PSR Payment Systems Regulator

Authorised push payment (APP) scams

Call for views

February 2021

CP21/3

If you would like to provide comments, please send these to us by **5pm on 8 April 2021**.

You can email your comments to **appscams.callforviews@psr.org.uk** or write to us at:

APP scams team
Payment Systems Regulator
12 Endeavour Square
London E20 1JN

We will consider your comments when preparing our response to this call for views.

We will make all non-confidential responses to this call for views available for public inspection.

We will not regard a standard confidentiality statement in an email message as a request for non-disclosure. If you want to claim commercial confidentiality over specific items in your response, you must identify those specific items which you claim to be commercially confidential. We may nonetheless be required to disclose all responses which include information marked as confidential in order to meet legal obligations, in particular if we are asked to disclose a confidential response under the Freedom of Information Act 2000. We will endeavour to consult you if we receive such a request. Any decision we make not to disclose a response can be reviewed by the Information Commissioner and the Information Rights Tribunal.

You can download this call for views from our website:
https://psr.org.uk/publications/consultations/cp21-3-authorised-push-payment-scams-call-for-views/

We take our data protection responsibilities seriously and will process any personal data that you provide to us in accordance with the Data Protection Act 2018, the General Data Protection Regulation and our PSR Data Privacy Policy. For more information on how and why we process your personal data, and your rights in respect of the personal data that you provide to us, please see our website privacy policy, available here: https://www.psr.org.uk/privacy-notice

Contents

1 Executive summary

1.1 An Authorised Push Payment (APP) scam occurs when someone is tricked into making a payment to a fraudster. These scams can have a devastating impact on victims. Reported APP scam losses from the first half of 2020 totalled £208 million, with the actual figure including unreported losses likely to be much higher.

1.2 Our aim is to deter APP scams from happening in the first place, and to reduce significantly the size of losses incurred by payment system users (customers) when they do. We have drafted three complementary measures that could help do this. We are seeking views on their viability, effectiveness and proportionality, and we want to engage with stakeholders on whether and how they should be implemented. We also remain interested in any other proposals to reduce fraud and improve the protections given to victims.

1.3 To date, we have advocated industry-led approaches to combating APP scams, partially due to statutory restrictions in the Payment Services Regulations 2017 (PSRs 2017) which implement the European Union's (EU) Second Payment Services Directive (PSD2) into UK law. The end of the UK's transition from the EU could provide the opportunity to pursue some measures where previously we could not, if legislative changes are made to the PSRs 2017.

1.4 The industry-led approach resulted in the Contingent Reimbursement Model Code (the CRM Code). Since May 2019, the CRM Code has been a key tool aimed at preventing APP scams and protecting victims via repatriation (i.e. fund recovery) or reimbursement (i.e. where the victim's payment service provider (PSP) covers the loss) where the victim's PSP has signed up to the CRM Code.

1.5 Though the CRM Code has improved outcomes for customers, our analysis suggests that its application hasn't yet led to the significant reduction in APP scam losses incurred by customers that is needed. We estimate the overall level of reimbursement and repatriation is less than 50% of APP losses assessed under the CRM Code. This figure also varies considerably across signatory PSPs.

1.6 This means customers are still bearing a high proportion of losses, despite the default requirement in the CRM Code being that customers should be reimbursed where they have acted appropriately.

1.7 Some PSPs are of the view that the exceptions to the reimbursement obligation in the CRM Code are open to interpretation, or difficult to apply in practice. This lack of clarity on how the CRM Code rules should be applied by PSPs appears to increase the role of the Financial Ombudsman Service (the Ombudsman) in adjudicating disputes. This issue of interpretation of the CRM Code is reflected in the thematic review of warnings given by PSPs to customers, published by the Lending Standards Board (LSB) in December 2020.[1] We are interested to hear stakeholder views on the nature and scale of any issues with the CRM Code.

1 https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/12/Thematic-review-of-Effective-Warnings-1.pdf

1.8 A further issue is that many customers fall outside the protections offered by the CRM Code, as it is not a requirement that PSPs participate, and non-participating PSPs are under no general requirement to refund their customers when they have done nothing wrong. Nonetheless, PSPs who are not CRM Code signatories can still reimburse their customers, and we note that some have made public commitments to do so either at CRM Code standards or an even higher standard than that of the CRM Code.

1.9 We want to move toward solutions. We acknowledge that the LSB has recently published a full review of the CRM Code[2], with recommendations on how the CRM Code's functioning could be improved. This work should continue. However, the issues that require action include a number that fall outside of the scope of the CRM Code.

1.10 Reflecting this, we set out in this paper three measures that we believe could help prevent APP scams and protect customers who do fall victim. These are, for Faster Payments and Bacs Direct Credit:

1. Improving transparency on outcomes, by requiring PSPs to publish their APP scam, reimbursement and repatriation levels.
2. Greater collaboration to share information about suspect transactions, by requiring PSPs to adopt a standardised approach to risk-rating transactions and to share the risk scores with other PSPs involved in the transaction.
3. Introducing mandatory protection of customers, by changing industry rules so that all payment firms are required to reimburse victims of APP scams who have acted appropriately.

1.11 We welcome your feedback on these measures, how they should be developed, and any additional options that should be explored. In assessing our next steps on APP scams, we are particularly mindful of our statutory objective to ensure that the operation and development of payment systems takes account of the interests of those who use (or may use) their services, but also the general principle that those who use services provided by payment systems should take responsibility for their decisions.[3]

1.12 We invite your views by 5pm on 8 April 2021.

2 https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/01/LSB-review-of-the-CRM-Code-FINAL-January-2021-.pdf

3 We have a duty to take into account the general principle that those who use services provided by payment systems should take responsibility for their decisions, under section 53 of the Financial Services (Banking Reform) Act (FSBRA).

2 Introduction

An APP scam occurs when someone is tricked into making a payment to a fraudster. These scams can have a devastating impact on victims. In the first half of 2020, losses due to APP scams totalled £208 million.[4]

Our aim is to try to prevent scams from happening in the first place, and to reduce significantly the harm to victims, including when they face the cost of those APP scams.

To date, we have primarily relied on advocating industry-led approaches to combatting APP scams, partially due to statutory restrictions in the PSRs 2017 which implement the EU's PSD2 into UK law. The end of the UK's transition from the EU could provide the opportunity to pursue some measures where previously we could not, if legislative changes are made to the PSRs 2017.

Since May 2019, the industry-led CRM Code has been a key tool aimed at preventing APP scams and protecting victims.

What is a push payment?

2.1 A push payment occurs when a payer instructs their PSP to send funds to a payee's account. Push payments are typically made via the following:

- **Faster Payments:** The UK's real-time, retail payments system. Customers can make single immediate payments, forward-dated payments or initiate standing orders through several channels including mobile, internet and telephone banking.
- **CHAPS:** The UK's same-day high-value payment system. For customers, it is generally used to make domestic property purchases.
- **Bacs (Direct Credit):** Primarily used to pay wages, salaries, or benefits, as well as for settling business-to-business invoices.
- **'On-us':** Payments where the payer's PSP and the payee's PSP are the same (or members of the same group) and the payment is executed using the PSP's internal system.[5] (Also known as 'internal book transfers'.)
- **International payment systems:** Payments made from accounts at UK PSPs to PSPs outside the UK.

4 This figure is likely to be an underestimate, as people can sometimes be unwilling to report losses due to scams or can sometimes be unaware that a scam has taken place. The real figure for losses to APP scams is therefore likely to be higher.

5 It may be that some PSPs that form part of the same group do not make 'on-us' transactions directly between themselves but may use systems such as Bacs and Faster Payments for these, possibly as a legacy from before their common ownership. In this paper, we use 'on us' transaction only for payments not made over a PSR-regulated payment system.

What is an APP scam?

2.2 An APP scam occurs when someone is tricked into making a push payment to a fraudster. There are eight main types of APP scam:

1. **Purchase scam:** The victim pays in advance for goods or services that are never received.
2. **Investment scam:** A scammer convinces their victim to move their money to a fictitious fund or to pay for a fake investment.
3. **Romance scam:** The victim is persuaded to make a payment to a person they have met, often online through social media or dating websites, and with whom they believe they are in a relationship.
4. **Advance fee scam:** A scammer convinces their victim to pay a fee which they claim would result in the release of a much larger payment or high value goods.
5. **Invoice and mandate scam:** The victim attempts to pay an invoice to a legitimate payee, but the scammer intervenes to convince the victim to redirect the payment to an account they control.
6. **CEO fraud:** A scammer manages to impersonate the CEO or other high-ranking official of the victim's organisation to convince the victim to make an urgent payment to the scammer's account.
7. **Impersonation – police/bank staff:** A scammer contacts the victim purporting to be from either the police or the victim's bank and convinces the victim to make a payment to an account they control.
8. **Impersonation – other:** A scammer claims to represent an organisation such as a utility company, communications service provider or government department.

2.3 Once the victim has sent the money to the scammer's account, the scammer will often quickly transfer it onward to numerous other accounts, making it difficult to trace and recover. Scammers will also often move the money out of the UK.

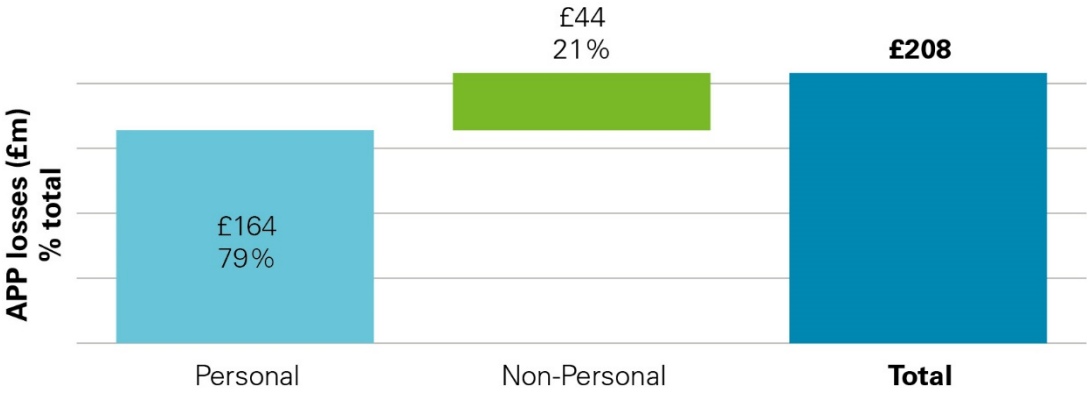
2.4 In contrast to victims of unauthorised transactions – where an account is hacked or security information stolen – under existing arrangements, victims of APP scams have no statutory protection.

2.5 APP scams can have a devastating impact on victims. Furthermore, with fraudsters adopting sophisticated techniques to manipulate behaviour, anyone can become a victim. The impact often isn't just financial, with victims also facing other negative impacts, such as the distress and anxiety of being scammed.

How large is the APP scam problem?

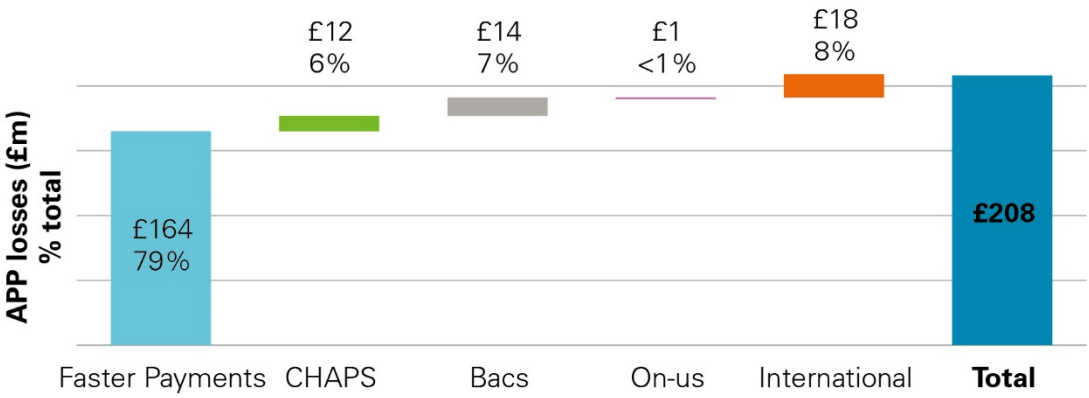
2.6 Reported losses due to APP scams were £208 million in the first half of 2020. This was split between personal (£164 million) and non-personal (£44 million) accounts.[6]

Figure 1: APP losses in H1 2020



Most APP scams occur over Faster Payments. In the first half of 2020, £164 million (79%) of the £208 million in total reported APP losses occurred over Faster Payments.

Figure 2: APP losses in H1 2020 by payment system



What do we want to achieve?

2.7 Our aim is both protecting customers from harm if they fall victim to an APP scam and preventing these scams from occurring in the first place. This aim is, of course, in the context of the legal requirement of consumers needing to take responsibility for their actions[7], and the need for them to be educated about the dangers of scams and take appropriate care to avoid being scammed. We have an objective to ensure that payment systems are operated and developed in a way that takes account of, and promotes, the interests of those who use, or are likely to use, services provided by payment systems. In discharging our functions, we are also required to have regard, among other things,

6 UK Finance – Half-year Fraud Update 2020: https://www.ukfinance.org.uk/system/files/Half-year-fraud-update-2020-FINAL.pdf

7 Under 49(3)(c) FSBRA, the PSR, in discharging its general functions relating to payment systems, must have regard to the regulatory principles in section 53, including 53(f), which states that that those who use services provided by payment systems should take responsibility for their decisions.

to the general principle that those who use services provided by payment systems should take responsibility for their decisions.

2.8 Our focus in this paper is on Faster Payments and Bacs Direct Credit. These payment systems account for 86% of APP scam losses. Certain types of payment transaction used for push payments are not considered in this paper because:

- our powers do not extend to the Bank of England as the operator of the CHAPS system
- internal book transfers that take place within the same PSP or group of PSPs (referred to as 'on-us' in this paper) do not occur over a regulated payment system (they occur within a PSP or between members of the same group)
- our regulation of UK payment systems does not include the cross-border element of any international payments and, in many cases, cross-border payments do not go across any UK payment systems at all and are moved entirely through correspondent networks

2.9 Also addressing the issue of **protecting customers from harm**, the PSR currently has a separate call for views open that considers consumer protection in interbank payment systems more generally.[8] The aim of this work is to understand how consumers might be harmed by a lack of adequate consumer protection in interbank payment systems, including considerations on what level of governance is required to deliver effective consumer protection.

Why are we calling for views now?

2.10 While the CRM Code has improved customer outcomes, our analysis (presented in Chapter 2) suggests its application hasn't led to the significant reduction in APP scam losses incurred by customers that we believe is needed. At our March 2020 roundtable, we called on the industry to improve customer outcomes, and said that the PSR would look to take action if outcomes did not improve.[9]

2.11 Given the evidence we have seen on CRM Code outcomes, we have now reached a point where it would be valuable to get stakeholder views on that evidence and potential PSR measures that we think could prevent APP scams and protect those who fall victim. We acknowledge that the LSB has recently published a review of the CRM Code, and we support the continuation of that work. But many customers fall outside of the protections offered by the CRM Code, as it is not a requirement that PSPs participate, and non-participating PSPs are under no general requirement to refund their customers when they have done nothing wrong.

2.12 In addition, following the end of the UK's transition from the EU, in future it may become possible for the PSR to pursue some measures that are currently prevented by requirements arising originally from EC Law (and codified in UK law in the PSRs 2017). PSD2, implemented in the UK by the PSRs 2017, has played a key role in limiting

8 https://psr.org.uk/publications/consultations/cp21-4-consumer-protection-in-interbank-payments-call-for-views/

9 https://www.psr.org.uk/publications/general/authorised-push-payment-app-scams-conference-call-30-march-2020/

our actions to date with respect to APP scams. It has affected our ability to require PSPs to reimburse APP scam victims who have acted appropriately.

2.13 At present, if a PSP has executed a transaction correctly – that is, processed the sort code and account number it was given by the customer correctly – then it is not liable to reimburse that customer for any resulting loss. The way that this obligation is included in UK law means public bodies in the UK cannot regulate to require PSPs to reimburse APP scam victims.

2.14 The PSRs 2017 continue to form part of UK law even though we have exited the EU. However, the government could legislate to remove the restrictions in the PSRs 2017. If this happened, it would mean the PSR could require reimbursement for APP scam victims provided it is effective and proportionate to do so. This is one of the measures we describe and ask for views on in this paper.

2.15 The current limitations on the PSR do not apply to all parties. Industry participants can take action, including by working to change the rules included in our payment systems. Reflecting this, steps to introduce mandatory reimbursement (Measure 3, described from paragraph 4.22 onwards) could still be progressed by industry, without legislative change.

2.16 However, this paper is not just about reimbursing APP scam victims, but also about how we enhance prevention efforts and protections for APP scam victims. The measures are discussed in Chapter 3. Before proceeding, we set out the background on the CRM Code.

What is the CRM Code?

2.17 In November 2017, the PSR consulted on whether a contingent reimbursement model should be developed. We proposed that the model set out the circumstances when PSPs are responsible for reimbursing APP scam victims who have acted appropriately. As well as offering better information and protection to customers, the intention was to establish stronger incentives for PSPs to prevent APP scams in the first place.

2.18 Following the consultation, we concluded that a CRM Code, developed collaboratively by industry and customer group representatives, would be an effective way to reduce the harm from APP scams.

2.19 We therefore established a steering group to develop the CRM Code, with the PSR providing support. In September 2018, the steering group consulted on the draft CRM Code, and in May 2019, the final CRM Code went into effect.

The CRM Code: A snapshot

An overarching principle of the CRM Code is that customers should be reimbursed where they have acted appropriately

1. The objectives of the CRM Code are:
    - to reduce the occurrence of APP scams
    - to increase the proportion of customers protected from the impact of APP scams, both through a reduction in APP scams and through reimbursement

- while minimising disruption to legitimate payment journeys

2. The CRM Code applies to payments made between GBP-denominated UK-domiciled accounts, over Faster Payments or CHAPS. It does not cover Bacs.
3. The CRM Code does not apply to unauthorised payments or buyer-seller disputes.
4. Sending firms should take reasonable steps to protect their customers from APP scams. Receiving firms should take reasonable steps to prevent accounts from being used to launder the proceeds of APP scams.
5. Subject to certain exceptions, when a customer has been the victim of an APP scam, firms should reimburse the customer. The exceptions are as follows:
   - The customer ignored effective warnings,
   - The customer ignored a clear negative Confirmation of Payee result – i.e. the name on the receiving account did not match the name entered by the payer (this exception is provisionally included in the CRM Code, although not yet operational)
   - The customer made the payment without a reasonable basis for believing that:
     - the payee was the person the customer was expecting to pay
     - the payment was for genuine goods or services
     - the person or business with whom they transacted was legitimate
   - 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
   - The customer has been grossly negligent for other reasons
6. Where the customer is identified as being vulnerable to an APP scam, they are not expected to protect themselves to the same standards. Vulnerability should be assessed on a case-by-case basis.

The CRM Code process

1. A customer who believes they have been the victim of an APP scam should tell their bank. The customer's PSP will try to trace their money, so the sooner they let the bank know, the more chance they have of getting it back.
2. If the customer's PSP is a member of the CRM Code, the PSP will then investigate whether they are entitled to reimbursement under the CRM Code. The PSP should normally let the customer know its decision within 15 business days (or up to 35 days in exceptional circumstances).
3. If the customer's PSP decides against reimbursement, the customer can lodge a complaint with the PSP. If the customer is not satisfied with the outcome of this complaint, or the PSP has delayed communicating their decision on the complaint[10], they can then lodge a complaint with the Financial Ombudsman Service.[11]

10 Beyond 15 business days after the day on which the customer reported the APP scam, unless exceptional circumstances apply.

11 In December 2018, the FCA extended the jurisdiction of the Ombudsman to include adjudicating complaints from APP scam victims about the actions or behaviour of the PSPs involved in their scam.

2.20 There are nine signatory PSPs to the CRM Code:

- Barclays
- HSBC (including HSBC, First Direct, and M&S Bank)
- Lloyds Banking Group (including Lloyds Bank, Halifax, Bank of Scotland, and Intelligent Finance)
- Metro Bank
- Nationwide
- RBS (including Royal Bank of Scotland, NatWest, and Ulster Bank)
- Santander (including Santander, Cahoot, and Carter Allen)
- Starling Bank
- The Co-operative Bank (joined in December 2019).

2.21 Through these signatories, the CRM Code covers more than 85% of transactions made over Faster Payments.[12] The CRM Code is governed by the LSB. The LSB is an industry-funded body that monitors and enforces the Standards of Lending Practice and makes sure registered firms provide a fair deal to their personal and business borrowing customers.

2.22 The next chapter looks at what's happened since the CRM Code came into effect and presents the issues we're seeing.

12 Figure from the LSB's Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams, January 2021.

3 The current framework

While the CRM Code has improved outcomes for customers, our analysis suggests that its application hasn't led to the significant reduction in APP scam losses incurred by customers that is needed. In addition, customer outcomes under the CRM Code appear to vary considerably across signatory PSPs. Some PSPs highlight that the exceptions to the reimbursement obligation in the CRM Code are open to interpretation and, as a result, difficult to apply consistently in practice. This is reflected in the LSB's thematic review findings and the Ombudsman feedback, outlined at our March roundtable. We would be interested in hearing views on the nature and scale of any issues with the CRM Code.

3.1 Before the CRM Code came into force in May 2019, reimbursement levels were significantly lower. In its recent Review of the CRM Code for Authorised Push Payment Scams, the LSB reported that the pre-CRM Code industry average was 19% by value in the first half of 2019.[13] Furthermore, there was no systematic protection for victims, and outcomes were uncertain and variable. In addition to the harm this caused victims, it also provided weak incentives for PSPs to work to prevent APP scams.

3.2 In light of this, the voluntary agreement by the signatories to the CRM Code was a major step forward, and we welcome the decision of those PSPs that have signed up or undertaken to provide an equivalent or additional standard of protection. It represented a substantial increase in the protection that customers were entitled to and set out standards for PSPs to improve fraud prevention and victim care.

3.3 The CRM Code seeks to allocate the costs of fraud between customers and PSPs in a way that should improve the incentives on PSPs to prevent fraud, while managing the risk that customers do not take sufficient responsibility. This is important, as those best placed to prevent APP scams need to have the incentive to do so. This includes PSPs, where they are well placed to act, and customers, where it is reasonable to expect them to take steps to prevent fraud.

3.4 This means PSPs reimbursing APP scam victims where they have acted appropriately or are vulnerable. Ideally, of course, scams would be prevented from occurring in the first place or PSPs would be able to recover funds from scammers.

13 https://www.lendingstandardsboard.org.uk/wp-content/uploads/2021/01/LSB-review-of-the-CRM-Code-FINAL-January-2021-.pdf page 20.

What has happened under the CRM Code?[14]

3.5 When an APP scam occurs, the following outcomes are possible under the CRM Code:

- All or some of the customer's funds are located and sent back (repatriation).
- The PSP(s) involved cover all or some of the customer's loss using their own funds (reimbursement).
- The customer bears the loss (either in full or in part due to partial repatriation/reimbursement).
- Following this, if the victim feels they have not been treated appropriately by the PSP they can lodge a complaint with the Financial Ombudsman Service. The Ombudsman will then either uphold the complaint, meaning it decides in favour of the customer, or not uphold the complaint.

Less than 50% of APP losses are repatriated or reimbursed

3.6 Since it came into effect on 28 May 2019, we have been monitoring outcomes under the CRM Code to understand whether it has been significantly reducing the APP scam losses incurred by customers. Our monitoring to date has made use of data provided to us by CRM Code signatories via UK Finance.

3.7 We have split the analysis into three time-segments: 28 May 2019 to 31 December 2019, 1 January 2020 to 30 June 2020, and 1 July 2020 to 31 December 2020.

28 May 2019 to 31 December 2019

3.8 As shown in Figure 3, in this period CRM Code signatories reimbursed and repatriated 41% of APP scam losses assessed under the CRM Code. That is, of £101 million assessed under the CRM Code in the period, £41 million was either reimbursed or repatriated.

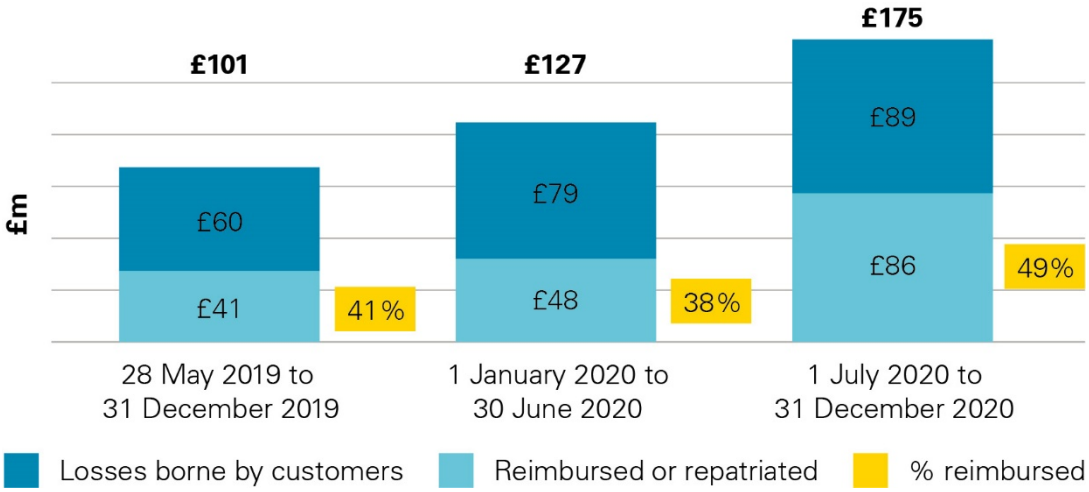
3.9 We understand the data for this period includes most repatriated funds but may not include a small percentage. CRM Code data is compiled on a monthly basis and repatriation efforts can sometimes extend beyond the month in which the APP scam took place.

3.10 The reporting template for this period didn't allow for delayed repatriation reporting. UK Finance addressed this issue in later periods. Based on our discussions with UK Finance and the reporting for later periods, we estimate that unaccounted for repatriation may constitute around 2–5% extra.

3.11 In the early part of this period, CRM Code signatories were embedding the CRM Code and associated data reporting into their systems. We therefore treated the insights from this period as tentative and looked to the following periods to supplement them.

14 The figures given in this section are the ones given to us by UK Finance as at 8 February 2021.

Figure 3: Reimbursement and repatriation under the CRM Code



Source: UK Finance.

1 January 2020 to 30 June 2020

3.12 In this period, the CRM Code was well embedded in PSP operations. As shown in Figure 3, Code signatories reimbursed and repatriated 38% of APP scam losses assessed under the Code between 1 January 2020 and 30 June 2020. That is, of £127 million assessed under the CRM Code in the period, £48 million was either reimbursed or repatriated. Much like the previous period, we understand this figure includes most repatriation, but there could be around 2–5% in addition.

3.13 It's clear that reimbursement and repatriation occurring under the CRM Code did not change significantly from the previous period, adding weight to the validity of the insights from the previous period.

1 July 2020 to 31 December 2020

3.14 Given the issue with delayed repatriation reporting in the previous periods, UK Finance amended the CRM Code reporting requirements to make sure all repatriation was captured. The change took effect from 1 July 2020. As shown in Figure 3, in the period from 1 July to 31 December 2020, 49% of APP scam losses (£86 million of £175 million) were reimbursed or repatriated, in line with the previous periods.

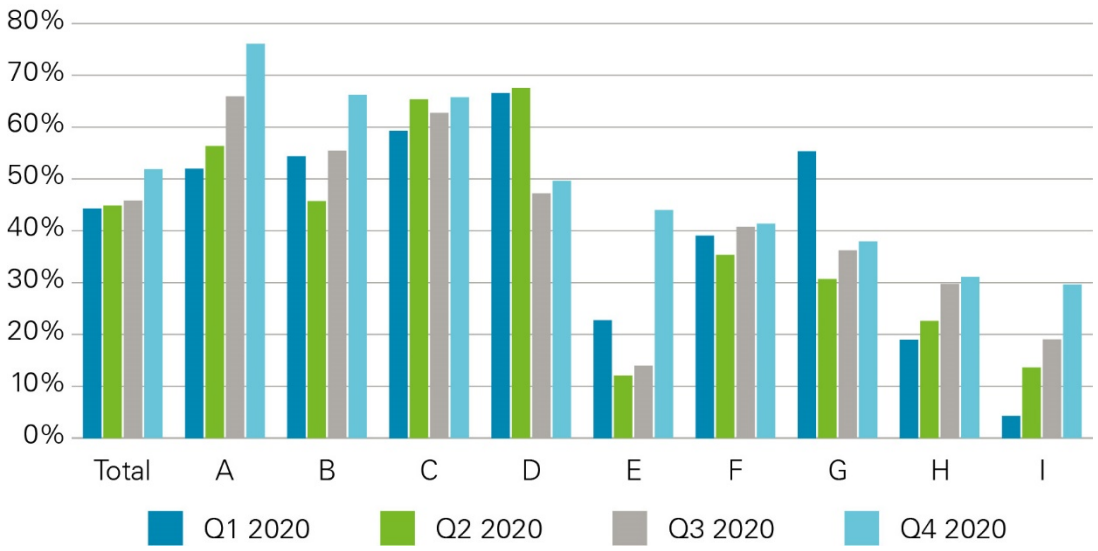
3.15 There appears to have been some improvement in outcomes for customers of a number of CRM Code signatories in Q4 of 2020. This has resulted in an increase for the average across all signatories. Notwithstanding this, the recent improvement is still far from the levels we would expect to see reimbursed, and there remains considerable variation between PSPs (see paragraph 3.17 and Figure 4 below).

Outcomes vary considerably across signatories

3.16 In addition to low levels, our analysis suggests that reimbursement and repatriation vary considerably across signatory PSPs. As shown in Figure 4, in Q4 2020, we estimate that across signatories the rate of reimbursement and repatriation ranged from around 30% to 76% of APP losses assessed under the CRM Code. Large disparities were also reflected in previous quarters, and the resulting averages for the year ranged from 18% to 64%.

3.17 The range of reimbursement rates across signatories is wide and appears persistent. We are not aware of any PSP-specific factors that explain why there should be such a variation in reimbursement rates, although it is still open to PSPs to explain this difference. It also isn't clear why other PSPs are failing to reach the reimbursement levels of the highest reimbursing PSPs. This strongly suggests that there are problems with reimbursement at a PSP level (and which are reflected in the average reimbursement rates). Ultimately, this means that the experience and outcome for APP scam victims will depend on who they bank with.

Figure 4: Reimbursement rates (%). Ranked on Q4 2020.



Source: UK Finance.[15]

Data quality

3.18 Lastly, the data produced by the CRM Code signatories does not appear to be of a highly reliable quality, and is often subject to revision, especially on the levels of reimbursement. We acknowledge that this is a difficult area in which to establish good quality data. However, it is important to improve this overall quality, so as to inform our ongoing efforts to address the underlying issues

Our conclusion

3.19 While the CRM Code has improved outcomes for customers, we estimate that less than 50% of losses assessed under the CRM Code are reimbursed or repatriated. There are number of reasons why these levels of reimbursement are of concern:

- There are high numbers of cases where a victim's PSP has refused to reimburse them, and the decision has been overturned on appeal to the Financial Ombudsman. Although Ombudsman decisions are not a direct measure of the operation of the CRM Code, this could suggest that there may be issues in the way the Code is

15 Note: We identified small differences in the results of two PSPs, which we were unable to resolve before publication. Where there was uncertainty, we have presented the upper limit of the range, giving rise to the highest possible reimbursement rates. For one difference, we were unsure as to which quarter it arose in. We have assumed it to have arisen in the most recent quarter, Quarter 4 2020.

being applied by PSPs. For their part, some PSPs have expressed concerns about whether Ombudsman decisions are consistent with the principles of the CRM Code.

- One of the default requirements in the CRM Code is that when a PSP's customer has been the victim of an APP scam, they should be reimbursed by the PSP if they have acted appropriately. On the evidence we have seen, it seems unlikely that victims will have acted irresponsibly in more than 50% of APP scam cases, with the correct application of the provisions of the CRM Code (for example, giving adequate and targeted warnings) having been insufficient to prevent a scam taking place.
- If liability for an APP scam falls on the party that is best able to prevent the scam (thereby impacting incentives to do so) the overall levels of successful scams are likely to be reduced. PSPs often have much more information in this respect, and liability could better reflect this.
- In addition, consideration of which party is best placed to weather the loss, where a scam was not prevented, is important. Without diminishing the importance of the personal responsibility of consumers, it should be considered whether the current balance of APP scams costs implied in the reimbursement figures is appropriate. In general terms, these costs can either fall on an individual – with the harm that this implies to that individual – or can fall on the individual's PSP (albeit that the cost would then be passed on to consumers in a way that spreads it across the PSP's consumer base).
- As well as relatively low levels of reimbursement, there appears to be a wide variation in these levels across CRM Code signatories. Given that the customer bases of the signatories are broadly similar, this may suggest the variance arises from the application of the CRM Code. It could be that there are features of the CRM Code that lend themselves to such variable application. It is also possible that the exceptions to the default obligation to reimburse are open to inappropriate variation in their interpretation by PSPs.

3.20 There is also the possibility that variable reimbursement rates may result from differing strengths of fraud prevention measures across banks, with some relatively unprotected banks simply making more reimbursement payments as a result. By the same token, a bank may be good at stopping fraud and have a low reimbursement rate, as those scams that do succeed are down to customer recklessness. There does not, however, seem to be a close correlation in the data between APP scam loss values and the proportion reimbursed.

3.21 The evidence suggests the CRM Code does not yet go far enough in achieving the aim of significantly reducing APP scam losses incurred by customers. Customers are still bearing a large proportion (the majority) of APP losses. We would be interested in receiving stakeholder views on the data we have presented and any supplementary information on customer outcomes under the CRM Code.

Question 1: **Do you have any comments on the data presented above? Do you have any supplementary information on customer outcomes under the CRM Code?**

Question 2: **Do you have any comments on the appropriate balance of liability for APP scams costs between individuals and PSPs?**

What is driving these outcomes?

3.22 Our assessment of the CRM Code indicates there are issues with how some CRM Code provisions are being interpreted and applied, hampering positive outcomes. In this section, we start by identifying the positive elements of the CRM Code, before moving on to an assessment of the provisions that are not working well.

The CRM Code has had a positive impact

3.23 We recognise that the CRM Code contains useful provisions, which constitute good practice. It sets minimum standards for firms to raise awareness and educate customers about APP scams. It also requires firms to collect and provide industry statistics and maintain policies and procedures to help customers with aftercare.

3.24 The CRM Code accounts for vulnerability, setting minimum standards for firms to identify and support customers deemed vulnerable to APP scams.

3.25 There are also standards for fraud prevention. Sending PSPs need to maintain procedures to detect, prevent and respond to APP scams. Receiving PSPs need to maintain procedures to prevent, detect and respond to accounts being used to receive the proceeds of APP scams.

It also has significant issues

3.26 Despite the positive elements of the CRM Code, the data, as we discussed above, suggests that reimbursement rates are variable, and arguably too low overall. One plausible explanation for this lies in the exemptions to reimbursement, some of which are arguably too open to interpretation by PSPs.

3.27 The CRM Code provides five exceptions to the obligation to reimburse. While these were intended to reflect a broad range of circumstances, the way these exemptions are applied in many cases arguably results in cases where signatories wrongly refuse to reimburse or where the Ombudsman overturns a decision where the signatory had correctly interpreted the exception as applying in the circumstances.

3.28 The lack of clarity on how the CRM Code exceptions should be applied (particularly those highlighted by the LSB's review as described below) not only makes it difficult for the PSPs to apply them consistently, but also increases the role of the Ombudsman in adjudicating disputes. This has, in turn, led to cases in which PSPs and consumers state that they are unable to understand why the Ombudsman has ruled in a certain way, in relation to the CRM Code exemptions.

3.29 The LSB's thematic review published in April 2020, indicates that, of the five exceptions to reimbursement, there have been issues with PSPs applying these three:

1. **The customer ignored effective warnings given by the sending PSP. The CRM Code says an effective warning at a minimum must be:**
    - understandable – in plain language, intelligible and meaningful to the customer
    - clear – in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses

- impactful – positively affects customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced; steps should be taken to ensure that the customer can reasonably understand the consequences of continuing with an irrevocable payment
- timely – given at points in the payment journey most likely to have impact on the customer's decision-making
- specific – tailored to the customer type and the APP scam risk identified by analytics during the payment journey, and/or during contact with the customer

3.30 Though there are minimum criteria, there is room for different interpretations of what constitutes an effective warning. This is reflected in the LSB's thematic review (December 2020)[16] and the Financial Ombudsman feedback outlined in our March roundtable. The LSB review found, among other things, that the content of the warnings provided by all nine signatory firms required further development, and that often warnings weren't present at all in payment journeys. It may be the case that insufficiently specific or inconsistently applied warnings can lead to them becoming ineffective. There was also found to be a lack of quality assurance and process formalisation at some firms, which could lead to inconsistent and substandard outcomes. If firms have varying views about what constitutes an effective warning, they are highly like to have varying views about when the above exception applies.

3.31 For their part, a number of PSPs have raised concerns that they are providing what they consider to be 'effective warnings' but that when customers do not respond to them, they are still being held liable for the resulting losses.

2. **The customer made the payment without a reasonable basis for believing that:**
   - the payee was the person the customer was expecting to pay
   - the payment was for genuine goods or services
   - the person or business with whom they transacted was legitimate

3.32 While a sound concept, the reasonable basis exception is arguably difficult to apply in practice. There is often no obvious way of linking the circumstances of an APP scam to the beliefs of a customer over the legitimacy of the payee. Reasonableness is also inherently open to interpretation and so this is one explanation for variability between PSPs, but we would welcome views on this.

3. **The customer has been grossly negligent for other reasons.**

3.33 There is no standard definition of gross negligence in this context. It is left up to PSPs to apply the exception, meaning there is broad scope for different interpretations by different PSPs. Again, this is one very likely explanation for variability between PSPs, and we would welcome views on this.

3.34 The available analysis suggests the CRM Code, in its current form, is not going far enough to reduce APP scam losses incurred by customers because the exceptions to reimbursement are open to interpretation by PSPs or difficult to apply in practice.

16 https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/12/Thematic-review-of-Effective-Warnings-1.pdf

3.35 Notwithstanding our analysis of the situation as set out here, it is important to highlight that we are not advocating that victims of APP scams should be absolved from the responsibility for their decisions, only that the provisions of any code prescribing the circumstances in which victims may be said not to have acted responsibly may be too broad and open to a variety of interpretations.[17]

Question 3: **Do you have any comments on our analysis of what is driving the Code outcomes we're seeing?**

Question 4: **What could be done to ensure consistency in the outcomes of dispute resolution, and to give customers and industry transparency about how these outcomes are arrived at?**

What are the other issues relating to APP scams?

The CRM Code only protects customers of signatories

3.36 While the nine current CRM Code PSPs cover most payment transactions, the Code does not protect customers of non-signatories, which are primarily smaller PSPs. Broadening participation in a clearly set-out scheme for reimbursement will improve outcomes for APP scam victims[18], and complement initiatives by other PSPs to deliver protection that is equivalent to or higher than the CRM Code.

3.37 Some of these PSPs have said there are provisions in the Code that act as a barrier to participation. For example, there are service-level requirements related to Code participation that some smaller PSPs would find difficult to abide by, such as a requirement to have a 24-hour helpline.

Funding for reimbursement of some cases has been in question

3.38 There are cases for which some Code signatories have suggested they will stop reimbursing, despite the victim having done nothing wrong. We would be extremely disappointed if this happened. The CRM Code states that APP scam victims should be reimbursed unless a specified exemption applies. In broad terms, APP scam victims that have acted reasonably should therefore be reimbursed. This includes cases in which neither the victim nor the bank involved has acted incorrectly according to the CRM Code ('no-blame' cases). Such cases deserve no less certainty of reimbursement for the victims than any other cases, and to act as if there is any less commitment on the part of PSPs to their funding is against this principle of the CRM Code.

17 One of the general principles that the PSR must have regard to (under s49(3)(c) FSBRA) in discharging its general functions relating to payment systems, which is that those who use services provided by payment systems should take responsibility for their decisions (s53(d)).

18 This is also reflected in the LSB's review of the CRM Code, which states that the CRM Code 'should recognise the wider range of participants within the payments industry while ensuring that it retains a consistent approach to the standards of protections provided'.

3.39 PSPs are entitled to decide how they fund payments in these circumstances, whether that is by themselves (as with all other reimbursements) or through some shared fund (provided competition law is not breached). The LSB does not make becoming a signatory to the Code contingent on signing up to any such fund. Notwithstanding this, there should not be any other requirements on CRM Code joiners – for example, to put in place any technical connectivity necessary for interaction with such a fund – by anybody related to the functioning of that fund, as part of the CRM onboarding process. Any such requirement would create an unnecessary administrative burden and barrier to joining, which could ultimately reduce the Code's coverage.

3.40 In addition, the fact that Code PSPs have the option to self-fund these cases, rather than make use of the shared fund, has still not been written into the CRM Code. This means potential signatories face uncertainty about funding options if they are considering joining the Code.[19]

3.41 Our view is that only the LSB, as the CRM Code's governing body, should be involved in onboarding signatories. There should be no requirement to sign up to any shared fund as part of joining the CRM Code, and this should be made explicit in the CRM Code and clear to potential members. This should be addressed urgently.

Question 5: **Are there any other issues with the CRM Code you would like to tell us about?**

What have we done to prompt industry to improve the current framework?

3.42 Over the last year, we have pursued several approaches to prompt industry to improve outcomes for customers, address concerns around broadening CRM Code participation, and commit to funding all cases where victims have acted reasonably.

We held an industry roundtable in March 2020

3.43 On 30 March 2020, we outlined our concerns to industry in a roundtable and published the speaking notes and presentation on our website.[20] We set out the options going forward to improve protections for APP scams.

1. The first (and preferred option) was for the industry to improve the application of the CRM Code by working closely with the LSB and Financial Ombudsman.
2. The second was for an industry-led Faster Payments rule change to embed reimbursement obligations for APP scams in payment system rules.
3. Failing the first two options, the third would involve the PSR considering action, recognising a wider set of actions may become available after the end of the UK's transition from the EU.

19 In their recent review of the CRM Code, the LSB have proposed changing its wording to reflect that firms may fund 'no-blame' cases from the shared fund or by themselves. We will monitor progress on this.

20 https://www.psr.org.uk/publications/general/authorised-push-payment-app-scams-conference-call-30-march-2020/

3.44 We followed the roundtable up with a series of one-to-one engagements with participants to understand what they were doing to improve customer outcomes under the CRM Code.

3.45 In August 2020, we published a thought piece[21] emphasising our expectation for industry that PSPs should work together to get the right outcomes for customers by improving reimbursement and repatriation levels and agreeing a suitable way to fund reimbursement in the long-term.

Industry engagement

3.46 As discussed above, in March 2020 we hosted a roundtable with industry where we set out our expectations, the concerns we had and the broad options as we saw them.

3.47 On 11 May 2020, the banking sector trade body UK Finance wrote to the PSR calling for legislation to tackle APP scams and for other industries that can help prevent APP scams (such as telecommunications) to play a role. We are sympathetic to the view that many stakeholders in the broader communications and social media world have a role to play. For example, in helping to prevent the recruitment of 'money mules' (people who are paid to allow funds to flow through an account open in their name) and to contribute to the education of consumers about protecting their information online. The FCA recently called for action to prevent fraudsters recruiting victims through social media advertising, at its Annual Public Meeting in September 2020.[22]

3.48 We remain supportive of the principle that PSPs should be able to look to other industries that have a role to play in preventing APP fraud, including when considering how to fund reimbursed APP scam losses.[23]

3.49 However, the PSR can only act within the current statutory framework. This means that, as things stand, there are only two broad choices for funding the losses to victims of APP scams: leaving the victim to meet the cost of the losses (with the harm that goes with this approach); or reimbursing the victim, and accepting that this is a cost of providing payment services to customers.

3.50 Furthermore, while we support efforts to broaden engagement on APP scams across industries in the future, this does not prevent PSPs from improving customer outcomes now.

3.51 We recognise the steps that have been taken so far to broaden industry involvement. The Stop Scams initiative is a good example of this. Stop Scams is an industry-led programme of work supported by Ofcom and the FCA. It was set up following industry calls to extend the discussion on tackling APP scams to other industries beyond financial services. Other examples include the government's Joint Fraud Taskforce, in which industry, law enforcement and the government work together to look at ways of dealing with fraud, and the Fraud Advisory Panel, a trustee-run organisation drawing its membership from the public, private and voluntary sectors, which gives advice on fraud prevention, detection and reporting.

---

21 https://www.psr.org.uk/news-updates/thought-pieces/thought-pieces/getting-the-right-outcomes-for-the-victims-of-app-scams/

22 https://www.fca.org.uk/publication/transcripts/annual-public-meeting-2020.pdf – see pages 42–45.

23 In our response letter, we asked the industry to set out the barriers to these losses being recovered, and would welcome a response to this point.

3.52 These initiatives have created opportunities for cross-sectoral cooperation, with members identifying and developing projects to prevent fraud and reduce customer harm.

We have engaged with the LSB

3.53 The LSB is the CRM Code's governing body. Since the CRM Code went live, we have engaged regularly with the LSB on CRM Code issues, such as customer outcomes, broadening participation, and clarifying the CRM Code on funding and the onboarding process.

3.54 We acknowledge that the LSB completed a review of the CRM Code in January 2021, and recently published a report with recommendations to improve the functioning of the Code. However, as many customers fall outside of the protections offered by the CRM Code, we need to look at the full scope of protections and not simply the effectiveness of the CRM Code.

Other actions

3.55 In recent years, the PSR has used its regulatory powers to require a number of UK PSPs to introduce Confirmation of Payee (CoP), a fraud-prevention tool that gives people the additional protection of checking an intended payee's name against the name associated with the account number being paid to. This service was designed to make it harder for fraudsters to pretend to be someone else, helping to reduce fraud and accidentally misdirected payments, and marked a significant milestone in reducing APP scams. At the PSR's request, CoP was adopted by members of the UK's six largest banking groups and has also now been adopted by other UK banks. The PSR is continuing to work with Pay.UK and industry on the next phase of CoP, which will enable even more PSPs to implement this fraud-prevention tool. Stakeholders will hear more about this from us later this year.

Our conclusion

3.56 The CRM Code has been in operation for over a year and a half now. Our analysis suggests that in that time, though it has improved both customer protection and incentives for PSPs to prevent APP scams in the first place, it hasn't gone far enough toward achieving the aim of significantly reducing APP scam losses incurred by customers. We would be interested in hearing views on the issues we're seeing with the Code to further our understanding.

3.57 Alongside receiving stakeholder feedback on CRM Code performance, we'd also like to move toward potential solutions to prevent APP scams and protect victims. In the next chapter, we present potential measures that we believe could contribute effectively to our objective of significantly reducing APP scam losses incurred by payment system users, and on which we are seeking views.

4 Potential measures

We set out three potential measures that we believe could contribute effectively to achieving our aim of significantly reducing APP scam losses incurred by customers. They are aimed at both preventing APP scams and protecting those who do fall victim.

In developing these options, the PSR will, of course, take into account the general principle that those who use services provided by payment systems should take responsibility for their decisions (section 53 of FSBRA).

We have set out a range of options: one focused on improving transparency and empowering consumers; one on preventing fraud by enhancing risk-detection by PSPs; and a third focused on introducing mandatory protection for customers.

We welcome your views on the measures, including any evidence or information on their viability, effectiveness, proportionality, and how they should be developed.

4.1 We are considering the following complementary potential measures:

1. Improving transparency on outcomes, by requiring PSPs to publish their APP scam, reimbursement and repatriation levels.
2. Greater collaboration to share information about suspect transactions, by requiring PSPs to adopt a standardised approach to risk-rating transactions and to share the risk scores with other PSPs involved in the transaction.
3. Introducing mandatory protection of customers, by changing industry rules so that all payment firms are required to reimburse victims of APP scams who have acted appropriately.

4.2 These measures could be introduced individually, or together to form a comprehensive package to prevent APP scams and protect victims. Some measures may be quicker to implement, such as the requirement for PSPs to publish APP scams data. The other measures would require further development through industry engagement or regulatory action, meaning a longer timeline for implementation.

Measure 1 – publishing APP scams data

4.3 At present, there is no firm-level information publicly available on APP scam losses, reimbursement and repatriation levels at PSP level. Making such information public would generate clear, easily comparable data about PSP performance that a range of stakeholders (including customers) could easily refer to. If such information were made publicly available, it would give PSPs a strong incentive to do more to prevent APP scams taking place and to protect customers when they do fall victim. Having the information published by a single body in one place – whether the PSR or another appropriate body – would also allow customers to compare PSP performance without having to search multiple websites.

4.4 If appropriate and proportionate, we could use our power under the Financial Services (Banking Reform) Act 2013 (FSBRA) to require PSPs to publish statistics on a quarterly or six-monthly basis for Faster Payments and Bacs Direct Credit. In assessing our next steps on APP scams, we are particularly mindful of our statutory objective to ensure that payment systems are operated and developed in a way that takes account of the interests of those who use (or may use) their services, but also the general principle that those who use services provided by payment systems should take responsibility for their decisions.

4.5 The publication of statistics would be designed to provide good reputational incentives to deliver appropriate outcomes. We recognise that reimbursement as a metric is not clear cut – for example, it is possible that higher levels of prevention might prompt lower levels of reimbursement. Therefore, we have set out some options and consider that the publication of a number of key metrics might provide a more accurate picture and therefore have a better impact on incentives. PSPs could set out:

1. the total number and value of APP scams their customers have fallen victim to during the period, and the average loss per customer
2. the total value of APP scams affecting all customers of the PSP in the period, broken down into:
    - amount repatriated
    - amount reimbursed
    - amount borne by customers

4.6 An alternative might be to require these figures to be expressed on a per-transaction (or per-1,000 transactions) basis, or a per-customer/account basis. This would weight the figures by the size of the PSP allowing a possibly more meaningful comparison across PSPs.

4.7 These metrics have been suggested as they would show clearly how banks are performing in preventing APP scams, and what happens with customers who do fall victim. The idea is to help customers to compare PSPs on this basis. There may also be benefit in publishing information about how APP scam cases are handled, such as:

- the number of cases resulting in a complaint to the PSP
- the number of cases referred to the Ombudsman
- the number of cases decided in the victim's favour by the Ombudsman

4.8 Again, these could be adjusted to reflect the size of the PSP. There may also be other metrics that would help provide a balanced overall summary of PSP performance. For example, it may be informative to report on the effectiveness of fraud prevention measures and the efforts made by PSPs to prevent fraud, such as:

- the effectiveness of scam warnings, expressed as the percentage of transactions stopped or paused by warnings
- the percentage of frauds attracting some form of bank intervention in advance

4.9 There are clearly a number of types of data that could be used, and it's possible that a solution might be to use these to develop a 'scorecard' for each institution, with indicators on key aspects of performance on APP scams. The ultimate aim would be to capture a balanced assessment of what actually matters to consumers/end-users.[24] We would welcome stakeholders' views on the metrics that might be useful in this regard.

4.10 This measure could be implemented relatively quickly for PSPs already signed up to the CRM Code, for a subset of the data set out above, because CRM Code signatories already collect this data. Implementation for other Faster Payments and Bacs PSPs could be phased, to give them extra time to collate and publish data.

4.11 There is a risk that scammers could use this information to target PSPs with higher levels of APP scam losses because of perceived weaker fraud controls. However, this appears to be a relatively small risk because if a PSP has relatively high fraud levels, that probably means scammers are already aware of the relative weaknesses. Overall, though, the measure should provide a strong incentive for PSPs to bolster their fraud systems to remain competitive.

Who would collate and publish the data?

4.12 UK Finance currently collates APP scams data from CRM Code signatories. The data is presented in aggregate form in their bi-annual fraud publications. PSP-level APP scams data is not published. We are interested to hear views on whether the requirement to present this data should be imposed only on current CRM Code signatories, or if it should be extended to other Faster Payments and Bacs PSPs.

4.13 We are also interested to hear who should be responsible for collating and publishing this data. There appear to be four main options:

- Pay.UK, potentially backed by a rule-change within Faster Payments and Bacs
- UK Finance acting on a voluntary basis (for both its members and any non-members who are members of Faster Payments and Bacs)
- the LSB (for both CRM Code signatories and non-signatories)
- the PSR

Question 6: **Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on the information we propose for publication outlined above, or on who should publish the data?**

24 In its recent review of the CRM Code, the LSB also concluded that: 'In order to fully assess the effectiveness of the Code, a series of success measures should be defined, which take account of, but look beyond reimbursement levels.'

Measure 2 – standardised shared fraud scoring

4.14 While PSPs generally already have processes in place to risk-rate transactions for fraud, our understanding is that these processes vary across PSPs, and the information produced is rarely shared with other PSPs in the transaction (for example, there is currently no way of doing this within a payment message). When information is shared, the process is manual and only done for a small number of transactions where the sending PSP has suspicions of fraud and has a way of communicating this with the receiving bank.

4.15 If appropriate and proportionate, we could use our power under FSBRA to require PSPs to adopt a standardised approach to risk-rating Faster Payments and Bacs transactions. We could also require PSPs to communicate these risk scores with other PSPs involved in a transaction.

4.16 The aim would be to facilitate better use of risk information and to improve coordination between PSPs to support identification of APP scam risks. This could support a number of different actions to prevent fraud and/or recover losses, as it would allow PSPs receiving high-risk transactions from multiple PSPs to understand more quickly when these transactions are going to a particular account. This might allow the receiving PSP to take a range of actions in response, such as:

- investigating whether the receiving account is a 'mule' account, under the control of a fraudster
- considering whether the receiving account is being used to support purchase scams
- suspending the onward transfer of funds from the receiving account, pending further investigation[25]
- alerting the appropriate authorities

4.17 We understand that the industry, through UK Finance, is looking at ways to improve co-ordination between sending and receiving PSPs, to support identification of high-risk transactions and improve fraud detection. In its recent review of the CRM Code, the LSB noted feedback from existing CRM Code signatories and consumer representatives that the division of responsibilities between sending and receiving PSPs should be reviewed and greater emphasis placed on the role of the receiving PSPs, with a corresponding sharing of liability.

4.18 One way for the PSR to take this forward could be to ask the industry to set up a working group to develop a common set of risk-scores. The group could develop a set of risk-scores and appropriate methodology for assigning risk-scores to payments, including dealing with issues such as the level of discretion PSPs would have in judging risk. The PSR could then consider (subject to legal requirements) using its FSBRA powers to require PSPs to use those scores in risk-rating payments, and automatically share the score with a receiving PSP in a payment transaction.

25 Any delay would need to be consistent with the provisions of the PSRs 2017 on execution of payment instructions.

How would scoring work?

4.19 If this measure were to be implemented, the sending PSP would use standardised scoring to assess the APP scam risk of each outgoing transaction. Potentially (and subject to the conclusions of the working group), one or more of the information sources listed below could be used by the sending PSP to establish the likelihood of the transaction being an APP scam:

- transaction analytics, including payment frequency and value
- behavioural analytics, such as a customer's spending habits
- information on the payee, such as the account number and sort code, and where applicable, the results from a Confirmation of Payee check
- how commonly payments have been made to that payee's account
- the purpose of payment
- whether the sending PSP has taken steps to warn the customer (for example, by providing in-branch advice)

How would sharing work?

4.20 The measure would rely on an agreed approach to scoring so PSPs could understand the scores shared by others. There would also need to be a requirement on PSPs to send the information as part of the payment message, to ensure it was passed automatically between the sending and receiving banks. There might be scope to use existing fields in a payment message to do this.

4.21 Again, one way for the PSR to take this forward could be to ask the industry to set up a working group to look at how to facilitate the sharing of standardised risk scores, with a view to requiring PSPs (using our FSBRA powers) to implement the outcome.

Question 7: **Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on its feasibility, how it could work, or whether the issues and requirements set out would be best dealt with by a working group?**

Measure 3 – reimbursing APP scam victims

4.22 As discussed earlier, the evidence suggests the protection offered to victims by CRM Code signatories hasn't led to the significant reduction in APP scam losses incurred by customers that we believe is needed.

4.23 Measure 3 is focused on two ways of addressing this problem:

- extending the obligation of reimbursement to all PSPs by the inclusion of a reimbursement requirement in system rules
- in doing this, providing a way to secure greater compliance with the reimbursement obligation

4.24 We have identified two general approaches to doing this, both of which rely on changing the scheme rules of Faster Payments (and, if appropriate, Bacs Direct Credit). The first (3A) seeks to incorporate the reimbursement obligation into scheme rules. The second (3B) seeks to make membership of, and compliance with, a PSR-approved code mandatory. A key difference between the two approaches is that, to extend the reimbursement obligation to all PSPs, 3A also necessarily raises the standard of protection to customers in order to define a scheme rule with sufficient certainty.

4.25 As discussed in Chapter 1, we cannot currently require PSPs to reimburse APP scam victims because of restrictions in the PSRs 2017. Now that the UK's transition from the EU has ended, it is open to the government to legislate to remove the restrictions.

4.26 While we are prevented from requiring reimbursement (through measure 3A or 3B) until any such changes are made, we want to be ready to act if restrictions are lifted. It also remains open to participants to propose rule changes to Pay.UK without the PSR requiring this. We discuss each measure below.

4.27 In each variant, this option involves imposing reimbursement liability on PSPs in order to protect customers and to also incentivise them to act more effectively to reduce the level of APP scams across Faster Payments (and, potentially, also Bacs Direct Credit). As previously discussed, in developing this option the PSR will also need to consider the general principle that those who use services provided by payment systems should take responsibility for their decisions (section 53 of FSBRA). We have therefore sought to strike a balance between:

- customer responsibility
- effectively incentivising PSPs to do more to drive down the level of APP scams
- ensuring that liability for scams where no party is at fault sits with that party most able to weather the loss

Measure 3A – Incorporating the obligation to reimburse in scheme rules

4.28 This approach would involve requiring incorporation into scheme rules of an obligation to reimburse customers who have acted appropriately. If enforced effectively by the scheme operator, this would be a significant increase in the protections offered to customers through the scheme rules.

4.29 However, it is not possible simply to reflect the language used in the CRM Code in the scheme rules. As discussed earlier in this document, this language appears open to a significant degree of interpretation by PSPs. If such language were to be included in Faster Payments or Bacs rules, it might simply lead to similar variability in outcomes. It may also imply that Pay.UK would need to develop and implement a significant monitoring and dispute resolution function when enforcing the rule.

4.30 Given this, to ensure this option is effective, the language used in the scheme rules would need to be less open to interpretation by PSPs, and any exception definitions would also need to be made less open to interpretation. Although it is not the aim of this approach, a natural consequence of establishing sufficient clarity in the definitions would be to reduce PSP discretion and so – in areas where there is currently doubt over

the scope of an exception – favour the customer. This would mean that more of the liability for APP scams would fall on PSPs. This is consistent with the way that the Direct Debit guarantee is currently codified into the Bacs scheme rules.

4.31 We have considered how such an approach could also be codified into scheme rules. This is set out in the following sections.

Who and what would the requirement cover?

4.32 The requirement would apply to payments made over Faster Payments and Bacs Direct Credit by the following:

a. **Consumers:** following the current definition in regulation 2(1) of the PSRs 2017, i.e. an individual acting for purposes other than a trade, business or profession.

b. **Micro-enterprises:** following the current definition in regulation 2(1) of the PSRs 2017, i.e. an enterprise that employs fewer than 10 people, with an annual turnover or annual balance sheet total not exceeding 2 million euros as at the date of the scam.

c. **Charities:** following the current definition in regulation 2(1) of the PSRs, i.e. a charity with an annual income of less than £1 million as at the date of the scam.

4.33 The above user coverage aligns with that in the CRM Code. The rationale for this scope would be that, of all payment system users, these groups are most susceptible to falling victim to an APP scam through no fault of their own. Larger corporations, for example, should have systems and processes in place to prevent fraud.

4.34 'On-us' transactions – which do not pass over payment systems such as Faster Payments and Bacs – constitute a small proportion of APP losses (<1% in H1 2020). The PSR would consider the possibility of applying the reimbursement requirement to 'on-us' payments to avoid the risk of creating a two-tiered system where payments between accounts in the same PSP go unprotected, while those to other PSPs are protected. We do however expect PSPs would have a strong incentive to offer the same level of protection for their customers for any on-us transactions even without PSR action in this regard.

When would reimbursement not occur?

4.35 Reflecting the need for simplicity in the application of the rules, under this approach PSPs could only deny reimbursement if:

- the sending PSP finds compelling evidence of first-party fraud, or
- the sending PSP finds compelling evidence that the loss did not arise from an APP scam

4.36 It is important to consider whether the increased level of protection afforded by mandatory reimbursement being written into scheme rules could have an effect on incentives faced by individuals to take responsibility for their own decisions. If this higher level of protection led to a higher level of successful scams, there would be an impact on the costs to PSPs. We would assess the likelihood of this in light of our statutory duties, and would welcome views on this potential risk.

Where would liability for reimbursement sit?

4.37 To make this option work, the key issue is that customers are reimbursed. As sending PSPs hold the relationship with payers, it makes sense that they are responsible for the initial reimbursement of customers. However, it is possible to allocate these losses between sending and receiving PSPs. This may have a better impact on the balance of incentives between PSPs to prevent fraud. The addition of liability for the receiving bank could further incentivise them to spot and deal with scammers' mule accounts – which they are best placed to do – and measure 2 outlined above would also give these banks more information with which to do this.

4.38 Reflecting this, the scheme rules could impose the obligation to reimburse the APP scam victim on the sending PSP, which would then be able to apply to recover some of those funds from the receiving PSP. An alternative would be to rely on a more complex set of rules – as is set out in the current CRM Code – to allocate liability. In principle, a set of allocation rules could be included in the scheme rules, or the scheme rules could incorporate the allocation principles in the code (for example by cross-reference).

Should all APP scams be covered?

4.39 We recognise there is a risk that customers may take less care when transacting if it's almost certain they'll be reimbursed. This risk may be higher for certain scam types (see Chapter 1 for detail on the different APP scam types). For example, purchase scams may be more susceptible to this risk than other scam types because the customer is responsible for selecting a vendor.

4.40 If this risk is too high, it may merit excluding certain scam types from the requirement, dealing with these under other consumer protection measures. Having said this, it is unlikely that many transactions are entered into by people not caring whether the other party could be a fraudster, and a high proportion of APP scams involve very significant amounts of money. It is very important, therefore, that the logic for any exclusions be clear and defensible.[26]

Question 8: **Do you have any comments on Measure 3A? For example, do you have feedback on the design, or its effectiveness and proportionality?**

Measure 3B – Requiring membership of an approved code

4.41 The objective of this approach is to change payment system rules to create an incentive for all PSPs to sign up to an effective code developed by industry then approved by the PSR, which would include a requirement to protect customers and to comply with that code's other obligations. Relative to measure 3A, this could allow more flexibility for PSPs, while still introducing a new payment-system rule ensuring protection to a regulator-approved standard. We would expect that the LSB would seek to secure approval for a modified version of the current CRM Code.

26 In their review of the CRM Code, the LSB also point out that excluding purchase scams from the Code could have unintended consequences on low-income customers.

4.42 To achieve this, the PSR would mandate inclusion in the Faster Payments (and, if appropriate, Bacs) rules of a requirement for PSPs to do one of two things:

- sign up to a PSR-approved reimbursement code, meeting criteria set out in advance by the PSR, and demonstrate a high-level of compliance with the obligations set out in that code, or
- reimburse all customers that fall victim to APP scams (subject only to very limited exceptions, such as evidence of first-party fraud)

4.43 It is likely that PSPs would be less inclined to opt for the latter approach, which might involve a reimbursement guarantee akin to the Direct Debit guarantee. However, if no code gains approved status (or there is one approved code which later loses approval) the second option would apply by default.

4.44 This measure would offer PSPs opportunity and incentive to develop a code that improves outcomes for customers, broadens protections to a wider range of customers, and provides more consistent outcomes for consumers. It would broaden customer protection beyond the current CRM Code members. It could also provide a route to address concerns about the inconsistent application of the current CRM Code, and concerns about a failure of a code to be developed appropriately.

4.45 We would expect the requirements for approval of a code to prompt ongoing review and improvement, in light of experience. As recent experience with the CRM Code highlights, this would not be a straightforward task. However, this option would provide a regulatory backing to current and prospective codes, and therefore provide greater assurance that they improve over time. For a code to receive approved status, the PSR would have to be satisfied that it would improve outcomes for APP scam victims, including in terms of the rules it sets, how these rules change over time and how the code is applied, including its governance and the monitoring and enforcement processes for securing compliance with its rules.

Question 9: **Do you have any comments on Measure 3B? For example, do you have feedback on the design, or its effectiveness and proportionality?**

Steps to implementing measures 3A and 3B

Who should take this forward?

4.46 As set out in Chapter 1, there are legislative restrictions preventing us from requiring reimbursement under measure 3A and 3B. It is open to the government to legislate to lift these restrictions.

4.47 While this limits our ability to mandate reimbursement until restrictions are lifted, it remains open to industry participants bringing forward rule change proposals, informed by the options we set out above.

Further issues to consider for all three measures

4.48 There are several issues that cut across all three measures.

Is a direction or rule change most appropriate?

4.49 If we were to use our formal powers, we could pursue each measure through either a direction on the relevant PSPs or requiring Pay.UK to change payment system rules.

4.50 We are open to both approaches, but provisionally consider a direction may be more appropriate for measure 1, and a rule change for measures 2 and 3. Measure 1 is purely a reporting exercise, whereas measures 2 and 3 are operational in nature. System rules seem a more appropriate place for detailed provisions on operational protocols that PSPs must follow.

Indirect PSPs

4.51 For each option, there is a question over how we account for indirect PSPs. A direct PSP is one that directly connects to the payment clearing infrastructure. An indirect PSP is one that has a contractual arrangement with an indirect access provider (a direct PSP) that allows it to pass transfer orders across a payment system so it can provide payment services to its customers.

4.52 A limitation of system rules is that they only apply to direct PSPs. A direct PSP that provides access for an indirect PSP may then be accountable for acts and omissions of that indirect PSPs.

4.53 If only direct PSPs are required to follow rules implementing measures 2 and/or 3, or if the enforcement mechanisms are weaker for indirect PSPs, this would risk creating a two-tier system. Customers may be more exposed to the risk of APP scams simply because they bank with an indirect PSP. We are conscious that the status of a PSP is a technical matter, and this information is often not readily available to customers.

4.54 Given this, the PSR would need to consider whether to extend any of the measures to indirect PSPs, any legal limitations on doing so and the most effective mechanism for including indirect PSPs.

4.55 It's worth noting that regulation 104 of the PSRs 2017 imposes requirements on PSPs in Faster Payments, Bacs and CHAPS.[27] One requirement is that PSPs must treat requests by authorised or registered PSPs for indirect access to the system in a proportionate, objective and non-discriminatory manner. They also must not prevent, restrict or inhibit access to or participation in the system more than is necessary to safeguard against specific risks; or impose any restrictions on the basis of institutional status. The PSR could not impose obligations on direct PSPs that conflict with the provisions of regulation 104 or encourage or incentivise them to act in a way that conflicts with that regulation. Whatever approach we take for indirect PSPs, it must be consistent with regulation 104 of the PSRs 2017.

27 Regulation 104 PSRs 2017 applies to designated payment systems. Under regulation 2(1) PSRs 2017, 'designated system' has the meaning given in regulation 2(1) of the Financial Markets and Insolvency (Settlement Finality) Regulations 1999.

Should Bacs be included?

4.56 As outlined in Chapter 1, we are focused here on Faster Payments and Bacs Direct Credit. 86% of APP scam losses occur over these two systems, although the vast majority occurs over Faster Payments (79%). In addition, the operation and user profile of the two systems is different. We would be interested in hearing views as to whether we should include Bacs Direct Credit in the measures outlined above.

How would the measures be enforced?

4.57 This depends on whether we pursue a measure via a direction or a rule change. The PSR has a clear statutory framework for enforcing directions and rule-change requirements, including use of financial penalties where there is evidence of non-compliance. However, the choice of instrument alters what the PSR can enforce, and against which persons. For a direction, the PSR would be able directly to monitor and enforce compliance by directed PSPs.

4.58 For a rule change, the PSR can use its enforcement powers to ensure that a system operator changes the rules as required. However, monitoring and enforcement of the new rules would sit with the system operator – Pay.UK in this case. Pay.UK has itself raised concerns about enforcement of rules under their existing set-up. For example, the effectiveness of the enforcement tools available to Pay.UK has already proven to be an issue in other areas such as Direct Debits. However, we believe this is something Pay.UK can fix itself, as it can change its own rulebook (albeit following consultation).

4.59 Alongside this call for views, the PSR has a separate call for views open that considers consumer protection in interbank payment systems more generally. This includes considerations on what level of payment system governance is required to deliver effective consumer protection, including what enforcement tools system operators require.

4.60 We are coordinating our work on APP scams with this broader work on consumer protection and would be interested in hearing views on the rule enforcement issue. If you would like to submit your views on rule enforcement, please see the Consumer Protection call for views at https://psr.org.uk/publications/consultations/cp21-4-consumer-protection-in-interbank-payments-call-for-views/. Submissions are open until 5pm on 8 April 2021.

Mule accounts

4.61 The public and private sectors are working to address the issue of mule accounts. The FCA has co-sponsored the Stop Scams UK Working Group, comprising FCA, PSPs, telecoms companies and social media platforms. This group is designed to develop cross-sectoral cooperation and coordination to prevent fraud, by heightening awareness of scams and money mules and developing initiatives to stop fraud at source. These include increasing the effectiveness of data sharing between industries and facilitating cross-industry profiling and sharing of characteristics of mules as they evolve.

4.62 The Joint Fraud Taskforce has also supported initiatives to promote awareness of mule accounts – for example, by promoting the free lesson plans designed by Cifas[28] to raise awareness amongst secondary school-aged children of the risks of becoming a money mule. Industry initiatives include the Mule Insights Tactical Solution (MITS), a project developed by Vocalink with Pay.UK and the major banks, which traces the money from a confirmed fraud between PSPs to identify suspect mule accounts and shut them down.

Question 10: Do you have any comments on these issues? For example, do you have feedback on whether we should use a direction or a rule change to pursue these measures, or whether Bacs should be included?

28 Cifas is a not-for-profit membership association representing organisations from across the public, private and voluntary sectors (www.cifas.org.uk).

5 Equality impact assessment

5.1 In considering how to address the problem of payment systems being used to facilitate APP scams, the Payment Systems Regulator has a duty to take account of the factors set out in section 149 of the Equality Act 2010 (public sector equality duty), particularly the impact of any action on people with protected characteristics.[29]

5.2 In line with this duty, we would assess the likely equality impacts and reasons for any measures we might propose (and consult on) following receipt of the views called for in this paper. Certain payers with protected characteristics may be more likely to be vulnerable to APP scams. This may include some elderly people, and people with certain mental health disabilities. It may also include some payers with attributes linked to protected characteristics, such as those who do not speak English as a first language.

5.3 Our assessment might, for example, include the risk that PSPs may seek to minimise the total number and value of APP scam losses for their business by limiting or denying services to people who may be vulnerable to APP scams. It is therefore our intention to undertake a full equality impact assessment at the next stage of policy development.

Question 11: Do you have any comments on our proposal to conduct an equality impact assessment for any measures developed following this call for views?

29 The relevant protected characteristics under section 149 are age; disability; gender reassignment; pregnancy and maternity; race; religion or belief; sex; sexual orientation.

6 Next steps

Respond to this call for views

6.1 We are asking for feedback on the issues set out in this paper by **5pm on 8 April 2021**. We welcome feedback from all stakeholders and interested parties, not only entities that we regulate.

6.2 You can provide your feedback by emailing us at **appscams.callforviews@psr.org.uk**. We would be grateful if you could provide your response in a Word document (rather than, or as well as, a PDF).

6.3 We will make all non-confidential responses available for public inspection. If your submission includes confidential information, please also provide a non-confidential version suitable for publication.

Timetable

6.4 The timetable for this consultation and the subsequent process is as follows:

8 April 2021	Call for views closes
April–June 2021	The PSR considers the responses and next steps
July–September 2021	Follow-up paper

Annex 1:
List of questions

Question 1: Do you have any comments on the data presented above? Do you have any supplementary information on customer outcomes under the CRM Code?

Question 2: Do you have any comments on the appropriate balance of liability for APP scams costs between individuals and PSPs?

Question 3: Do you have any comments on our analysis of what is driving the CRM Code outcomes we're seeing?

Question 4: What could be done to ensure consistency in the outcomes of dispute resolution, and to give customers and industry transparency into how these outcomes are arrived at?

Question 5: Are there any other issues with the CRM Code you would like to tell us about?

Question 6: Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on the information we propose for publication outlined above, or on who should publish the data?

Question 7: Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on its feasibility, how it could work, or whether the issues and requirements set out would be best dealt with by a working group?

Question 8: Do you have any comments on Measure 3A? For example, do you have feedback on the design, or its effectiveness and proportionality?

Question 9: Do you have any comments on Measure 3B? For example, do you have feedback on the design, or its effectiveness and proportionality?

Question 10: Do you have any comments on these issues? For example, do you have feedback on whether we should use a direction or a rule change to pursue these measures, or whether Bacs should be included?

Question 11: Do you have any comments on our proposal to conduct an equality impact assessment for any measures developed following this call for views?

PUB REF: CP21/3

12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: www.psr.org.uk