to be viable and international firms may choose to close their UK accounts.

It is important to highlight the implications the PSR's proposals for APP reimbursement may have on the development and adoption of Account to Account (A2A) Retail Transactions if this payment model were to be adopted by industry. The PSR believe that A2A payments will increase choice for merchants and consumers and give an additional option for both POS and e-commerce transactions, however if the proposals for APP reimbursement were to set the benchmark for A2A this could significantly damage this proposed new payment option. A 'reimburse first, investigate later' model applied to A2A payments may mean that PSPs build such a robust and defensive economic model around them that they are unlikely to be economically appealing to merchants. Added friction in Faster Payments would also reduce their ability to compete effectively with other forms of retail transactions. PSPs may be disincentivised to onboard certain merchants, those from perceived higher risk sectors for example. And we may see a significantly increased in the number of consumers who feel that any 'change of heart' on a transaction, or slight grievance with a product, can be pursued as a reimbursement from their PSP in the first instance.

The PSR propose the inclusion of PISP initiated payments within scope of the FPS rule, although there was no detail provided in the consultation paper on how this might work in practice. There are limitations on what PSPs might do to mitigate fraud risk in a PISP initiated payment, owing to rules on the CMA9 requiring frictionless transaction. There is no indication within the consultation that PISPs will be included within the liability model. If it is proposed that sending and receiving PSPs continue to share the burden of liability, some UK Finance members argue that the restrictions within the OBIE Customer Experience Guidelines must be lifted, as well as placing requirements on PISPs to share payment information with the ASPSP that is relevant for fraud detection, including payment purpose. However, UK Finance PISP members have expressed concerns that removing such restrictions would reduce the overall Open Banking payment proposition and customer experience.

Central to the PSR's proposals is the exception for gross negligence. No clear definition of gross negligence has ever been found that is suitable to be applied to fraud cases, especially those linked to digital or modern payment systems. Without clear and precise guidance, for each specific scam type, there will be disparity in interpretation across PSPs which may ultimately, with receiving PSP liability based on the sending PSP victim assessment, result in conflict between PSPs and an increase in consumer complaints. In addition, there is the risk that we see repetition of the failures of the Code, where there was huge disparity across PSPs and the Financial Ombudsman Service (FOS) both in interpretation and case outcome. This ultimately damaged the credibility of the Code across consumers.

The PSR proposal that PSPs may only deny reimbursement where a consumer has been grossly negligent or there is evidence of first party fraud brings significant risks for PSPs. In H1 of 2022, 56% of all scams were purchase scams, of which 90% of these were under £1000. Low value purchase scam payments are extremely difficult for PSPs to detect and prevent because they are not easily differentiated from other low-value payments. Once identified it is then often challenging to determine if they fall within the scope of a scam or a dispute, as there is often very limited evidence available. On the other end of the scale, only 5% of all scams were investment scams, but these made up a significant 25% of the value. Whilst generally more likely to be detected by transaction monitoring tools, investment scams pose their own challenges, as once a risk is identified, it can be difficult to deter customers from making what they believe is a sound investment using warnings alone. The inherent delay in a consumer recognising that they have been the victim of an investment scam also hampers PSPs ability to freeze and repatriate funds to the victim, which can be further complicated by assessing whether the claim is an investment scam or a poor return on a failed investment. Without the right framework in place there is considerable risk that the proposed rule change would lead to the financial industry underwriting online purchases and high-risk investments conducted with

little or no care taken by the consumer. Additionally, the PSR proposals, in placing reimbursement entirely on the shoulders of PSPs, removes all responsibility from online auction sites and social media platforms to create additional controls to prevent low-value scams and high value fraudulent investments. It is only through greater scrutiny of online sellers that these scams can be prevented.

PSPs must be provided with the necessary tools to enable them to achieve good customer outcomes. If relevant amendments to legislation are not agreed, where potential risk is identified, PSPs will face a “liability dilemma”, make the payment and risk liability or decline the payment and risk legal action by their customer for breach of mandate.

The loss of life savings can have a significant emotional and financial impact on customers. As such, protecting against this risk should be a higher priority to the regulator than allowing customers to have immediate access to funds or to have those funds transferred in all circumstances. Whilst we accept that the instances where thorough extended investigation might be necessary are small, the key point is that the impact on customers where APP fraud does arise can be life-changing. In short, the risk of an APP scam occurring is low probability but high impact, and a proportionate solution which enables PSPs to hold payments where risk is identified would appear to be the right approach to achieve good outcomes for customers versus the relatively limited downside of delaying certain payments

The PSRs 2017 require firms to comply with the payment execution timescales. Whilst PSPs can intervene, warn, and advise customers where it is believed they may be being scammed, PSPs currently have no regulatory comfort to hold the payments past D+1 or to stop the execution of that payment unless instructed by the customer to do so. We ask for changes to Reg 86 to enable PSPs to pause the execution of a payment past D+1 where there is a high risk of fraud. We have a similar situation for receiving PSPs. Many PSPs have implemented inbound transactional monitoring and are actively, successfully freezing funds as they are received. However, this approach is inconsistent, and some PSPs question the legality of the process when considered against the requirements within Regulation 89 of the PSRs 2017. Where PSPs identify funds, they suspect may be the proceeds of a scam, we ask for changes to Reg 89 to allow the payment to be paused and assessed, on the balance of probabilities, suspicions of fraud and seek return of any of the customer’s funds that have been able to be frozen, alongside protections for the receiving PSP to freeze and release funds back to the account of a sending PSP following an assessment of fraud.

Changes to the PSRs 2017 to enable PSPs to take the necessary actions to intervene were they have reasonable suspicion of fraud, supported by industry agreed wording for PSP T&Cs to mitigate the risk of a consumers taking legal action against PSPs on the grounds of unfair terms where a payment is delayed, must be delivered prior to or at the very least, in parallel to the proposed reimbursement model.

Where consumers are resistant to fraud warnings and wider engagement both from PSPs and Law Enforcement, and continue to engage in scam activity, PSPs recognise the importance of maintaining the PSP and customer relationship, limiting the risk of continued victimisation if they provide notice to close their account and the customer moved to an alternative account provider. Under the current regime, there is no industry guidance or standard of care for PSPs to follow when responding to a customer who is “under the spell” of a scam. The increased liability risk to PSPs may incentivise PSPs to take an earlier decision to provide notice to close in such situations. To counteract this risk, we ask the PSR to work collaboratively with UK Finance and its members to develop a standard of care for victims of scams who are “under the spell”. We propose that this would necessitate engagement with victim care charities, Law Enforcement and Social Services. The standard should provide PSPs with a clear indication of when the customers care should be handed over to an external agency.

Finally, we cannot ignore the operational and administrative costs which will accompany the introduction of this model. It is not clear what the costs may be for PSPs in supporting the central administration regime, but these are likely to be significant. In addition, the costs and resources required to operationalise this model within PSPs are likely to create disproportionate burden on smaller firms who have no previous experience of a centrally managed reimbursement model. This must be considered when determining the timeline for implementation.

### **Question 3: Do you have views on the scope we propose for our requirements on reimbursement?**

It is essential that the 'scope' of PSPs, sending and receiving accounts and the specific payments which fall within bounds of the reimbursement rule are clearly defined and not open to interpretation. The scope must be robust and clearly defined with key examples detailed within supporting guidance. Lack of specification will lead to inconsistent interpretation across PSPs, the regulator and the FOS and ultimately deliver inconsistent customer outcomes.

The consultation is clear that the scope of the proposed reimbursement model covers all payers who are:

- consumers
- micro-enterprises who employ fewer than ten persons and whose annual turnover and / or annual balance sheet total does not exceed €2 million and
- charities with annual income of less than €1 million and is a charity as defined in relevant legislation in the UK
- included in measure three is Faster Payments only, with on-us payments proposed to be voluntary. We discourage this voluntary approach and instead ask that the PSR be clear in their requirement and mandate the inclusion of on-us payments for all PSPs. Without specific direction, the reporting across firms will be inconsistent.

The PSR clearly articulate their expectation that PSPs reimburse on-us payments in the same way as payments made via the Faster Payment Scheme but note that their powers do not extend to regulating payments which fall outside of designated financial services. Irrelevant of this we discourage the voluntary approach proposed and ask that the PSR be clear in their requirement, mandating the inclusion of on-us payments for all firms, mirroring the approach taken with Confirmation of Payee. Without specific direction there is the risk that adoption across firms will be inconsistent.

Payee account scope must be clarified by the PSR. In the introduction to the consultation, the phrase "APP scams happen when fraudsters trick someone into sending a payment to a bank account controlled by the fraudster" is used. Our view is that the rules should be positioned directly around this point, limiting the rules specifically to one generation of payment, i.e., the singular payment which placed the scam funds into the control of the criminal.

It is essential that the reimbursement framework be applied to all PSPs who hold the account of customers receiving payments via the Faster Payment Scheme. For regulated financial institutions holding payment accounts, their inclusion seems clear, however this is less clear when we move into the realm of Foreign Exchange and Crypto Exchange firms where funds are layered through wallets or paid into unregulated firms.

The use of Crypto and Foreign Exchange firms to launder the proceeds of scams is a consistent challenge for industry, and with the use of holding accounts across these business models, there is often differing interpretations between PSPs, the regulator, and the FOS as to what point in the payment chain, the scam has occurred. It will be essential that this is clearly defined within the reimbursement rules.



In September 2021, UK Finance with its members developed a set of industry principles to help define the origination of a scam.

These principles are outlined below:

- If the account at the crypto / foreign exchange was opened in the consumer's name, without the consumer being aware and the consumer is subsequently socially engineered into moving funds into the holding account, at which point the criminal has control, this will be classified as one generation payment as in scope for the victim PSP to assess. For the avoidance of doubt if a consumer was intending to invest in the commodity being offered through the exchange/account then we would consider the customer to have had awareness and this exception would not apply.
- If the account at the crypto / foreign exchange was opened by the consumer, either independently or via an instructed third party and was done so either through their own decision or under the direction of the criminal and the consumer then knowingly transferred funds into their wallet before creating an onward payment to a wallet under the control of the criminal, then this will be out of scope for the victims PSP to assess as this involves multiple transactions and the consumer's first payment was to an account held in their name. PSPs should direct the consumer to contact the crypto exchange at which they hold the wallet.
- If the account at the crypto / foreign exchange was opened by the consumer, either independently or via an instructed third party and was done so through their own decision or under the direction of the criminal, and the consumer knowingly transferred funds into the wallet, where they reasonably were aware that another party had access, or where they subsequently provided their credentials to a third party, any subsequent payments made out of that account either authorised or unauthorised will be out of the scope for the victims PSP to assess and will be the responsibility of the crypto exchange firm to resolve.

For the avoidance of doubt, as well as sharing security credentials with a third party, allowing a third party to set up the account on their behalf or providing remote access during the process will be considered sufficient to confirm the customer was reasonably aware that a third party had access. The customer choosing not to attempt to access the wallet directly, either before or after the transaction should not negate this point.

For unregulated firms who are the recipient of first-generation scam funds, we encourage the PSR to consider a rule which ensures the regulated entity who own the client relationship be mandated to pass any losses onto that client, should they be found to exist – i.e., levy a charge against that client equal to their loss, minus any repatriation.

Crucially, the PSR must provide a clear definition, supported by guidance of what constitutes an APP scam.

The PSR are clear that mandatory reimbursement would not apply to private civil disputes, however without clear definition and guidance on how firms are required to identify a poor investment, a purchase dispute or other civil dispute, there is considerable risk that the proposed rule change would lead to extended closure times for customer claims, disputes between PSPs, and the financial industry underwriting consumer purchases and high-risk investments.

Mindful of this risk and of the high proportion of purchase scams which originate due to enablers outside of the financial industry, it is the preferred option of a proportion of the UK Finance membership that this scam type be excluded from scope of the proposed mandatory reimbursement

model. Purchase scams are fundamentally different to any other scam type. They rarely involve any element of social engineering and in most cases will not have the lasting emotional and financial impact of other scams. Instead, members recommend that an alternative separate reimbursement process should be developed recognising these fundamental differences, with specific SLA's and detailed documentation providing PSPs with clear guidance to ensure consistency in interpretation between a purchase scam and a civil dispute. UK Finance propose working with the PSR and its membership to develop this alternative model.

We recognise that this will not be an appealing proposal and therefore urge the PSR, if purchase scams in scope, to ensure the necessary guidance be provided to PSPs to mitigate the inconsistencies which will occur when investigating these cases both across PSPs and the FOS.

Equally, greater clarity is required when considering the scope of an investment scam. Firms should not be required to provide reimbursement for investments made to unregulated firms or where the consumer had prior awareness of the high risks.

In the circumstances around the formation and operation of 'pyramid schemes', advice was sought from experts and professionals from several different fields – Gambling Commission, Trading Standards, City of London Crime Academy, Crime registrar and Corporation of London Solicitors. They summarised that these schemes are a specific offence under Section 43 Gambling Act (Chain Gift scheme). The offence is committed by a person who 'invites another to join a scheme or knowingly participates in the promotion, administration, or management of such a scheme.

The operation of 'Chain Gift Schemes' is a specific crime. In its defined form there would be no dishonesty element as these schemes are run on an invitation basis and entry is by paying a joining fee, the fee is then recouped by recruiting others to join, it is on this basis a gamble on the part of the participant that they will recover their original outlay and even make a profit. It is not an offence for persons to join the scheme, but it is for that person to invite others to join.

Taking the above into account, if it is made clear to the person at the outset that the basis of joining the scheme and ultimately making money is through the recruitment of others then there is no dishonesty and therefore falls outside of Sec2 Fraud Act 2006 and anyone who joins on the back of this does so at their own risk.

The PSR note that it is their expectation that payments initiated by Payment Initiation Service Providers (PISPs) are in scope for the new reimbursement model. However, no further detail is provided on how this might work in practice. For instance, it is unclear from the consultation how the role of PISPs will be considered within the proposed 50:50 liability model to ensure that all PSPs within the payment chain are accountable for fraud prevention and are liable for their share when a scam takes place. As demonstrated by the Enhanced Fraud Data Proof of Concept developed and coordinated by UK Finance with its members, an important part of scam detection and prevention is based on the Sending PSP knowing information about the payment (including the payment purpose), so that they can provide effective and timely scam warnings to the customer, to try to 'break the spell'. Transaction Risk Indicators do exist within Open Banking, but with no mandate for PISPs to supply the data and a lack of detailed guidance, the necessary data is generally not available for the ASPSP to effectively detect fraud risk. The CMA9 are further hampered in this space through the restrictions imposed through the Customer Experience Guidelines, which limit the level of friction allowed within an Open Banking transaction, removing the ability of these PSPs to overlay effective fraud warnings and Confirmation of Payee checks.

However, it is important to recognise that there are several different payment propositions offered by PISPs in the market, and that these propositions present significantly different levels of risk for APP fraud. One of the more common PISP propositions is known as "Merchant Initiation via PISP",

where a PISP has an underlying contract with a merchant and a PIS payment option is made available by the merchant to customers. The OBIE recently evaluated different PISP propositions for risk of APP fraud and concluded that “Merchant Initiation via PISP” payments were of “exceptionally low” risk. This is due to several factors including pre-population of payee account details and PISP due diligence on merchants. Further, the OBIE argued that introducing confirmation of payee or additional warning screens to these payments would introduce “inappropriate and unnecessary friction”, “additional unnecessary cost and effort” and risked “degradation of overall effectiveness of warning interventions”. Any extension of scope of the PSR’s proposals to PISP payments, and associated treatment by ASPSPs, needs to be risk-based and take account of the different types of PISP propositions and associated risk of APP scams.

To consider PISP payments in scope of the proposed reimbursement model, these issues will need careful addressing, to ensure that Open Banking payments do not become a target for fraudsters, who seek to avoid the controls and warnings that are otherwise in place in FPS payments made through ASPSPs’ direct channels, whilst not disproportionately hampering PISP payments from being able to develop further, and to support PSR’s other policy objective of greater competition for retail transactions from account-to-account payments.

This would include mandating PISPs to share the necessary data with ASPSPs so they can effectively detect and prevent a scam, updating the Customer Experience Guidelines to allow ASPSPs to put in place effective and timely scam warnings into the customer payment journey, where appropriate, and incentivising PISPs to put in place necessary fraud prevention, by sharing the ‘Sending PSP’ liability for reimbursement in a defined set of circumstances where this would be appropriate, as in effect both the PISP and the ASPSP share the role of ‘Sending PSP’. All participants in the Open Banking payment chain needs to be appropriately incentivised and accountable to detect and prevent fraud and scams, and therefore the model needs to be set up appropriately to ensure this is the case.

Finally, we encourage the PSR to drive a consistency in approach to data sharing across firms for all fraud cases, including those which fall outside the scope of the reimbursement model. For example, where a corporate firm is the victim of a scam, whilst there is no basis for the recipient PSP to support reimbursement, there will be benefit in notifying the recipient PSP for investigation and potential closure of the mule account.

#### **Question 4: Do you have comments on our proposals:**

- **that there should be a consumer caution exception to mandatory reimbursement**

UK Finance and its members support the proposal that there should be a consumer caution exception to mandatory reimbursement. We strongly believe that consumer caution plays a vital role in countering fraud risk. This stance has been echoed by the PSR in its previous consultation, in November 2021, the PSR stated that “we agree that consumers need to exercise caution.” It is disappointing therefore to see the PSR propose such a low level for consumer caution in the form of gross negligence.

The PSR acknowledges that there is a potential risk that consumers will take less care if they are more confident of receiving reimbursement. We urge the PSR to explore the level of consumer caution required to sufficiently counteract this risk. PSPs will need to be able to operationalise case decision processes around liability and caution, so anything created should be clear, fair, and supported by well-defined guidance to enable consistency in interpretation across PSPs.

- to use gross negligence as the consumer caution exception

No clear definition of gross negligence has ever been found that is suitable to be applied to fraud cases, especially those linked to digital or modern payment systems. However, the general understanding and use of the term is in situations where severe and reckless disregard has been taken in response to a clear risk. It is of our opinion that this sets the bar too high and rather than the PSR's proposals driving a reduction in APP scams, they may instead create moral hazard, enabling consumers to take risks which would previously have been out of character, and hence could lead to the opposite outcome to that which PSR intends – i.e., an increase in APP scam volumes.

We recognise that the PSR has chosen this term to intentionally create a model which will see most victims of APP scams reimbursed, but we cannot accept an approach where consumers are not required to take some responsibility, through exerting a level of caution, when making payments.

Instead, we suggest that the consumers behaviour must form part of the assessment when reviewing the claim. The general principle behind any mitigation of moral hazard is to provide incentives to the consumer that align with the appropriate effort in reducing fraud: to give benefits to the consumer when effort is exerted, and to raise costs to the consumer when effort is not exerted<sup>3</sup>.

Following this theory our recommendation is that, unlike the complex model which exists within the Contingent Reimbursement Model Code, based around the consumers reasonable basis for belief, which lacks specificity and is open to interpretation, the consumer negligence determination be based on simple principles which are easily communicated to consumers, and which can evolve over time. These may be as modest as, did the consumer conduct any basic checks prior to making the payment, did they proceed despite a Confirmation of Payee mismatch, did they ignore a directly relevant warning or recommendation from the PSP or did they provide misleading information when questioned at the point of making the payment.

Where there is the presence of sufficiently sophisticated social engineering or vulnerability, it may not be reasonable to expect the consumer to have recognised the risk and protected themselves. In these circumstances the consumer should be reimbursed.

Recognising that no scam type is the same, case studies must be used within both communications with consumers and within the industry guidance that supports the reimbursement model.

The inclusion of a basic contributory negligence model will reduce the risk of moral hazard whilst still achieving the PSR's objective of incentivising firms to continue to develop innovative fraud prevention tools and to increase the level of consumer reimbursement. A more balanced liability framework, recognising consumer contributory negligence will also positively influence the level of friction introduced across FPS payments.

- not to provide additional guidance on gross negligence

Whether it be gross negligence or consumer contributory negligence, if this is the key factor to be assessed as part of the operational process to work an APP Claim, a definition must be provided. The definition must be supported by guidance, illustrated by case studies, for each specific scam type. We would suggest that the indicators of negligence would also vary dependent of payment value and customer type, therefore this should also be addressed within the guidance.

---

<sup>3</sup> [Winter, *Optimal insurance under moral hazard*, Handbook of Insurance]

Without precise guidance, for each specific scam type, there will be disparity in interpretation across PSPs which ultimately, with receiving PSP liability based on the sending PSP victim assessment, may result in disputes between firms.

Furthermore, public confidence in the Contingent Reimbursement Model Code diminished rapidly as FOS decisions set customer liability expectations far removed from those of PSPs. The PSR must learn from this previous mistake and provide clear and detailed guidance or risk creating a model which will quickly lack consumer confidence.

UK Finance and its members would be happy to support the PSR in the development of any guidance associated with the final reimbursement model.

**Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?**

We support this approach, contingent on recognition within the agreed vulnerability definition that in the context of an APP scam, evidence of a vulnerable situation, in isolation, may not necessarily increase the likelihood of, or result in the customer falling victim to an APP scam. For example, the fact that a customer is suffering with a physical health condition, may not make the customer vulnerable to an APP scam. However, where there is evidence to suggest that the nature and extent of the customer's vulnerability is such that it would not have been reasonable for the customer to have protected themselves from falling victim to a scam, PSPs should be required to reimburse.

PSPs will still conduct a full investigation, even where vulnerability is identified early in the claim process, as this provides the PSP the opportunity to support and educate their vulnerable customer, to try to prevent them from becoming a repeat victim.

**Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?**

The FCA definition of a vulnerable customer lacks the specificity required in the sphere of APP scams. The definition assumes that vulnerability makes the consumer especially susceptible to harm. However, vulnerability can be a fluctuating state, and the impact may vary in degrees of permanence and presentation. Factors such as life events, physical health, cognitive conditions including, mental health, literacy and numeracy and caring responsibilities can put anyone in a vulnerable situation.

As outlined in our response to question 5, in the context of an APP scam, evidence of a vulnerable situation may not necessarily increase the likelihood of or result in the customer falling victim to an APP scam, equally a consumer may in normal circumstances not be deemed as vulnerable, but the timing and nature of the scam makes them vulnerable. We therefore recommend continuing with the existing definition of vulnerability as outlined within the CRM Code.

**Question 7: Do you have comments on our proposals that:**

- sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- any 'excess' should be set at no more than £35
- PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

We recognise the PSR's intention in suggesting this 'excess' to reimbursement but a significant proportion of our members strongly believe this proposal should be removed from the final reimbursement model.

The ability for PSPs to set their own excess of up to but no more than £35 would create a confusing landscape for consumers who may hold accounts with multiple PSPs across which the thresholds differ. Furthermore, this would create operational complexities with the receiving PSP having no alternative but to accept the excess value set by the sending PSP, which may differ from their own accepted level. Both points apply equally to question 8 and 9.

We have already articulated within this response our belief that consumers take greater care when a payment is of a higher value. We believe that setting such a low excess will not incentivise consumers, who believe that they are making a genuine transaction or where a consumer is tempted by potential 'too good to be true' products or investments, to take greater caution. Instead, we refer to our previous points around consumer contributory negligence as we believe that this is the only option which will reduce the impact of moral hazard.

Furthermore, the PSR should note the learnings from the existence of excess values within other payment models. As outlined by the PSR, section 77 of the PSRs 2017 allows PSPs to require that a payer is liable up to £35 for losses incurred in respect of unauthorised transactions. This excess is only used in exceptionally rare circumstances, with most firms citing it as uneconomical to do so both from an operational impact perspective but also due to the level of customer complaints this generated on its introduction.

One member has proposed that an alternative for consideration may be the introduction of a percentage excess, i.e., a percentage of the total scam claim. Noting that as the value of the potential fraud gets larger, the relative value of the proposed £35 excess becomes increasingly small – meaning that only limited risk is transferred to the consumer and moral hazard is less effectively mitigated, a percentage of the total scam may therefore maintain consumer awareness.

#### **Question 8. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a minimum claim threshold**
- **any threshold should be set at no more than £100**
- **PSPs should be able to exempt vulnerable consumers from any threshold they set?**

There are mixed views amongst our membership on whether a minimum threshold should be part of the proposed mandatory reimbursement model, or not.

Some PSPs have suggested that the £100 threshold risks deterring customers from reporting scams, meaning the Receiving PSP will not be notified of a potential mule account that may be being used for other scams, or be used subsequently for a further higher value scam. Furthermore, ensuring the customer reports the scam means that the PSP can identify any underlying vulnerability and take the appropriate steps to limit further victimisation.

Other PSPs regard the minimum threshold as a crucial element to driving consumer caution, particularly in relation to lower value purchase scams, noting that mule accounts usually build credibility with legitimate activity on an account rather than low value scams. They also regard the minimum threshold as crucial to support the operation of claims and maintain focus on those claims that will be more material in impact.



Clearly, if the PSR dismiss the inclusion of a consumer contributory negligence exemption, a minimum claim threshold will be key to ensure that consumers continue to take care when making payments. We would suggest that £100 may not be significant enough a sum to disincentivise buyer seller disputes and promote 'buyer beware' for purchase scams. The level at which the threshold would be set therefore requires further thought and economic analysis.

Due in part to the varying business models of the PSPs who submitted data, there is significant variation in the kind of APP scams cases they see within these value bands. High-street PSPs are more likely to have higher volumes of low-value scams reported to them, whereas other PSPs see a much lower volume of these types of frauds. We will continue to collate this data from our remaining members outside of the consultation period. Updated figures will be supplied to the PSR when available.

If a minimum threshold is designed into the reimbursement model, it must be consistent across all PSPs, providing a clear, easily communicated model for consumers. Industry agrees that vulnerable consumers, where the vulnerability may have impacted their ability to protect themselves from the specific scam, must be exempt from any threshold set.

#### **Question 9. Do you have comments on our proposal not to have a maximum threshold?**

We strongly disagree with the PSR's proposal to not have a maximum threshold. The PSR state that the rationale for proposing no maximum threshold on claims is that "PSPs should have the strongest safeguards in place for the largest payments" and that, "in practice, most PSPs' Faster Payments transaction limits are very well below £1 million.". When outlining the PSR's proposal for the minimum threshold, the PSR make clear that the minimum threshold "would apply only if an APP scam had a total value (including all payments made as part of the scam) greater than the level of the minimum threshold". We would thus expect the PSR to consider the upper threshold in the same way and recognise that scam cases regularly consist of multiple payments, often executed over an extended period. It is not unusual to see scams which start as small regular payments between accounts, establishing what appears to be a known, trusted beneficiary relationship, which over time increase in value so that when the scam is identified significant sums have been paid away.

The lack of an upper threshold will bring unlimited risk for PSPs and may see smaller PSPs, who will be less able to manage this risk, responding by lowering transaction limits on specific payments.

We would also highlight the existence of a compensation limit for cases raised through the FOS and upper thresholds across other consumer protection schemes. We cannot emphasise enough the importance of an upper threshold as a control for maintaining consumer caution. A maximum threshold may incentivise the consumer to reduce the payment size that is put at risk of fraud. Whilst for larger transactions, the maximum threshold would transfer risk back to the consumer, in term incentivising the consumer to exert a level of effort to protect their funds.

However, customers with higher value claims should not be disadvantaged by this limit, therefore we propose that to evaluate the more complex, high-value cases there should be an extraordinary process which should be developed through industry working groups to ensure consistency for consumers.

#### **Question 10. Do you have comments on our proposals that:**

- **sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement**
- **any time-limit should be set at no less than 13 months?**

We agree with the need to set a time-limit for claims but emphasise again the importance of setting an industry wide time-limit. Allowing firms to set their own will result in inconsistent messaging and confusion for consumers. This will also create operational complexities with receiving firms responding to claims across differing timelines.

We agree that 13 months is an acceptable time limit. Having analysed industry data, the number of claims raised outside of this timeline are minimal. Where claims are raised outside of the industry time-limit firms should have the flexibility to choose to take the claim forward where there is indication of vulnerability or the decision not to investigate may have a detrimental effect on the consumer. In these cases, sending PSPs should notify the receiving PSP to enable full investigation of the claim and assessment of the receiving account, however any reimbursement will be funded as a gesture of goodwill by the sending PSP.

**Question 11. Do you have comments on our proposals that:**

- **the sending PSP is responsible for reimbursing the consumer**
- **reimbursement should be as soon as possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?**

We agree that, as the sending firm holds the relationship with the customer, it is a better customer experience for all engagement, including reimbursement to occur via the sending PSP. This process already exists across CRM Firms and works well.

UK Finance and its members, however, cannot support the proposal that reimbursement should be as soon as possible, and no later than 48 hours after a claim is made. We agree that where it is in the consumers benefit to do so, reimbursement should be made within the shortest timeframe possible.

We recognise that the PSR's intention in suggesting this timeline may have been to achieve consistency for consumer claims across fraud types, bringing authorised push payment fraud reimbursement in line with unauthorised fraud, but the fraud types are fundamentally different. For unauthorised transactions, sending PSPs can, generally, quickly determine if the transaction in question was made by their customer or an unnamed third party. In the case of authorised push payments scams, the investigation is far more complex. The underlying question being if the intent of the recipient account holder was to deliberately deceive.

The initial hurdle to overcome in the investigation is obtaining the relevant information from the victim. This is an emotionally stressful time for consumers, and it is often the case that they will not remember the full facts of the scam on their first engagement with the PSP. Complying with a 48hr window may therefore create additional emotional distress, not lead to the right outcome for consumers and will be a poor customer experience. PSPs may also experience challenges engaging either the sending or receiving account holder, the PSR have not clarified if, where firms are waiting for customer evidence, the clock will stop?

Once the information has been obtained, sending PSPs must engage with the receiving PSP to clarify the validity of the consumers claim. If the recipient PSP is not available 24 / 7, where the case



is more complex, or the recipient account demonstrates no risk indicators the investigation may take an extended time frame to complete.

From a consumer perspective, setting unrealistic expectations will create additional emotional distress. This will also create additional operational overheads as PSPs are required to engage with consumers more frequently to update of the status of the claim and any reason for delay past the initial 48hours. We worry that in circumstances where the criminal is still in contact with the victim such rapid reimbursement may not always be in the victim's best interest.

We have concerns that, if the timeline for investigation was shortened so significantly, incorrect decisions could be made regarding the recipient account resulting in funds being frozen and consumer accounts being exited incorrectly for mule activity. This will generate an increase in complaints and will be emotionally stressful for consumers incorrectly labelled as a money mule.

The PSR's proposal does not clarify whether the 48 hours includes bank holidays and weekends, or how the timeline would work in the scenario that one or both PSPs do not operate a 24 /7 service. There is the risk that PSPs may see a spike in claims, both genuine and potentially fraudulent, outside of 9 – 5 hours, when specialist fraud professionals are less able to be available to make informed decisions.

Recognising the challenges faced by firms in assessing APP scams, and the unintended consequences for consumers if the timeline were to be reduced, we would recommend maintaining the existing 15 / 35 day timeline of the CRM Code, for a period following implementation. If the new reimbursement model can resolve several of the current operational challenges, through delivery of a clear definition on scope and simplified consumer contributory negligence, the current timelines may in the long term be shortened. But we must be mindful of the significant increase in number of PSPs who will be engaging in this reimbursement approach who are not CRM participants and therefore have no experience in operating within an APP liability framework. It would be reckless to shorten existing timelines at a time when the number of cases being shared for reimbursement will increase significantly.

It is important to highlight the need for exceptions to be built into the reimbursement timeline. Complex cases, which may be subject to law enforcement and or FCA investigation, which involve the layered and cycled movement of funds across multiple firms, including unregulated entities cannot be resolved within a set timeframe. There must also be exceptions for occasions where the consumer has not provided sufficient evidence to the PSP to enable the investigation to move forward.

Finally, we must raise the risk that the speed of reimbursement may lead to an increase in first party fraud claims. In the space of APP scams such claims are difficult to determine, we may therefore see criminals profiting from the reimbursement model.

**Question 12. What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Gross negligence is used as an exemption from reimbursement for unauthorised fraud, with a 48 hour PSP time frame. In an unauthorised transaction, gross negligence is typically linked to the customer having been careless with their security credentials, an action which is possible for a PSP to identify and evidence. However, under a 'gross negligence' test for an APP scam, a PSP would need to show that the customer recognised the risk and disregarded it. This is very difficult for a PSP to evidence, even if it suspects this to be the case. Likewise, the PSP will need a period – and cooperation from the customer – to ask questions and collate evidence to determine any indication

of gross negligence. Often it is the absence of evidence that can indicate risk. Lack of cooperation on the part of the customer may be seen as a red flag that warrants further investigation, but this may not be enough to determine gross negligence or first party fraud.

As outlined in our response to the previous question, UK Finance and its members cannot support a 48 hour timeline for reimbursement. We have articulated why, even with a streamlined assessment process, an average APP claim investigation will take more than 48hours. We have also articulated our reasons for why the current CRM timeline should be maintained, for the short term at least.

There must also be adequate time built into the model to enable relevant evidence to be collected from the Receiving PSP. SLAs would need to be included to ensure receiving PSPs provide the evidence in sufficient time.

Finally, any standards of evidence needed will need to be adapted per scam type and customer type – given nuances across each of these.

### **Question 13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?**

UK Finance strongly believe that an equal balance of responsibility between sending and receiving PSP for victim reimbursement, will drive improved behaviours and investment in appropriate detection tools across receiving PSPs. We strongly support this element of the PSR's proposals.

At its inception the CRM Code was, in principle, designed to distribute potential liability equally across both sending and receiving PSP and consumer. In practice the requirements on PSPs were weighted far more towards sending PSP liability, with receiving PSPs on average accepting liability in only 2% of claims.

UK Finance and its members are therefore supportive of the 50:50 default allocation of reimbursement costs between sending and receiving firms as a foundation for the reimbursement model.

One alternative to this approach would be to include PISPs within the liability model. As outlined earlier in this response, payments through Open Banking involve multiple players within one payment journey with the PISP and ASPSP effectively sharing the role of sending PSP. To incentivize PISPs to ensure that they have in place necessary fraud prevention tools, an alternative model may place a percentage of liability on the PISP in a defined set of circumstances where this would be appropriate. The correct level of PISP liability percentage would need to be developed through industry engagement. UK Finance would be happy to support these discussions.

Alongside the reimbursement model, as outlined previously within this response, it will be essential that the PSR provide clear definition on scope and a simplified consumer contributory negligence model. This will ensure a clear understanding across PSPs of where claims are in scope, enable sending PSPs to efficiently direct the consumers claim, and allow receiving PSPs to have greater trust in the sending PSPs assessment of the claim.

The PSR must mandate strict timelines for the reimbursement of receiving PSP liability funds to the sending PSP. It should not be an acceptable position for sending PSPs to have the additional burden of chasing for the reimbursement of funds.

**Question 14. Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?**

Most UK Finance members do not support this proposal and instead advocate the development of a fair and balanced mandatory reimbursement model.

Members recognise the PSR's intentions when making this proposal but have concerns that this would be a costly exercise both in terms of central administration of the scheme and operational burden across PSPs. There is the risk that, if not developed alongside a strict set of criteria this process would result in a backlog of claims with PSP resource allocated to claim evidence rather than more meaningful prevention roles.

Members also have concerns that this may erode the collaborative relationship which exists across the UK fraud prevention community.

If PSPs do wish to dispute their liability allocation, members propose that, as is the current standard within the CRM Code, PSPs can choose to engage the services of an external Dispute Resolution company.

One member does however suggest that as a minimum, there should be analysis of the outcomes in the early months of the new reimbursement model to gauge whether 50:50 is more or less optimal or whether there are fundamental issues that might support the case for a dispute process and associated 'allocation criteria'.

**Question 15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?**

UK Finance and its members are clear that we do not support the inclusion of multi-generation scams within the scope of this reimbursement model. We outline in detail in our response to question 3 our view that the rules should be positioned directly around the premise of 'a payment to a bank account controlled by the fraudster', limiting the rules specifically to one generation payment, i.e., the singular payment which places the scam funds into the control of the criminal.

Consideration has been given to various models which may allow the operationalisation of a multi-generation liability model, however within the current legislative framework there is neither the ability to share the necessary data concerning multiple victims and beneficiaries across PSPs for end to end analysis of the case nor is there a framework for repatriation of funds across multiple payment generations where funds are frozen in an account further along that the first generation beneficiary.

**Question 16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?**

Generally, industry agree that allocation of repatriated funds should mirror the default allocation for reimbursement.

However, an alternative option has been raised by one of our members. The PSP suggests that receiving PSPs should retain the full value of any repatriated funds, up to the value of the PSPs 50% liability share. Where more than 50% of the scam value is recovered, the excess should then be returned to the sending PSP. The member believes that this alternative approach will incentivise receiving PSPs to amplify investment in inbound profiling tools and dedicate resources to develop alerts, therefore achieving the PSR's objective of reducing the value of fraudulent funds being paid to criminal gangs. The member makes the case that, where repatriation of funds takes place, within the current regulatory framework, receiving PSPs are operating at risk.

To be clear, this is the proposal of one member PSP. The thoughts of the UK Finance wider membership, in response to this proposal have not been collated. As such, industry engagement would be required following closure of the consultation period, if the PSR chose to investigate this suggestion further.

Where a consumer has not been found to be eligible for reimbursement, any repatriated funds should be returned in full to the consumer.

#### **Question 17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?**

We fully support the proposal that the rules on allocation of costs of mandatory reimbursement should apply to all directly connected PSP participants sending and receiving payments over Faster Payments as well as PSPs indirectly sending and receiving payments.

It is essential that the PSR establish clear mechanisms to ensure that all participants within the payment landscape are incentivised to develop effective fraud controls, inclusive of PISPs and unregulated firms such as crypto exchange firms.

If these firms are excluded from the reimbursement model, the risk to PSPs of payments being made across Open Banking and to unregulated firms will be elevated. Firms will take a much firmer risk approach which will impact the growth of Open Banking as well as the development and adoption of account-to-account retail transactions, restricting the opportunity for innovation in this market. Consumers making payments to crypto exchange firms will encounter significant challenge. We are already seeing PSPs introducing strict controls in this space, including daily payment limits and full blocks on payments to individual firms, these controls will continue and potentially escalate if unregulated firms are not brought into the reimbursement model.

It is essential, when operationalising the reimbursement model that it is done so unilaterally across all PSPs, and not via a phased approach.

#### **Question 18. Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?**

The PSR state 'it is the PSO that has the operational oversight, the expertise on system rules and what works in practice, and the ability to coordinate across participants, which are needed. Scheme rules can be managed and refined more efficiently and quickly than regulatory instruments.'

Whilst we agree that Pay.UK have a significant role to play in the management of fraud risk across the FPS scheme, we do not believe that they are the appropriate body to fulfil the role as set out by the PSR.

UK Finance and a significant proportion of its members instead propose that the PSR place Directions on all FPS participating PSPs to adhere to the mandatory reimbursement rule. This would allow for a consistent and clear reimbursement framework to be applied across the industry, to all participants, mitigating the many challenges the PSR has noted which would exist if they were to require Pay.UK to implement. Our view is that a direction is the more appropriate vehicle, allowing for the reimbursement framework to be implemented within an expedited timeframe. We would suggest that scheme rules be used in parallel to set minimum standards for participation to the scheme. These may then evolve over time with the changing fraud landscape and the introduction of new prevention measures. Scheme rules may include but not be limited to onboarding requirements, the provision of effective warnings, data sharing and performance reporting to name a few. The provisions within the rules must be high level enough to cover all business models with more specific detail, for individual business models and fraud types within separate guidance.

In the long term, and as stated in UK Finance's previous consultation responses on APP scams, we strongly believe the reimbursement framework for authorised fraud must be placed on the same legislative footing as unauthorised within the PSRs 2017. This will help to mitigate the risk, highlighted earlier in this response, of the authorised fraud threat migrating to other payments schemes where no appropriate minimum standards are already in place, whilst providing consistency for consumers. Whilst directions are in place, UK Finance and its members would propose to work with HMT and regulators to agree changes to PSRs 2017 to include a specific and detailed definition of an authorised payment scam, clarity regarding scope and the obligations and liability framework. Alongside the liability framework, it will be necessary to make clear in legislation who has responsibility for the monitoring and enforcement aspects of the reimbursement framework, we strongly believe that these roles should fall to the regulator, leveraging enforcement capability already available to them.

The Financial Service and Markets Bill provides a significant opportunity to move forward, in ways that were not possible without the prospect of legislative change. The Bill as drafted states that "the Payment Systems Regulator must prepare and publish a draft of a relevant requirement for reimbursement in such qualifying cases of payment order as the Regulator considers should be eligible for reimbursement. The Payment Systems Regulator must impose a relevant requirement, in whatever way and to whatever extent it considers appropriate, for reimbursement to be made in qualifying cases of payment orders." A 'relevant requirement' means a requirement imposed by or under section 54 or 55 of the Financial Services (Banking Reform) Act 2013 (or by or under a combination of those sections). Section 54 relates to Directions, and Section 55 relates to System Rules.

The PSR's proposal currently chooses implementation via System Rules, which presents several significant challenges:

- Pay.UK do not have the necessary powers to enact a scheme change without significant support from their participants, as well as the regulator – if mandatory reimbursement is to be brought in quickly, it will require detailed Directions from the regulator on PSPs and Pay.UK unless the proposals have widespread support.
- Legal limitations will make it difficult for Pay.UK to implement changes designed to manage and mitigate operational risks which occur at the payment service provider or consumer level. This points to a need for PSR to define the reimbursement framework, not Pay.UK
- We question, as outlined within the PSR consultation, the powers, and options available to Pay.UK to ensure compliance with the suggested scheme rules. Existing enforcement, to delist a Direct Participant from FPS, does not seem appropriate for this issue.
- Also, as the PSR notes, whilst Pay.UK has very limited rulemaking and enforcement powers over the direct participants' relationship with consumers, it has none over the indirect participants. This would require a workaround that would carry significant complexity across industry. The PSR outline that the preferred approach would be to apply rules to indirect participants, by applying rules to all payments. However, this would likely mean:

- If the indirect participant did not meet the requirements of the FPS Rules, it is the direct participant (the IAP) which would be in breach, not the indirect participant, despite the lack of fault by the direct participant.
- Potentially the direct participant (the IAP) could have to cover the 50:50 split and recover this from the indirect participant, which would create significant credit risk in the process.
- The consequence of this would be significant for a direct participant IAP. It would create barriers to direct participants providing services to indirect participants and may lead to existing indirect access providers withdrawing from the market or further limiting their risk appetite in a market which does not have a surfeit of indirect access providers.
- Pay.UK cannot impose rules on direct or indirect participants to ensure the regulated entity who own the client relationship with unregulated firms be mandated to pass any losses onto that client, should they be found to exist – i.e., levy a charge against that client.

It is unclear to us why the PSR has chosen the route of implementing the mandatory reimbursement model via System Rules. We urge the PSR to reconsider and to instead implement via Directions, followed by long term legislative change. This methodology would overcome a significant number of the issues which would be a by-product of the PSR's proposed approach. This would eliminate the need for a short and long term approach, which is operationally inefficient for PSPs. Ultimately this will also enable Pay.UK to focus on delivering the NPA programme and working with UK Finance to deliver the Enhanced Fraud Data initiative which has the potential to significantly reduce the APP threat across the UK.

**Question 19. Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?**

The PSR sets out that as a minimum they expect Pay.UK to implement into Faster Payment Scheme rules the following:

- when a consumer must be reimbursed by its sending PSP
- a default 50:50 allocation of reimbursement costs (and of any repatriated funds) between the sending and receiving PSP, and any arrangements needed to enable sending and receiving PSPs to transfer funds between them
- designated arrangements to enable PSPs to choose to depart from default allocation by negotiation, mediation or dispute resolution based on more tailored allocation criteria (implementation of this is discussed further in the next section)

We have clearly articulated throughout this response that we do not support the delivery of these industry requirements via FPS rules and instead advocate the use of directions on all PSPs, followed by long term legislative change, supported by FPS scheme rules.

We propose the development of a basic consumer contributory negligence model, based on simple principles, and supported by a clear definition of an APP scam to determine scope. Both the contributory negligence model and the definition of an APP scam should be locked into legislation.

We support 50:50 reimbursement as a starting position but suggest further thought regarding the potential inclusion of PISPs where they are present in the creation of the payment.

The Best Practice Standards (BPS) platform, developed and overseen by UK Finance, is well positioned to act as the mechanism for PSPs to share information, in real-time, from the point of the



PSP becoming aware of the scam, through to repatriation and the allocation of funds across firms. The BPS platform already has participation of PSPs which hold approximately 90% of UK retail payment accounts. Whilst we acknowledge that the system will need some enhancements, this will be significantly faster to deliver and more cost effective, both for Pay.UK and BPS participating firms, than the PSR requiring Pay.UK to develop a new system for this purpose.

#### **Question 20. Do you have views on how we should exercise our powers under FSBRA to implement our requirements?**

As outlined, we strongly believe that the only effective method to implement a mandatory reimbursement model in the short run, is through PSR directions on all FPS participating PSPs, including PISPs. This should be inclusive of a rule which brings unregulated firms who are the recipient of first generation scam funds into scope for reimbursement. We have outlined our desire to see the PSR consider a rule which ensures the regulated entity who own the client relationship be mandated to pass any losses onto that client, should they be found to exist – i.e., levy a charge against that client equal to their loss, minus any repatriation. In the long run we wish to work with HMT and regulators to agree changes to PSRs 2017. This will mitigate the risk, highlighted earlier in this response, of the fraud threat migrating to other payments schemes.

We also propose that, separate to the reimbursement framework, the PSR use their powers under FSBRA to direct all payment schemes, to develop minimum standards, where appropriate and where they are not already present, for participation to the payment scheme. These would evolve over time with the changing fraud landscape and the introduction of new prevention initiatives. These may include but not be limited to, the provision of effective warnings, data sharing and performance reporting to name a few. The provisions within the rules must be high level enough to cover all business models with more specific detail, for individual business models and fraud types within separate guidance.

The direction must cover all payment schemes, where appropriate and where no such standards currently exist. This will ensure consistency in outcome for victims of authorised scams, irrelevant of payment method, and limit the migration of scam risk to other schemes who may not yet be fully prepared to respond to the increased threat.

#### **Question 21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?**

UK Finance has a proven track record in supporting industry in the development and implementation of industry policy. The development of an allocation criteria within a mandatory reimbursement model is a complex and potentially provocative issue. The various options will require careful consideration including analysis of the costs and benefit both to industry and consumers.

UK Finance are well placed to work with our members in supporting the PSR and the payment schemes with the development of a suitable allocation criteria which supports the PSR's objectives of increasing consumer reimbursement, incentivising all industry participants to continue to invest in APP scam prevention tools and consumer education whilst also maintaining consumer awareness when making payments.

We have already outlined proposals within this response centred around the inclusion of PISPs within the reimbursement model and the development of a simple consumer contributory negligence assessment. We would be keen to support the PSR and industry in considering these, and any other options, in more detail.

We do not support the proposal that a dispute resolution process be developed and instead advocate that time be invested in the development of a fair and balanced mandatory reimbursement model. On the rare occasion that firms may want to dispute the allocation of a claim, they may choose to do so through the appointment of an independent dispute resolution firm.

**22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?**

**23. Do you have views on the costs and benefits of Pay.UK implementing a real time compliance monitoring system and when it could be introduced?**

UK Finance and its members consider The Best Practice Standards (BPS) platform well positioned to act as the mechanism for PSPs to share information, in real-time, from the point of the PSP becoming aware of the scam, through to repatriation and the allocation of funds across PSPs. The BPS platform already has participation of PSPs which hold approximately 90% of UK retail payment accounts.

UK Finance and its members have invested heavily, both through allocation of time and funds, in the development and implementation of the BPS platform. Participating PSPs have developed advanced technology within their own business, both in the capacity of sending and receiving PSP, to enable real-time or near to real-time interaction with the platform to expedite the sharing of data to capitalize on the potential to freeze funds remaining with the beneficiary account.

There are no barriers to non-UK Finance members accessing and utilising the platform.

Further development will be required to bring the platform functionality in line with the ultimate PSR vision, however, we would reason that development of a platform already approved for use by a significant number of PSP information security and data privacy officers will be simpler, more cost effective and timely to implement than the alternative of requiring Pay.UK to design and implement a new compliance monitoring regime.

The existing BPS platform can be further enhanced to deliver additional benefits:

- real time availability of compliance management information – the system already contains a comprehensive set of management information reports. These could be developed further to enable both PSPs and the body overseeing compliance to access reports specific to their role.
- real time accountancy functionality – the current standard across PSPs is to finalise and submit the allocation of funds between PSPs on a case by case basis. There are currently only 10 PSPs voluntarily participating in the CRM Code and a total of 35 using the BPS platform. With the number of PSPs participating in a mandatory reimbursement model set to increase exponentially, the ability to continue to reconcile on a case by case basis will become untenable. To limit the operational impact on PSP and to ensure that funds are submitted to sending PSPs within agreed SLAs we would suggest the development of accountancy functionality to provide a balance of funds to be returned to individual PSPs at an agreed frequency. Reports would highlight any occurrences of SLAs not being met.

The PSR's vision for development of a short-term compliance regime centred around the requirement for PSPs to report regularly to Pay.UK is neither proportionate nor effective. The PSR have not outlined the specifics of the reporting they propose but we would anticipate the level of detail required, and the ability to report only on the payments within scope, will require development of new functionality which will be both a costly and time-consuming process. To introduce this as a



short term requirement is not proportionate and we would argue that submission of this data to Pay.UK, who have no enforcement capability would be a futile exercise.

If the PSR introduce a short term compliance monitoring regime, we would reason that any such reports should be submitted directly to the PSR. We would however seek clarity from the PSR as to how they would use this data in engaging with and incentivising the worst performing PSPs to improve.

#### **Question 24. Do you have views on the best option for short-term enforcement arrangements?**

The fraud landscape as it stands is a disparate model of administration, compliance, and enforcement across a wide range of bodies. These include the Lending Standards Board (LSB), PSR, FCA and the various payment scheme operators. In our previous consultation response, we encouraged the PSR to take a more holistic view and to consider legislation which would be applicable to all PSPs and which, importantly, would be enforced by one central body.

Our view in this regard has not altered. We continue to believe that fundamental to the industry's ability to succeed in tackling authorised payment fraud is the establishment of one central body to ensure consistency in response to the authorised payment fraud risk across PSPs and payment schemes.

The PSR state that 'If the PSR were to initially implement the reimbursement requirements on PSPs through a direction, with Pay.UK operationalising those requirements, enforcement of those requirements would also fall to PSR. We would use our usual enforcement processes and principles in deciding when to act, and what action to take.' The PSR note that this is not their preferred option. We would argue that this should be the only option for enforcement of this process which will ensure consistency across all PSPs

#### **Question 25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?**

#### **Question 26. If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?**

Both questions have been answered in full within our response to question 18.

#### **Question 27. Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?**

We agree with the PSR's assessment that the level of reimbursement will increase, creating additional cost for PSPs and benefit for victims of scams. However, we have fundamental concerns with the PSR's assessment of the wider costs and benefits of the proposed approach to mandatory reimbursement and would suggest that further, evidence based analysis is required.

The PSR briefly touch on the risk of moral hazard, listing the risk of this occurring as low. However, economic theory indicates that moral hazard is highest when consumers are fully reimbursed against fraud. The more risk that is transferred to consumers, the more effort they will make to reduce the likelihood of fraud. Unless it is effectively mitigated, moral hazard will therefore increase the level of fraud, which increases PSP' costs. As outlined within this response, we would expect this to be at least partially passed-through to consumers in the form of higher prices, increased friction in payments and reductions in competition and innovation. This is potentially most clearly evidenced in

the health and motor insurance market where numerous large scale experiments have been conducted to test the theory.

The Seguro Popular Experiment in Mexico<sup>4</sup> (2004) provides the most direct evidence on consumers reducing risk-mitigating effort because of obtaining insurance coverage. The author, using data from the Seguro Popular Experiment, which randomly assigned the participants with a catastrophic health insurance, finds evidence that insured individuals had a lower demand for self-protection in the form of preventative care, e.g., reduced take-up of flu shots and mammograms, in response to greater insurance coverage. This indicates the presence of moral hazard, as consumers that were insured appeared to take less care in preventing an adverse outcome.

As previously suggested within this response, we respectfully request that the PSR conduct a more complete economic assessment, potentially including quantitative analysis of similar reimbursement schemes, and the experience of the health and motor insurance markets, before moving forward with a reimbursement framework, if it is to be based on a gross negligence exception alone.

The PSR suggest that greater investment by PSPs in prevention tools will fundamentally reduce the volume of APP scams, but make no reference to the platforms, internet service providers and telecommunications sectors, who bring risk into the system. Without greater collaboration and investment by them, consumers will still face the embarrassment and emotional impact of social engineering.

The PSR propose that their policy will lead to PSPs more effectively pursuing funds that are lost, possibly following the trail of funds through multiple accounts and PSPs, then recovering these to reduce PSPs own cost in reimbursing victims. This statement does not acknowledge the lack of a clear legislative framework to enable PSPs to freeze and repatriate funds to victims of fraud. The current framework which supports PSP repatriation for APP scams is governed by an industry developed voluntary APP Best Practice Standards (BPS) which only covers first generation payments. The PSRs 2017 does not expressly provide a means for Firm A to repatriate funds to Firm B to reimburse a victim. BPS participating firms have been proceeding at legal risk in doing so and the status quo enables considerable inconsistency in approach and outcome. To enable an increase in funds repatriation, the government must first implement a statutory framework to prescribe minimum standards and processes to govern investigation, response, and repatriation of funds to victims and make changes to the PSRs 2017 to enable PSPs to hold payments where they identify a level of suspicion.

More widely, the cost benefit analysis makes no reference to significant market risks including the potential impact on competition and innovation and ultimately consumer choice outlined in detail within this response, and whilst the PSR note the potential migration of fraud risk to other payment methods and prudential implications for some PSPs, they have not sought to quantify the potential costs.

### **Question 28. Do you have any other comments on the proposals in this consultation?**

We have fundamental concerns that the timelines proposed for implementation of a mandatory reimbursement model to span all PSPs are unrealistic.

The development of a mandatory reimbursement model is a complex and potentially provocative issue. Detailed cost / benefit analysis will need to be conducted to ensure that any significant costs

---

<sup>4</sup> Spenkuch, 2012, Journal of Health Economics ([Link](#))

either to industry or consumers are recognised and are acceptable relative to the benefits the reimbursement model will deliver.

It cannot be underestimated how long it will take to develop detailed guidance to support the liability framework and definition of an authorised scam. And then subsequently for PSPs, a significant proportion of which will have no prior knowledge of operationalising a liability framework, to implement processes and procedures across the firm.

The availability of a secure mechanism to enable the exchange of claim data, to allocate reimbursement and to facilitate large scale reconciliation of accounts will be essential to the success of the reimbursement model. We have outlined our proposal that the BPS platform may be best placed to support this data exchange. However, development of the necessary enhancements cannot be scoped until the PSR finalise in full the scope and reimbursement framework. Furthermore, we cannot emphasise enough the significant undertaking it will be to onboard all remaining direct and indirect FPS participants. Providing PSP access to the platform requires acceptance of the UK Finance data sharing agreements and often involves detailed information security assessments.

UK Finance and its members feel that it is essential that all elements of the model are developed in full and implemented across all PSPs. We do not support the suggestion of short term solutions forming part of the initial implementation. It is critical that this is not delivered in phases across PSPs.

Finally, we ask the PSR to be mindful of the other significant developments PSPs are supporting, including wider implementation of CoP, development of the EFD solution and execution of Consumer Duty.

# Unity Trust Bank

	QUESTIONS	RESPONSES
1.	<p><b>Do you have views on the impact of our proposals on consumers?</b></p>	<p>The proposed changes will provide exceptional protection for consumers. This may be to the detriment of small PSPs. The proposals generally may encourage consumers to take less care when instructing their bank to make payments on their behalf.</p> <p>The increased liability on PSPs may result in smaller PSPs reviewing their criteria and risk appetite for specific less security aware customer groups. This may result in some financial exclusion risks for these groups.</p>
2.	<p><b>Do you have views on the impact of our proposals on PSPs?</b></p>	<p>We accept that improvements are necessary and support the sentiment of the proposals within the consultation. We believe that some of the specific proposals within the consultation will have unintended consequences for small challenger banks/PSPs.</p> <p>Specifically, the absence of a maximum threshold for the PSP's liability will have a disproportionate financial burden on small PSPs. Such a burden increases liquidity and capital exposure for small PSPs.</p> <p><u>Effective prevention and detection of APP scams depends on the conduct of both the customer and the PSP.</u> The customer needs to take responsibility and do what they can to mitigate the risk of falling victim to APP Scams. Currently many PSPs provide awareness communication and warnings to their customers towards prevention and detection of APP scams. Customers will be encouraged to pay attention to these communications and avoid falling victim to APP Scams if they are aware that their negligence in ignoring these messages will undermine any claim against the PSP in the event of an APP scam. Consumers should be encouraged to take some responsibility for their own actions. Where those actions are negligent, particularly where they ignore warnings and guidance, they should not be able to claim. Furthermore, the time limitation for potential reimbursement does not allow PSPs sufficient time to make enquiries and conduct investigations to determine negligence.</p> <p>Customers cannot be absolved of all responsibility; this will not encourage good security practices by consumers and will increase the incidents of APP scams if customers have the impression that they are not expected to be vigilant on their part as they will be reimbursed in any event. This impression will be reinforced by the proposed uncapped reimbursement limit coupled with the high standard of gross negligence set out in the proposals.</p> <p>From the perspective of the PSP, safeguards and customer education are ongoing elements of our service to protect consumers from fraud. The PSP should not be responsible where the consumer refuses to adopt the basic safeguards and processes recommended.</p>

	QUESTIONS	RESPONSES
		<p>We are a PSP with a significant number of micro-enterprises and both small registered and unregistered charities who are often late adopters of technology, using single signatories for payment release and who often operate with pre-printed direct debit mandates. This type of customer presents a greater risk to smaller PSPs as they are less likely to adopt the best security practices for their own protection.</p> <p>In the event that the PSP would be liable irrespective of the contribution of the consumer to the fraud could result in PSPs no longer choosing to bank smaller entities leading to financial exclusion.</p>
3.	<p><b>Do you have views on the scope we propose for our requirements on reimbursement?</b></p>	<p>We would agree with the proposed scope of the reimbursement requirements.</p>
4.	<p><b>Do you have comments on our proposals:</b></p> <ul style="list-style-type: none"> <li>• <b>that there should be a consumer caution exception to mandatory reimbursement</b></li> <li>• <b>to use gross negligence as the consumer caution exception</b></li> <li>• <b>not to provide additional guidance on gross negligence?</b></li> </ul>	<p>In our view the threshold for gross negligence is unrealistic the prevention of APP Scams can only be successful if customers are vigilant and motivated to help themselves falling prey to scams.</p> <p>We would suggest that setting the threshold at negligence and not gross negligence would be more proportionate in these circumstances. We would also suggest that the PSR will need to provide detailed guidance and definition of negligence/gross negligence to ensure clarity and uniformity within the payment services market.</p>
5.	<p><b>Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?</b></p>	<p>As a starting point, where a customer has acted with gross negligence they should not be entitled to reimbursement. PSPs should be encouraged to consider whether the gross negligence was because of customer vulnerability and apply their judgement as to whether they should reimburse the customer. PSPs should be encouraged to consider any causal link between their negligence and the vulnerability when assessing reimbursement.</p>
6.	<p><b>Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?</b></p>	<p>We would support the use of the FCA definition. This is a recognised definition across the industry, and it maintains consistency.</p>

	<b>QUESTIONS</b>	<b>RESPONSES</b>
7.	<p><b>Do you have comments on our proposals that:</b></p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement</li> <li>• any 'excess' should be set at no more than £35</li> <li>• PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?</li> </ul>	<p>We agree that an excess should be applied.</p> <p>We believe the minimum threshold of £35 is too low. It does not provide sufficient motivation for customers to take their own security seriously; we would recommend a higher threshold such as 10% of the value of the transaction.</p> <p>In our view, a low threshold would not deter a potential fraudster from attempting to use the APP scam for their own benefit. A higher percentage-based threshold is more likely to act as a deterrent.</p> <p>We do not believe in an automatic exemption for vulnerable customers. PSPs should be able to evaluate the circumstances of the scam and the role of the consumer in enabling the scammers.</p>
8.	<p><b>Do you have comments on our proposals that:</b></p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to set a minimum claim threshold</li> <li>• any threshold should be set at no more than £100</li> <li>• PSPs should be able to exempt vulnerable consumers from any threshold they set?</li> </ul>	<p>We believe there should be a maximum threshold set, otherwise PSPs are open to unlimited liability, and this may have a detrimental impact on the integrity of the financial system, as small banks will struggle to handle such a burden. In addition, this may drive smaller PSPs to set an upper limit to the value of payments that customers are allowed, to limit their potential liability. This would result in poor outcomes for consumers influencing financial inclusion for consumers, micro-enterprises and charities who form the bulk of the customer demographic for small PSPs. They could face transaction value limits not applicable to other customers.</p>
9.	<p><b>Do you have comments on our proposal not to have a maximum threshold?</b></p>	
10.	<p><b>Do you have comments on our proposals that:</b></p> <ul style="list-style-type: none"> <li>• sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement</li> <li>• any time-limit should be set at no less than 13 months?</li> <li>• reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?</li> </ul>	<p>The 48-hour timeframe proposed for reimbursement does not allow adequate time for PSP to investigate any suspicion of first party fraud or gross negligence. A longer period, perhaps akin to that allowed for investigation under the Contingent Reimbursement Model could allow PSPs adequate time to investigate.</p>
11.	<p><b>Do you have comments on our proposals that:</b></p>	<p>The proposed approach does not reflect the situation for small PSPs using counterparty banks to transact. Whilst we may be the sending PSP, we are reliant to a large extent on</p>



	<b>QUESTIONS</b>	<b>RESPONSES</b>
	<ul style="list-style-type: none"> <li>the sending PSP is responsible for reimbursing the consumer</li> </ul>	<p>effective systems at our counterparty. We believe they must take responsibility for the actions of their staff and systems and bear some of the reimbursement costs.</p>
12.	<p><b>What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?</b></p>	<p>The threshold of evidence to prove gross negligence is too high. Prevention of APP Scams requires customer vigilance to avoid falling prey to scams. Therefore, setting the threshold at negligence and not gross negligence should be more proportionate in these circumstances. As mentioned above, we suggest that the PSR should provide detailed guidance on the definition of negligence/gross negligence to ensure clarity and uniformity within the payment services market.</p>
13.	<p><b>Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?</b></p>	<p>The rules proposed do not seem to consider the smaller PSPs who transact through counterparty relationships. Errors or frauds in counterparty banks will be difficult, if not impossible, for smaller PSPs to detect but the smaller PSP will have equal liability.</p> <p>The proposals need to provide much more detailed guidance for counterparty relationships making proposals for the allocation of reimbursement in these situations.</p>
14.	<p><b>Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?</b></p>	<p>We would suggest that PSPs should be able to depart from the 50:50 default reimbursement. Both mediation and dispute resolution could add further delay to the process. Negotiation would seem the most appropriate proposal.</p>
15.	<p><b>Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?</b></p>	<p>No comments</p>
16.	<p><b>Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?</b></p>	<p>We would agree that the approach to repatriation should follow the same model adopted for reimbursement. We would favour PSPs being able to negotiate the allocation split based on their own contractual relationships and so any repatriation should follow these contractual agreements.</p>
17.	<p><b>Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?</b></p>	<p>No comments</p>



	<b>QUESTIONS</b>	<b>RESPONSES</b>
18.	<b>Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?</b>	We note the long-term ambition for Pay.UK to become the payment system operator and take responsibility for mitigating fraud through the development of scheme rules rather than regulation. We would suggest that a proportionate approach be adopted by Pay.UK in the development of scheme rules with considerations given to the size and variety of firms included within the PSP market.
19.	<b>Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?</b>	No comments
20.	<b>Do you have views on how we should exercise our powers under FSBRA to implement our requirements?</b>	Our key concern in the application of requirements whether by rules or regulation is to ensure a proportionate approach to their application. As mentioned above the PSP market is hugely diverse and we would ask that any implementation engages with firms from all parts of the sector and considers the nuances of the market and the customers served to support firms to deliver good customer outcomes.
21.	<b>Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?</b>	As a small PSP challenger bank, we would suggest that a voice be given to this section of the PSP community to ensure a proportionate approach is applied and to inform the implementation approach based on all segments of the PSP sector.
22.	<b>Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?</b>	A short-term manual reporting approach to monitoring which relies upon PSPs to report compliance should not be overburdensome. The focus should for all PSPs and Pay.UK should be looking to strengthen existing mitigating processes like CoP and RtB rather than producing lengthy compliance reports.
23.	<b>Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?</b>	We would support a real-time monitoring system regardless of provider. To implement this type of monitoring system will require a significant amount of expertise and understanding. A clear structure to the implementation, clear protocols for dealing with PSPs of all sizes and complexity including those which choose to outsource this type of implementation; well communicated timescales and a strong support and engagement network would be considerations we would suggest as part of the programme.
24.	<b>Do you have views on the best option for short-term enforcement arrangements?</b>	No comments
25.	<b>Do you have views on the best way to apply the rules on reimbursement to indirect participants?</b>	No comments

	<b>QUESTIONS</b>	<b>RESPONSES</b>
26.	<b>If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?</b>	No comments
27.	<b>Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?</b>	No comments
28.	<b>Do you have any other comments on the proposals in this consultation?</b>	No further comments

# Victim Support



## **PSR Consultation paper: Authorised Push Payment Scams: Requiring Reimbursement response**

### **Introduction**

Victim Support is an independent charity dedicated to supporting people affected by crime and traumatic incidents in England and Wales. We provide specialist services to help people cope and recover.

In 2021/2022 we supported more than 8,000 victims of fraud across England and Wales, many of whom were victims of authorised push payment fraud. We provide a dedicated support line for the customers of a number of national high street banks, and in some geographic areas we have projects with specialist fraud caseworkers. We have developed fraud-specific resources to help people after they have been a victim of fraud. We are also involved in several Operation Signature initiatives in conjunction with local police services.

Victim Support welcomes the PSR consultation, and its stated aims of increasing fraud prevention and increasing reimbursement to victims, and making reimbursement for scams victims mandatory.

### **Consultation Question Responses**

We have confined our responses to those questions relevant to the experiences of fraud victims with whom we have contact

1. Do you have views on the impact of our proposals on customers?

We welcome the introduction of mandatory reimbursement for victims of authorised push payment fraud. We know from our work that victims routinely face significant anxiety and distress in direct response to the fraud itself, and in relation to their subsequent concerns about whether their PSP can recover their funds, whether they will be reimbursed and if so how much, and when that will occur. A mandatory scheme with prompt reimbursement of lost funds will reduce much of the worry and hardship caused by APP fraud

2. Do you have views on the impact of our proposals on PSPs?

We share similar concerns to the PSR, that the voluntary CRM has not facilitated the volume or percentage of reimbursements that the scheme was designed to deliver and that fraud victims should receive. Currently the voluntary nature of the CRM means that only some PSPs are routinely reimbursing, and even where they do, this is often inconsistent. This creates an opaque and unfair environment for fraud victims, who may or may not be reimbursed, depending on their PSP's efficiency and effectiveness. We therefore welcome the emphasis on all PSPs doing more to prevent APP fraud and to reimburse victims where they have failed to

# OFFICIAL

prevent fraud. We think it likely that customers will tolerate a degree of payment friction if this is in their interests in order to prevent fraud

Furthermore we believe these measures will encourage PSPs to take a more proactive role in preventing and detecting fraud, and promptly recovering customer funds where this is possible.

The consultation document sets out an expectation that 'On-Us' payments are brought within scope of a mandatory reimbursement scheme. We would suggest the PSR should go further and make this a pre-requisite, so that no customers are disadvantaged by their bank overseeing both sending and receiving accounts

### 3. Do you have views on the scope we propose for our requirements on reimbursement

Although APP frauds are largely conducted within the Faster Payments System (and we accept that the PSR has a limited remit in this respect), it is imperative that a broader view of the payments process is adopted. PSPs have a responsibility to ensure robust verification of new customer identities, to prevent bad actors from entering and operating within the payments system. We recommend that the PSR and its key partners focus also on improving verification and security, in order to design out fraud from the outset of the customer journey. We welcome the inclusion of all categories of APP fraud, and accept that civil disputes between customers and legitimate suppliers will be excluded

### 4. Do you have comments on our proposals:

- a. that there should be a consumer caution exception to mandatory reimbursement
- b. to use gross negligence as the consumer caution exception
- c. not to provide additional guidance on gross negligence?

Our experience is that customers are not financially careless and do not willingly open themselves up to fraud - it is hugely distressing; it impacts on finances, health and wellbeing, as well as personal and professional relationships; it often has life-changing consequences. We are not aware of any evidence that customers will take less care if reimbursement is more likely. Indeed the existence and experience of s75 Consumer Credit Act and chargeback reimbursements suggests that this safety net does not increase less cautious behaviours.

Our view is that there are already significant barriers to customers identifying and self-reporting fraud (evidenced in the low levels of fraud reporting compared to other crime types), and a customer caution exception could be readily exploited by PSPs to deny customer reimbursement and therefore dissuade people from reporting in the first place.

We are concerned that PSPs may have varying or inconsistent applications on what constitutes 'gross negligence' and are particularly concerned that banks may decide that not responding to a Confirmation of Payee response becomes a threshold for not reimbursing. We therefore recommend that the PSR should mandate that Pay.UK have strong compliance monitoring responsibilities for auditing the application of this, in order to ensure accountability and transparency

### 5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?

We support the reimbursement of vulnerable customers under all circumstances, including those who may have acted with what appears to be gross negligence. We have also seen examples of highly vulnerable victims being groomed, coerced, or threatened into assisting fraudsters. We would therefore recommend that the PSR go further on this issue, and require PSPs to evaluate potential vulnerability (and reimbursement) when investigating suspected first party frauds, and 'money mules'.

# OFFICIAL

## 6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?

We accept that the FCA definition of a vulnerable customer is an adequate starting point.

We understand that defining and then identifying vulnerabilities -especially temporary characteristics - is challenging. Many victims behave differently to how they 'typically' would at the time of the fraud, due in part to the highly sophisticated social engineering techniques used, the presence of external/personal factors, and broader societal issues such as varying levels of financial or digital literacy.

Not all customers who have these characteristics will experience harm. But they may be more likely to have additional or different needs which, if firms do not meet them, could limit their ability to make decisions or represent their own interests, putting them at greater risk of harm.

We are concerned that PSPs may tend to adopt a 'checklist' approach to identifying vulnerability, with the attendant risks that unless a customer explicitly exhibits a readily identifiable characteristic then their vulnerability is overlooked. PSPs (and Pay.UK) will need to continually review the applications of vulnerability in the light of emerging fraud, as fraudsters find new and innovative ways to exploit people and to circumvent the existing FPS obstacles to fraud.

## 7. Do you have comments on our proposals that:

- a. sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
- b. any 'excess' should be set at no more than £35
- c. PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

We understand that the £35 and £100 thresholds and the 13 month time claim being proposed by PSR echo existing thresholds relating to unauthorised fraud. Our view is that - unless there is an evidence base that demonstrates that these thresholds will specifically and demonstrably prevent authorised push payment fraud and increase reimbursement - these thresholds should not apply. We believe that symmetry or neatness of rules is insufficient reason alone, especially as the authorised push payment fraud environment is substantively different to that of unauthorised fraud.

As one of the PSR stated purposes of mandatory reimbursement is to incentivise PSPs to reduce fraud from the outset, then any proposed excess may mitigate against this. Whilst the sum of £35 may conveniently echo the existing excess deducted for unauthorised losses, this is not an evidence base for introducing it, and does not by itself justify it. Furthermore when coupled with the proposal to allow PSPs to set a threshold of £100, these measures appear to push against incentivising PSPs to reduce fraud.

We know that fraud is a significantly under-reported crime, and the introduction of an excess and a claims threshold could in our view act as a further deterrent for victims to report, especially on lower value fraud. This then raises the risk of creating unintended consequences, whereby victims are even less likely to report lower value fraud, PSPs are less likely to investigate, and fraudsters are more likely to exploit this area

We believe the PSR should mandate that all vulnerable victims are exempted from any excess, rather than leaving this a matter for each PSP to decide

# OFFICIAL

8. Do you have comments on our proposals that:
  - a. sending PSPs should be allowed to set a minimum claim threshold
  - b. any threshold should be set at no more than £100
  - c. PSPs should be able to exempt vulnerable consumers from any threshold they set?

Our view is that the proposed minimum threshold will disadvantage many victims for whom £100 is a lot of money, especially in the current economic climate. A loss of under £100 may appear modest, but for some people this will have significant and harmful impacts.

We supported Mr A, who had a poor credit score and intermittent employment history and was trying to obtain a 'payday' loan to meet a pressing financial demand. A fraudster contacted him posing as a legitimate company and requested an upfront fee of £90 to process their application. Mr A has now lost this sum, still has immediate and longer term financial difficulties, and had to receive our assistance to approach his local adult social services team for an emergency food package

Should the PSR retain the proposed £100 threshold, we recommend that detailed guidance is issued to PSPs. This should make clear that where multiple individual transactions under £100 are made, it is the composite value of the fraud is taken into account. Our experience is that victims are sometimes subject to repeat fraud, and so it is important that they are not disadvantaged by lower value but repetitive and therefore cumulative losses

9. Do you have comments on our proposal not to have a maximum threshold?

We support this recommendation not to have a maximum threshold, for the reasons set out by the PSR

10. Do you have comments on our proposals that:
  - a. sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
  - b. any time-limit should be set at no less than 13 months?

Our view is that the proposed maximum claim time will disadvantage many victims, who may not be aware that a fraud has taken place.

We worked with Ms B, who was defrauded into investing in a non-existent financial product. She received periodic 'updates' from the fake company telling her how well her investment was performing. However when she did not receive the dividends she was expecting at 24 months, Ms B made further enquiries and established she was a victim of a large and elaborate fraud that had also created over 4,000 other victims.

We also supported Mr C, who had transferred £20,000 into 'investments' he had seen on the website of well-known financial management company. The website had been 'cloned', and it was only when Mr C read about this in a national newspaper two years later that he realised he had been defrauded. His bank refused to reimburse him until - with our support - Mr C complained to the Financial Ombudsman Service. He was then reimbursed in full.

We believe that a 13 month time limit for claims will rule out reimbursement for many victims of pensions or investments fraud, and also victims of relationship/romance fraud, due to the length of time over which these frauds are perpetrated, and only then subsequently come to light. Our view is that this will undermine the PSR's commitment to ensure that victims of higher value and lower volume fraud are reimbursed

# OFFICIAL

11. Do you have comments on our proposals that:
- a. the sending PSP is responsible for reimbursing the consumer
  - b. reimbursements should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?

We support the recommendation that reimbursement should be administered by the sending PSP and should be prompt, for the reasons set out by the PSR. This will lessen the distress, anxiety and financial difficulties or hardships experienced by fraud victims, and will reduce the victim's need to access other services. We also agree that sharing reimbursement costs split 50/50 between sending and receiving PSPs may encourage receiving PSPs to be more proactive in detecting fraudulent activity within their own accounts, and to be quicker in freezing and repatriating funds

28. Do you have any other comments on the proposals in this consultation?

The current CRM Code contains a number of directions to PSP signatories relating to customer information, advice, support, and consumer education. Our view is that these are important additions to PSPs responsibilities under the CRM, and we recommend these responsibilities are not 'lost' in the move to a new reimbursement regime. As set out earlier in our response, our experience is that customers do not want to fall victim to fraud, with all the subsequent anxieties and obstacles this entails. We would therefore recommend that the PSR mandates requirements within the new scheme to ensure that PSPs have robust responsibilities to ensure their customers are properly verified when setting up new accounts, are given tailored, meaningful and timely information, advice and guidance on how to stay safe from fraud, and lastly are properly supported in the event that a fraud takes place

  
National Fraud Lead  
Victim Support  
09 December 2022



# Virgin Money UK

**Virgin Money response to PSR CP22/4 Authorised push payment (APP) scams: Requiring reimbursement**

***Question 1: Do you have views on the impact of our proposals on consumers?***

VMUK are supportive of the goal of the proposals, to significantly reduce APP scams and are pleased to see that the proposals cover all PSPs. VMUK expect better protection across the industry will build consumer confidence in faster payments. Including Indirect PSPs and having limited exceptions will also ensure that consumers of all PSPs will be treated fairly.

VMUK agree that there could be potential consequences for consumers because of the proposals, whilst VMUK would not expect to see vulnerable customers prevented from using banking services consumers should be informed to expect increased levels of intervention and challenge from PSPs to confirm payments instructions are not a result of a scam. This may also lead to increased levels of payment instructions being refused and accounts blocked as a result of PSP scam concerns.

***Question 2: Do you have views on the impact of our proposals on PSPs?***

VMUK believe that PSPs that are already part of the CRM code will continue the good work which has already been achieved to invest in scam prevention and mule identification. PSPs which are not part of the voluntary code and do not have equivalent or greater scam prevention protections in place will be required to significantly increase capabilities which will benefit all consumers.

VMUK understand the proposals are set out within the remit of the PSR, however the mandatory reimbursement proposal may have the unintended consequence to reduce incentives and focus on the enablers of APP scams which would not meet the recommendations from the House Of Lords report "Fighting Fraud: Breaking the Chain".

***Question 3: Do you have views on the scope we propose for our requirements on reimbursement?***

VMUK are pleased to see all payments initiated through Faster Payments are in scope of the proposals and agree with the expectation that on-us payments should be treated similarly.

VMUK understand the proposal for all categories of APP scams to be in scope given the impact all APP scams have on consumers. Clear rules and guidance should be given to PSPs and Consumers at a Scam type level, for example a consumer committing to a legitimate high-risk investment should not be given the misunderstanding that they would be protected by these rules if the investment produces a loss.

***Question 4: Do you have comments on our proposals:***

- *that there should be a consumer caution exception to mandatory reimbursement*

VMUK supports the exception to mandatory reimbursements to encourage consumer caution. VMUK agree with the comment that consumers don't want to be scammed, though levels of consumer caution may vary depending on the scam type. The expectation is that consumers will generally exercise greater caution during an impersonation/safe account scam, compared to a purchase scam given the likely variation in amount and reason for payment.

- *to use gross negligence as the consumer caution exception*

Whilst VMUK agree that gross negligence should play a part in determining the reimbursement, without clear guidance across different scam types as to what factors would be determined as gross negligence it is difficult to determine the circumstances where this exception would be applied, if at all.

- *not to provide additional guidance on gross negligence?*

Despite the challenges noted in the proposal, VMUK would urge the PSR to reconsider to provide guidance on gross negligence so that PSPs and consumers are clear as to the expectations and a consistent application of gross negligence exception can be applied. Standards should not be lowered through the adoption of guidance for gross negligence.

***Question 5: Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?***

VMUK agrees that vulnerable customers should be provided with additional levels of protection against APP scams, like the approach taken with the CRM code.

***Question 6: Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?***

The FCA definition of vulnerability is not specific to APP Scams so may not be the most appropriate definition to use. There may be value in considering the CRM code definition of vulnerability which extended to the customers susceptibility to a scam. This would see consumers who are not typically deemed as vulnerable, but were at the time of the scam, included within the scope of mandatory reimbursement exceptions.

***Question 7: Do you have comments on our proposals that:***

- *sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement*

VMUK would not expect the excess to be used in most situations, unlike the insurance excess which a customer sets when entering a contract, the expectation is this is solely at the discretion of the PSP and may vary between different PSPs.

- *any 'excess' should be set at no more than £35*

VMUK would recommend that the PSR either removes this measure from the proposal or directs an excess value so that there is a clear expectation from consumers, although PSPs could take the view that they will return the excess as a gesture of goodwill if the excess is mandated.

- *PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?*

VMUK agree that vulnerable customers should receive additional support, which would include being exempt from such measures.

***Question 8: Do you have comments on our proposals that:***

- *sending PSPs should be allowed to set a minimum claim threshold*

Like the excess measure, VMUK would recommend that any thresholds should be directed by the PSR or included in scheme rules, as this is a consumer protection measure it should not be competitive and should protect all consumers equally.

- *any threshold should be set at no more than £100*

The proposed threshold limit would likely not be sufficient to drive consumer caution as any proposed payment incentives (i.e. too good to be true products and services) will likely outweigh potential risks.

- *PSPs should be able to exempt vulnerable consumers from any threshold they set?*

VMUK agree that vulnerable customers should receive additional support, which would include being exempt from such measures.

**Question 9: Do you have comments on our proposal not to have a maximum threshold?**

A maximum threshold for mandatory reimbursement should be considered, this would not result in payments above the threshold being excluded from reimbursement but, similar to the TSB refund guarantee and Credit Card protections highlighted in the proposal, provide an incentive for consumer caution and avoid an automatic unlimited liability for PSPs.

Above threshold guidelines could be provided which determine the actions which should be taken on reimbursements for any claims applicable which may extend below the high level gross negligence bar whilst taking into account the circumstances and actions of the consumer, Sending and Receiving PSP.

**Question 10: Do you have comments on our proposals that:**

- *sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement*
- *any time-limit should be set at no less than 13 months?*

VMUK agree with the setting of a time-limit for claims for mandatory reimbursement and would urge the PSR to direct the time-limit to ensure consumers receive consistent levels of protection.

Scam payments which extend over long periods and may fall out with the time limits often involved customers making payments from multiple PSPs. Noting that the time-limit starts from the last scam payment can this be clarified to be the last successful scam payment at the PSP.

**Question 11: Do you have comments on our proposals that:**

- *the sending PSP is responsible for reimbursing the consumer*

VMUK Agree that the Sending PSP should be responsible for reimbursing the customer.

- *reimbursement should be as soon possible, and no later than 48 hours after a claim is made, unless the PSP can evidence suspicions of first party fraud or gross negligence?*

VMUK agree that consumers who are eligible for a reimbursement receive this at the earliest opportunity. 48 hours does not seem sufficient time to ascertain the relevant facts surrounding an APP claim to reach an accurate decision as to the relevance of first party fraud or gross negligence. In addition to accurately identify and understand vulnerability and after care needs appropriately.

There is a higher risk within the proposed timeframe that additional evidence is identified following a reimbursement leading to a requirement to alter the original decision, guidance on how PSPs should approach this would be required.

**Question 12: What standard of evidence for gross negligence or first party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?**

Evidence is likely to vary depending on the type of scam being reported, it will therefore be difficult for PSPs to gather and interpret all relevant evidence within a 48 hour timeframe. VMUK would

recommend that the existing CRM timeframes be considered as an alternative. This would support accurate first-time outcomes, avoiding rework and reducing risk where evidence points to a different outcome to that available within the first 48 hours.

Guidance will also be required as to when the 48 hour time period should be calculated, taking into account weekends, public holidays etc...

***Question 13: Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?***

VMUK are supportive of the proposed default allocation between sending and receiving PSPs.

With the increase in open banking payments expected over the next few years further guidance on PISP payments would be appreciated.

***Question 14: Do you have views on our proposal that PSPs are able to choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?***

VMUK understand the intent of the proposals for PSPs to depart from the default allocation, however if the proposals achieve the aims to incentivise and guidance is clear to all PSPs there should be little requirement to depart from the default position.

Should departure from 50:50 allocation be progressed VMUK would welcome additional guidance/more tailored allocation criteria and how PSPs would be assessed in their application and assessment of allocation.

***Question 15: Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?***

VMUK believe the proposals would not work with multi-generational scams and should be restricted to the point in which the funds leave the consumers control, limiting the scope to a single generation of payment.

***Question 16: Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?***

VMUK agree with the position that repatriated funds should follow the 50:50 default allocation when a consumer has been reimbursed in line with the mandatory reimbursement proposal.

VMUK would also support further investigation of more tailored criteria for allocation of repatriation costs and associated dispute arrangements. Like the criteria for allocation of reimbursements costs, the criteria/process for repatriation should be robust and easy to understand by all parties.

***Question 17: Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?***

VMUK support the inclusion of all PSPs within the scope of allocating the costs of mandatory reimbursement and welcome the inclusion of Indirect PSPs in the scope as this should hopefully incentivise all parties to improve their fraud capabilities.

***Question 18: Do you have views on our long-term vision, and our rationale for the PSO being the rule-setter responsible for mitigating fraud?***

VMUK agree that the PSO has a significant role to play in the mitigation of fraud across the industry, however, we feel that longer term legislative change is required and it would be more appropriate for the PSR to place a Direction on all PSPs to comply. Pay.UK currently does not have the appropriate powers of enforcement in place and we would question whether the challenges raised by the PSR could be suitably covered to enable them to govern effectively and consistently where non-compliance to rules is identified.

As fraud continues to grow, it is imperative that the industry has robust processes and rules in place for reimbursement to ensure consistency and that all PSPs can be governed appropriately by these rules. Currently, for Credit Payment Recovery where reimbursement is on a best endeavours basis, Pay.UK have no powers to engage or influence recovery rates of Indirect PSPs and rely on the contract between the sponsoring bank and Indirect PSP, which can produce varying levels of recovery.

***Question 19: Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?***

VMUK do not support mandatory reimbursement via scheme rules. Significant changes would be required to FPS rules and as such would require the agreement of all PSPs. Sponsoring banks would also need to engage their Indirect PSPs and we feel that this would be a lengthy process to even obtain agreement from all parties before any tangible change could be considered. We feel that a Direction and longer-term legislative change would be more appropriate. FPS scheme rules could be used to support any changes in legislation in the future.

***Question 20: Do you have views on how we should exercise our powers under FSBRA to implement our requirements?***

As outlined within the response, VMUK believe a direction would be a more appropriate method to implement the proposed requirements.

***Question 21: Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?***

The allocation of criteria for dispute resolution is subjective and we would welcome further industry discussion on costs and benefits as to how this could be developed and achieved, and whether it is in fact the correct approach.

***Question 22: Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?***

VMUK agree that compliance monitoring is key to any new initiative, however, the controls in place need to cover all PSPs (including Indirect PSPs) and PISPs, for which Pay.UK has no control currently.

***Question 23: Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system and when it could be introduced?***

VMUK agree that real-time monitoring would be the most effective form of monitoring and would be expected to realise the most benefits. Further discussion would be required on costs and benefits as to how a short-term approach could be implemented.

Pay.UK and the industry have a significant schedule of work over the next few years to deliver NPA so careful consideration should be given to current resource and time constraints to ensure that what can be delivered is fit for purpose and also does not detract from implementing NPA.

***Question 24: Do you have views on the best option for short-term enforcement arrangements?***

The key priority is to ensure consistency across the industry, and VMUK feel that the best option for enforcement is to introduce legislative changes to tackle authorised payment fraud. As most of the options considered for enforcement involve the PSR it would seem the appropriate option is through direction and existing enforcement avenues.

***Question 25: Do you have views on the best way to apply the rules on reimbursement to indirect participants?***

As per previous responses VMUK believe the best way to apply the rules on reimbursement to indirect participants is through a direction.

***Question 26: If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or IAPs?***

As per previous responses VMUK believe all PSPs should be included in a direction.

***Question 27: Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?***

VMUK broadly agree with the cost benefit analysis, though would highlight those benefits may be lower than anticipated when considering the latest available MI in relation to APP scams. Provided by UK Finance Half Year Fraud Report 2022 which highlights reductions in APP scams and increases to reimbursement rates in the first half of 2022.

The analysis assumes that all scam types are equal, which is not the case, the moral hazard impact may be low where a customer is being called to send significant sums in the case of an impersonation scam. However, the inclusion of purchase scams, may see very different approach with customer more likely to take the risk on a smaller purchase to obtain goods and services that they want to acquire, knowing that they will receive mandatory reimbursement.

***Question 28: Do you have any other comments on the proposals in this consultation?***

Significant changes would be required to FPS rules and as such would require the agreement of all PSPs. Sponsoring banks would also need to engage their Indirect PSPs and we feel that this would be a lengthy process to even obtain agreement from all parties before any tangible change could be considered. Timescales would therefore need to be realistic.

Confirmation of Payee is a perfect example of where a Direction was required to gain consistency across the industry and better protect customers.

# Which?



## Consultation Response

### **Which? response to PSR's consultation on *Authorised push payment (APP) scams: Requiring reimbursement***

#### **Summary**

- **Which? welcomes the PSR's proposals for mandatory reimbursement of authorised push payment (APP) scam victims.** Having highlighted this issue to the government, regulators and industry for a number of years, including through a super-complaint to the PSR in 2016, we believe these proposals could have a huge impact in reducing the financial and related emotional impact of APP fraud on victims if it leads to fairer decision-making by payment service providers (PSPs), and help incentivise better reporting and prevention measures across industry.
- **We strongly support the PSR requiring all PSPs sending payments over Faster Payments to fully reimburse APP scam victims in all but exceptional circumstances.** Putting a reimbursement obligation on firms involved in a fraudulent transaction is by no means novel; it is a statutory requirement on PSPs involved in unauthorised bank payment transactions, with the exception of cases where victims are 'grossly negligent,' and is a core principle underscoring the voluntary Contingent Reimbursement Model (CRM) Code.
- **Given the many unfair and inconsistent decisions on reimbursement made by the 10 signatories to the CRM Code using its four exclusions for reimbursement, the PSR's proposal for a single consumer caution exception to mandatory reimbursement will be a fairer and more effective approach to apply to around 400 PSPs, if it is properly implemented.** Crucially, the consumer caution exception should only apply in cases where the PSP is not at fault. Firms must also be required to base their decisions on the reality of victims' experiences in which they believed they were acting appropriately at the time. In doing so, the burden of proof should be on the firm to establish exceptional circumstances.
- **We are not aware of convincing evidence to suggest that moving to a system of mandatory reimbursement could lead to customers taking less care when making payments, due to an awareness of consumer protections.** Such theoretical claims are at odds with TSB's real-life experience of reimbursing 98% of authorised and unauthorised scam victims under its Fraud Refund Guarantee. TSB has



been clear that it has not seen evidence of “additional moral hazard” nor any significant change in the amount of fraud being reported as a result of its reimbursement policy.<sup>1</sup>

- Rather than relying solely on a direction on Pay.UK, the PSR should direct all PSPs to implement its rules on reimbursement.** We are concerned with the PSR’s current proposal to direct Pay.UK to introduce this reimbursement obligation into Faster Payments scheme rules, given that Pay.UK lacks the PSR’s enforcement powers, cannot currently make rules for indirect Faster Payments participants, and does not cover CHAPS payments. Rather than relying solely on a direction on Pay.UK, the PSR should direct all PSPs to implement its rules on reimbursement to minimise gaps in protections, and so that the PSR can use its enforcement powers to sanction firms that do not meet its expectations. Though the PSR would be responsible for enforcing the reimbursement obligation under a direction, Pay.UK will need to play a key role in supporting PSPs to implement the direction, which may require the PSR to direct Pay.UK as well as PSPs to ensure that it fully meets its expectations in this regard. Moreover, the Government should also legislate so that scam victims can take action to enforce their rights directly against firms that are in breach of these obligations.

**The following table briefly outlines Which?’s positions on the PSR’s proposals.** We explain our positions in further detail in our response.

Policy issue	Our position in brief
Scope and implementation of mandatory reimbursement	<p>We strongly support the PSR's proposal for the reimbursement obligation to apply to all types of APP scams.</p> <p>Rather than relying solely on a direction on Pay.UK, the PSR should direct all PSPs to implement its rules on reimbursement. The PSR may also need to direct Pay.UK to introduce rules to support the implementation of the reimbursement obligation. HM Treasury should separately conduct a broader review of fraud protections, including whether any new payment systems should be regulated by the PSR.</p>
Consumer caution exception to mandatory reimbursement	<p>The PSR’s proposal for a single consumer caution exception to mandatory reimbursement will be a fairer and more effective approach than the CRM Code’s four exclusions for reimbursement, if it is properly implemented. Crucially, the consumer caution exception should:</p> <ul style="list-style-type: none"> <li>only apply in cases where the PSP is not at fault;</li> <li>be based on the reality of victims' experiences in which they believed they were acting appropriately at the time; and</li> </ul>

<sup>1</sup> House of Lords (Nov 2022) Fraud Act 2006 and Digital Fraud Committee, Report of Session 2022-23. Fighting Fraud: Breaking the Chain, p.116. Available at: <https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf>

	<ul style="list-style-type: none"> <li>place the burden of proof on PSPs to establish exceptional circumstances.</li> </ul>
Vulnerable consumers	We support the PSR's proposal that any consumer caution exception will not apply to vulnerable consumers, and the use of the FCA definition to identify consumers vulnerable to APP scams - though it is vital that PSP's consider a wider range of contextual factors when seeking to understand a consumer's behaviour and how this interacts with the nature of the scam.
Excess charge of no more than £35	We oppose the proposal for an excess charge.
Minimum threshold of no more than £100	We oppose the proposal for a de minimis.
No maximum threshold	We support the PSR's decision to not have a maximum threshold on claims. The FCA should also ensure that any APP scam cases going to the Financial Ombudsman Service, either for appeal or after the time limit set on claims for mandatory reimbursement has expired, comply with the PSR's proposal to not have a maximum threshold on claims.
Time limit on claims of no less than 13 months	The PSR should instead implement a general limitation period of six years after the victim becomes aware that they have been scammed, in line with Section 75 protections under the Consumer Credit Act.
48 hours to reimburse a victim	PSPs and victims may need more time than 48 hours to ensure decisions are fair and so that victims are not put under undue pressure for further information too soon.
50:50 default allocation of reimbursement costs	We support 50:50 default allocation of reimbursement costs as a fair starting point, which could evolve based on evidence of where the risk is greatest between PSPs.
Multigenerational scams (ie multiple payment steps including to different accounts held by the victim, before being transferred into an account under the fraudster's control)	This should be addressed through bringing the other payment methods used in these types of scams under a reimbursement obligation. HM Treasury should address this as part of a broader review of fraud protections.

### **Why mandatory reimbursement is needed**

Though the fraudulent payment may be the last step in the scam, the choice of payment method and payment provider is integral to the scam. Fraudsters have to plan ahead with how they will receive and launder these funds, either operating an account directly or via money mules. Most scams involve a payment between two UK accounts first, to help avoid suspicions,

so fraudsters typically target the weakest points in the UK's payment systems. It is no accident that the prime target is currently the Faster Payments scheme, where there is no explicit requirement for banks to reimburse victims when a payment turns out to be to a fraudster, unlike for many other payment methods such as cards. As we have long argued, this lack of consumer protection means there are insufficient incentives for banks and PSPs to prevent authorised fraud. Providing a direct financial incentive for both sending and receiving PSPs to tackle fraud through these new proposals could drive better reporting and prevention measures across industry. Therefore, addressing this gap in protections is as key to our attempts in preventing fraud as it is to providing a fairer system of allocating losses.

Since Which? issued a super-complaint to the PSR in 2016, calling attention to the striking gap in fraud protections and redress for fraud via authorised push payments compared to other payment methods such as cards, reported losses to APP scams have risen year on year. In 2021, victims lost a total of £583.2 million, a 39% increase on the previous year.<sup>2</sup> This figure accounts for 33 UK Finance members only, thus the scale of the problem involving smaller PSPs is not fully known. Despite a commitment to the CRM Code by ten PSPs - who account for more than 90% of Faster Payments transactions - victims still shoulder two-fifths of these losses. In H1 2022, 60% of losses were reimbursed to APP scam victims under the industry Code, totalling £117.2 million.<sup>3</sup> Though this data reflects the first half of this year only, it is higher than previous years: 51% of losses were reimbursed in 2021,<sup>4</sup> 47% in 2020, and in 2019, just 41% of cases assessed under the Code were reimbursed.<sup>5</sup>

However, the application of the CRM Code has failed to provide fair and consistent outcomes for APP scam victims. Although signatory banks are reimbursing victims more under the Code, reimbursement levels remain shockingly low, to the extent that the PSR itself has expressed that the Code has not led to the significant reduction in APP scam losses incurred by victims that is needed.<sup>6</sup> The inconsistent and arbitrary application of the four overlapping consumer exclusions under the Code by banks, and the lack of appropriate regulatory oversight and enforcement to hold firms to these standards, has led to a 'reimbursement lottery' for scam victims. Since 2019/20, the Financial Ombudsman Service has upheld around three-quarters of complaints by victims against banks for authorised fraud, compared to an uphold rate for all types of complaints of around a third.<sup>7</sup> Uphold rates for individual firms for authorised fraud

---

<sup>2</sup> UK Finance (2022) Annual Fraud Report: The definitive overview of payment industry fraud in 2021, p.47. Available at: [https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022\\_FINAL.pdf](https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL.pdf).

<sup>3</sup> UK Finance (2022) 2022 Half year fraud update, p.22. Available at: <https://www.ukfinance.org.uk/system/files/2022-10/Half%20year%20fraud%20update%202022.pdf>.

<sup>4</sup> UK Finance (2022) Annual Fraud Report: The definitive overview of payment industry fraud in 2021, p.49. Available at: [https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022\\_FINAL.pdf](https://www.ukfinance.org.uk/system/files/2022-06/Annual%20Fraud%20Report%202022_FINAL.pdf).

<sup>5</sup> UK Finance (2021) Fraud - The Facts 2021: The definitive overview of the payment industry, p.55. Available at: <https://www.ukfinance.org.uk/system/files/Fraud%20The%20Facts%202021-%20FINAL.pdf>.

<sup>6</sup> Payment Systems Regulator (Feb 2021), Authorised push payment (APP) scams: Call for views, p.4. Available at: [https://www.psr.org.uk/media/5yvpidyc/psr\\_cp21-3\\_app\\_scams\\_call\\_for\\_views\\_feb-2021.pdf](https://www.psr.org.uk/media/5yvpidyc/psr_cp21-3_app_scams_call_for_views_feb-2021.pdf).

<sup>7</sup> In 2019/20, the FOS upheld an average of 75% complaints involving authorised fraud. In 2020/21, this figure was 73%. In Q2 2021/22, the FOS reports that it upheld around three quarters in the consumers' favour. See Financial Ombudsman Service (2021) Annual complaints data and insight 2020/21, available at:

vary significantly, but are as high as 86%.<sup>8</sup> Our qualitative research into the scam journeys of 20 APP scam victims found that, amongst those we spoke to, banks did not clearly explain to customers the reasoning as to why they were denied reimbursement under the CRM Code.<sup>9</sup> This lack of clarity can prevent victims from understanding that in these circumstances they would have the ability to appeal the decision to the Ombudsman, which frequently finds in favour of scams victims.

Further to this, as a consequence of the case backlog that the Ombudsman is currently tackling, the median time taken to convert all cases to closing is currently six months instead of four.<sup>10</sup> However, many fraud cases often take longer to resolve. This is a significant amount of time for scam victims to wait on a reimbursement decision, and can exacerbate the major emotional and psychological distress they may feel as a result of being scammed, and leave some individuals in a position of financial difficulty.<sup>11</sup>

Moreover, in a series of reviews of the CRM Code, the Lending Standards Board (LSB) repeatedly found inconsistencies in the application and outcomes under the Code.<sup>12</sup> It found that “The presumption in the Code that victims should be reimbursed unless there is a clear ground for attributing blame to the consumer was sometimes reversed so that the customer was held liable in many cases where the bank was not.”<sup>13</sup> In June 2021, the LSB warned CRM Code signatories of “systemic failings,” stating that “work must be undertaken by signatory firms without delay to ensure the best outcomes for customers.”<sup>14</sup>

## **Ensuring that mandatory reimbursement is implemented fairly and consistently**

With approximately 400 direct and indirect PSPs in scope under new measures, consistent outcomes will be even more challenging to achieve than under the voluntary CRM Code among its ten signatories. Given that how the proposals are implemented and enforced will be critical

---

<https://www.financial-ombudsman.org.uk/data-insight/annual-complaints-data>, and Financial Ombudsman Service (2021) Quarterly complaints data, available at:

<https://www.financial-ombudsman.org.uk/data-insight/quarterly-complaints-data>.

<sup>8</sup> Which? (2021) Banks wrongly denying fraud victims compensation in up to 8 in 10 cases. Available at:

<https://www.which.co.uk/news/2021/11/banks-wrongly-denying-fraud-victims-compensation-in-up-to-8-in-10-cases/>

<sup>9</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

<sup>10</sup> Financial Ombudsman Service (Dec 2021) Plans and Budget 2022-23 consultation, p.13. Available at:

<https://www.financial-ombudsman.org.uk/files/320493/plans-and-budget-consultation-2022-23.pdf>.

<sup>11</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

<sup>12</sup> Lending Standards Board (Jan 2021), Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams, p.4. Available at:

<https://lendingstandardsboard.org.uk/wp-content/uploads/2021/01/LSB-review-of-the-CRM-Code-FINAL-January-2021-1-.pdf>.

<sup>13</sup> Lending Standards Board (June 2021), Contingent Reimbursement Model Code for Authorised Push Payment Scams: Review of approach to reimbursement of customers, p.2. Available at:

<https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/06/CRM-Review-R21c-Follow-Up-Summary-Report.pdf>.

<sup>14</sup> Lending Standards Board (2021), LSB issues warning to CRM Code signatories over Authorised Push Payment (APP) scams. Available at:

<https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/06/Press-release-CRM-Code-follow-up-review.pdf>.

to its potential impact, we are concerned with the PSR's current proposal to direct Pay.UK to introduce this reimbursement obligation into Faster Payments scheme rules, as Pay.UK lacks the PSR's enforcement powers, cannot currently make rules for around 350 PSPs which are indirect participants in Faster Payments, and does not cover CHAPS payments.

Rather than relying solely on a direction on Pay.UK, the PSR should direct all PSPs to implement its rules on reimbursement, to minimise gaps in protections and so that the PSR can use its enforcement powers to sanction firms that do not meet its expectations. This would be similar to the approach the regulator has taken in implementing Confirmation of Payee, where it recently directed approximately 400 PSPs that send and receive Faster Payments and CHAPS payments to implement the service, broadening consumer protections to more payment system users.<sup>15</sup> We therefore see a PSR direction on PSPs as a way to better ensure that the reimbursement requirements apply to all PSPs as soon as they are in place, including indirect PSPs and Payment Initiation Service Providers (PISPs), as well as applying to CHAPS payments.

Given the risk of unfair outcomes for individual consumers that could cause life-changing harm, the Government should also legislate so that scam victims can take action to enforce their rights directly against firms that are in breach of these obligations. This could also have a strong impact in further incentivising PSPs to introduce better reporting and prevention measures in efforts to tackle APP scams.

Though the PSR would be responsible for enforcing the reimbursement obligation under a direction on PSPs, Pay.UK will need to play a key role in supporting PSPs to implement the direction, which may require the PSR to direct Pay.UK as well as PSPs to ensure that it fully meets its expectations in this regard. In the longer term, the PSR and Pay.UK should consider how Pay.UK's role could evolve on APP scams, which will require greater consideration towards how it operates and may require further regulatory intervention.

## **Which?'s positions on the specifics of how the PSR will introduce mandatory reimbursement**

### **Consumer caution exception to mandatory reimbursement**

Given the many unfair and inconsistent decisions on reimbursement made by the 10 signatories to the CRM Code using its four exclusions for reimbursement, the PSR's proposal for a single consumer caution exception to mandatory reimbursement will be a fairer and more effective approach to apply to around 400 PSPs, if it is properly implemented.

Crucially, the consumer caution exception should only apply in cases where the PSP is not at fault. Firms must also be required to base their decisions on the reality of victims' experiences in which they believed they were acting appropriately at the time. In doing so, the burden of proof

---

<sup>15</sup> PSR (May 2022) Confirmation of Payee: Requirements for further participation in CoP. Available at: [https://www.psr.org.uk/media/gc1bfva1/psr-cp22-2-requirements-for-further-participation-in-cop\\_may-2022.pdf](https://www.psr.org.uk/media/gc1bfva1/psr-cp22-2-requirements-for-further-participation-in-cop_may-2022.pdf).



should be on the firm to establish exceptional circumstances where reimbursement is not justified.

Some stakeholders argue that the regulator's proposals could lead to 'moral hazard', with consumers being knowingly reckless when making payments because they are aware that they are more likely to get their money back if things go wrong. Like the PSR states in its consultation, we are not aware of any convincing evidence to suggest that moving to a system of mandatory reimbursement could lead to customers taking less care when making payments due to an awareness of consumer protections. As our qualitative research shows, when consumers are scammed, it is not because they are acting irresponsibly - the way in which fraudsters manipulate normal, human behavioural biases makes it incredibly difficult for an individual to spot a scam in action and protect themselves from being scammed.<sup>16</sup> Therefore, the expectations of consumer behaviour to merit a refusal to reimburse must be based on a reasonable understanding of normal human behaviour and psychology.

Such theoretical claims are at odds with TSB's real-life experience of reimbursing 98% of authorised and unauthorised scam victims under its Fraud Refund Guarantee. TSB has been clear that it has not seen evidence of "additional moral hazard" nor any significant change in the amount of fraud being reported as a result of its reimbursement policy.<sup>17</sup>

### **Vulnerable consumers**

We strongly support the PSR's proposal that any consumer caution exception will not apply to vulnerable consumers. An individual should not be held responsible for making unwise decisions or not thinking clearly in a situation where it was incredibly difficult for them to do so. For this reason, though we oppose the proposed excess charge and minimum threshold, if the PSR were to proceed with these proposals, they should not apply to vulnerable consumers. We think it would be especially unfair on vulnerable victims for firms to withhold an excess of up to £35 from their reimbursement claims, and to deny them reimbursement for scam losses under £100, considering that under the PSR's proposals, there is a clear principle that vulnerable consumers should be reimbursed in all circumstances.

We support the use of the FCA definition to identify consumers vulnerable to APP scams. This could help improve consistency in reimbursement outcomes for consumers who may be "especially susceptible to harm." FCA guidance on vulnerability recognises that "all customers are at risk of becoming vulnerable," and that this risk is increased by characteristics of vulnerability, which can be driven by: health conditions or illnesses (health); low knowledge of, or confidence in, managing financial matters (capability); low ability to withstand financial or emotional shocks (resilience); or significant life events such as bereavement, job loss or

---

<sup>16</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

<sup>17</sup> House of Lords (Nov 2022) Fraud Act 2006 and Digital Fraud Committee, Report of Session 2022-23. Fighting Fraud: Breaking the Chain, p.116. Available at: <https://publications.parliament.uk/pa/ld5803/ldselect/ldfraudact/87/87.pdf>

relationship breakdown (life events).<sup>18</sup> Our research shows that as well as major life events, the accumulation of everyday stresses such as being busy at work, studying for exams or moving home can also push victims to their limits and impede their decision-making, making them more susceptible to APP scams.<sup>19</sup> With fraudsters often exploiting people in a distracted and vulnerable state, it is vital that PSP's consider a wider range of contextual factors when seeking to understand a consumer's behaviour, beyond those captured by the FCA's definition of vulnerability.

In using the FCA's definition, it is also important that we do not lose how vulnerability is set out under the current CRM Code. The LSB states that a customer is vulnerable to APP scams "if it would not be reasonable to expect that Customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered." It adds that "All Customers can be vulnerable to APP scams and vulnerability is dynamic," which may be due to "the personal circumstances of the Customer; the timing and nature of the APP scam itself; the capacity the Customer had to protect themselves; and the impact of the APP scam on that Customer."<sup>20</sup> Seeing that the way in which fraudsters manipulate normal behavioural and psychological biases can make it incredibly difficult for individuals to protect themselves and cope with the financial and emotional impact of fraud, it is likely to be even more difficult for victims who are especially vulnerable.<sup>21</sup> Firms should carefully understand their customer's circumstances and the context in which the APP scam took place when determining whether there is evidence of exceptional circumstances that would mean that a victim should not be reimbursed.

Further to this, all PSPs should train relevant staff on how to support victims of APP fraud. The LSB has previously found that among the ten signatory banks, it was not always clear that all staff who are impacted by the Code had received training.<sup>22</sup> Without proper training, vulnerable customers risk being overlooked and lacking the wider support needed to help them recover and to avoid becoming a victim again.

## Scope of reimbursement obligation

We strongly agree that the PSR's mandatory reimbursement obligation should apply to all types of APP scams. As the regulator acknowledges, significant consumer harms arise from all types of APP scam. Our qualitative research into the scam journeys of APP victims identifies

---

<sup>18</sup> FCA (Feb 2021) Guidance for firms on the fair treatment of vulnerable customers, pp.3, 9. Available at: <https://www.fca.org.uk/publication/finalised-guidance/fg21-1.pdf>.

<sup>19</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

<sup>20</sup> Lending Standards Board (April 2021) Contingent Reimbursement Model Code for Authorised Push Payment Scams, p.15. Available at:

<https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/04/CRM-Code-LSB-Final-April-2021.pdf>.

<sup>21</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

<sup>22</sup> Lending Standards Board (June 2021), Contingent Reimbursement Model Code for Authorised Push Payment Scams: Review of approach to reimbursement of customers, p.9. Available at:

<https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/06/CRM-Review-R21c-Follow-Up-Summary-Report.pdf>.



similarities in the methods used by fraudsters in impersonation, investment, romance, and purchase scams to manipulate victims into sending them money. Each of these different types involves a fraudster operating an account with a receiving PSP and typically exploiting the Faster Payments system.

Whilst the vast majority of reported APP scams take place via Faster Payments, according to UK Finance's data, fraudsters can change their approach to exploit gaps in protections across payment systems. Which? has previously called on the government to tackle this through setting out an industry-wide reimbursement obligation and liability regime in legislation, helping to ensure that any new or existing payment methods would be covered, but this approach was rejected. The PSR could, however, mitigate this issue by reconsidering how it introduced the reimbursement obligation. Other payment methods beyond Faster Payments are not currently in scope of the PSR's proposals for reimbursement because the PSR is proposing to direct Pay.UK. A PSR direction on PSPs would ensure that the reimbursement requirements can apply to CHAPS payments. We have also called on HM Treasury to review the consumer protections which apply to different payment methods, and consider whether the list of PSR-designated payment systems should be extended. Crucially, we would not want this wider work to slow down the urgent need to tackle reimbursement for APP scams via Faster Payments, where 98% of reported APP scams take place according to UK Finance figures.<sup>23</sup>

### **Thresholds and the excess charge**

We understand the case the PSR makes for a de minimis, however we oppose the proposal to allow PSPs to implement a minimum threshold for a reimbursement claim of up to £100. We are concerned that allowing firms to set a minimum threshold for claims could lead to a reduction in consumer protections with signatory PSPs, which since 2019 have committed to reimburse victims regardless of the value of losses as part of the CRM Code.

There is also potential for other issues as a result of a minimum threshold:

- A de minimis could potentially discourage some victims from reporting APP scam losses under £100, as consumers may be aware that they will not be able to be reimbursed for their losses under the mandatory reimbursement obligation.
- Repeat victims of APP scams, who are making payments below £100 in response to multiple different scams, may not qualify for reimbursement under this proposal.
- There is a potential for consumer confusion if all the payment service providers a consumer uses have varying minimum threshold levels under £100.

It is important to recognise that scam losses of any value can cause significant financial and emotional distress for consumers, including losses under £100. Recent research from the Money and Pensions Service found that a quarter of UK adults have less than £100 to put away in

---

<sup>23</sup> UK Finance (2022) 2022 Half year fraud update, p.35. Available at: <https://www.ukfinance.org.uk/system/files/2022-10/Half%20year%20fraud%20update%202022.pdf>.

savings.<sup>24</sup> Allowing victims to claim for APP scam losses of any amount would be a significant development in consumer protections. If the PSR does move forward with its proposal for a minimum threshold, there is a need for research and an evaluation on its effect, especially on the reporting of APP scams and reimbursement rates for lower value scams.

We support the PSR's decision to not have a maximum threshold on claims. This would ensure that APP scam victims who have lost substantial and often life-changing amounts of money to a fraudster are able to be reimbursed under the new requirements in all but exceptional circumstances. We note that the Financial Ombudsman Service sets limits on compensation for financial losses, depending on when the case was brought to them: for complaints referred to the Ombudsman on or after 1 April 2022, the limit is £375,000.<sup>25</sup> Given this, the FCA should ensure through an applicable policy statement that any APP scam cases going to the Ombudsman, either for appeal or after the time limit set on claims for mandatory reimbursement has expired, comply with the PSR's proposal to not have a maximum threshold on claims.

We oppose the PSR's proposal to allow PSPs to withhold an excess of no more than £35 from the reimbursement claim amount received by the scam victim. This fixed excess figure is in no way proportional to the value stolen from the victim, and is a significant amount to withhold from reimbursement payments, especially for claims of a lower value. Also, considering that the sending PSP would have already gone through the process of investigating the scam, it is not clear how reducing what the victim is entitled to will have any meaningful impact on costs for PSPs.

## Timings

Under the CRM Code, signatories are required to make a decision as to whether or not to reimburse a scam victim 'without undue delay', which should be no later than 15 business days after the day the victim reports the APP scam, or 35 days in exceptional cases. Once a decision has been made, the sending PSP should reimburse the victim without delay.<sup>26</sup>

The PSR's proposal to reduce this timeframe to just 48 hours is positive for some scam victims. We know that many victims may suffer both financially and emotionally as a result of being scammed, and a delay to reimbursement can leave some individuals in a position of financial difficulty.<sup>27</sup> Therefore, requiring the sending PSP to reimburse the victim as soon as possible

---

<sup>24</sup> Money and Pensions Service (Nov 2022) One in six UK adults have no savings. Available at: <https://moneyandpensionsservice.org.uk/2022/11/07/one-in-six-uk-adults-have-no-savings/>.

<sup>25</sup> Financial Ombudsman Service (June 2022) Compensation. Available at: <https://www.financial-ombudsman.org.uk/consumers/expect/compensation>.

<sup>26</sup> Lending Standards Board (April 2021) Contingent Reimbursement Model Code for Authorised Push Payment Scams, p.16. Available at: <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/04/CRM-Code-LSB-Final-April-2021.pdf>.

<sup>27</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

may help alleviate some of the pressures scam victims may feel while waiting for their money back.

However, PSPs may need more time than 48 hours to make fair, informed decisions, particularly for more complex cases and cases regarding vulnerable consumers. This could run the risk of PSPs making poor reimbursement decisions, and could lead to more consumers taking their case to the Financial Ombudsman Service for appeal. Given that the median time taken to convert all cases to closing is currently six months,<sup>28</sup> and is often longer for fraud cases, this is a significant amount of time for victims to wait on a reimbursement decision and can exacerbate the emotional and psychological distress they may feel. Hence, it is vital that firms are making fair and consistent decisions initially and have sufficient time to do so.

It may also be distressing for victims to have to delve into the details of the scam so soon after it has happened. Our research shows that dealing with the bank and other institutions in the aftermath of being scammed can often cause victims further distress, with some feeling confused, disheartened and upset with the process.<sup>29</sup> Some victims may therefore need more time to process the scam before being questioned by their bank on the specific details.

Under the PSR's current proposals, victims would have 13 months from the final payment involved in the APP scam to claim for mandatory reimbursement, after which they would have to take their case to the Ombudsman. However, some APP scam victims will not be aware that they have been scammed until days, weeks or even months after making the final payment to the fraudster. For this reason, the PSR should implement a general limitation period of six years after the victim becomes aware that they have been scammed. This timeframe would be in line with Section 75 protections under the Consumer Credit Act.

### **Allocation of reimbursement costs**

We support the PSR's proposal to allocate the costs of reimbursement equally between sending and receiving PSPs with a default 50:50 split. This is a fair starting point, but the allocation could evolve based on evidence of where the risk of fraud is greatest. For example, if there is evidence to show that receiving PSPs, in general, or an individual PSP is more likely to be used by fraudsters to commit APP fraud, a higher rate could be applied.

In principle, both sending and receiving firms should be contributing to reimbursement, given how integral both payment providers are to the APP scam taking place and the responsibility that the sending PSP owes to its customer. But, at present, sending firms are primarily responsible for reimbursing victims for APP losses, meaning there is little financial incentive on receiving firms to prevent fraud. The CRM Code does state that where signatories have both breached the standards that firms should meet, each should contribute 50% of the cost of

---

<sup>28</sup> Financial Ombudsman Service (Dec 2021) Plans and Budget 2022-23 consultation, p.13. Available at: <https://www.financial-ombudsman.org.uk/files/320493/plans-and-budget-consultation-2022-23.pdf>.

<sup>29</sup> Which? (Dec 2022) The psychology of scams: Understanding why consumers fall for APP scams.

reimbursement.<sup>30</sup> But due to the voluntary nature of the Code and a lack of enforcement, receiving banks often refuse to pay in practice. With regulatory enforcement, a 50:50 split will provide stronger financial incentives for receiving firms involved in scams to better detect and prevent APP fraud.

With regards to a dispute management process, we are concerned that firms may be hesitant to come to a shared decision on the allocation of reimbursement costs, especially if the split leans more towards the receiving firm. Crucially, any deliberation on allocation must not in any way delay reimbursement for consumers.

We do not think the PSR's proposal to allocate the costs of reimbursement equally between sending and receiving PSP's with a default 50:50 split is appropriate in the context of multigenerational scams. Multigenerational scams typically involve a fraudster persuading a victim to move money to another account the victim holds with a different PSP, or to a newly opened account in their name, before persuading the victim to transfer the money into an account under the fraudster's control. This account could be held by a PSP or be a different type of account, such as that held with a crypto platform.

As these scams can often involve several payees, PSPs and payment methods, it would be unfair for the sending PSP to be primarily responsible for reimbursing losses. It would be difficult to split this cost with the firm that receives the final payment, especially if the payment journey involves several PSPs. The issue of multigenerational scams needs to be addressed through bringing the other payment methods used in these types of scams under a reimbursement obligation. As explained, we have called on the Government to conduct a broader review of fraud protections and consider whether the list of designated payment systems should be extended, and for the PSR to work with other relevant regulators to address fraud through different payment systems.

## About Which?

Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers to make change happen. We fund our work mainly through member subscriptions, we're not influenced by third parties and we buy all the products that we test.

**For more information, contact [REDACTED] Policy Adviser**  
[REDACTED]

**December 2022**

---

<sup>30</sup> Lending Standards Board (April 2021) Contingent Reimbursement Model Code for Authorised Push Payment Scams, p.17. Available at: <https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/04/CRM-Code-LSB-Final-April-2021.pdf>.

PUB REF: CP22/4 Submissions

© The Payment Systems Regulator Limited 2023

12 Endeavour Square

London E20 1JN

Telephone: 0300 456 3677

Website: [www.psr.org.uk](http://www.psr.org.uk)

All rights reserved