FINANCIAL CONDUCT AUTHORITY
PAYMENT SYSTEMS REGULATOR

Preventing and responding to authorised push payment scams: The role of payment system operators

Draft Terms of Reference

February 2017

Contents

1. Introduction

1.1 We are going to do work considering the potential for payment system operators (PSOs) to play a role in minimising the consumer harm caused by authorised push payment (APP) scams in the UK. We committed to do this in our response to a super-complaint we received from Which?. These draft Terms of Reference (ToR) explain how we intend to carry out this work.

1.2 Push payments are payments where a customer instructs their bank to transfer money from their account to someone else's account. In contrast, pull payments involve the person who is due to receive the money instructing their bank to collect it from the payer's bank. An authorised payment is one where the customer has consented to the money being paid from the account. Unauthorised payments are those where a bank pays money from a customer's account without their consent – for example, a payment made using a stolen payment card. In an APP scam, a victim is tricked into authorising a push payment. We explain APP scams in detail in the annex to these ToR.

1.3 There are two payment systems which customers might use when falling victim to APP scams: CHAPS and Faster Payments Scheme (FPS). In our response to the Which? super-complaint, we found that the operators of CHAPS and FPS do not have any rules, policies or procedures in place related to consumer protection against fraud or scams. They considered it to be outside their remit to intervene in what they view as private contractual matters between payment service providers (PSPs) and their customers.

1.4 With the work we propose in these draft ToR, we want to understand whether there is more that operators of push payment systems could do to minimise the consumer harm from APP scams. Consumer harm can be reduced by preventing a scam, and by improving how PSPs and PSOs react to scams. We will consider two overarching questions:

- Are there actions that the operators could take directly that would be effective and proportionate?
- Are there requirements that the operators could place on PSPs using the system that would be effective and proportionate?

1.5 In answering these questions, we will consider:

- any impediments that might prevent the operators from doing more, including legal restrictions
- any relevant developments on the horizon that might affect the role the operators should play

Why we are doing this project

1.6 On 23 September 2016 the consumer body Which? submitted a super-complaint to us regarding the consumer safeguards for push payments. Which? was concerned that there are no measures in place to protect victims of APP scams. Which? suggested that customers have more legal protection in scams where they have paid with a pull payment rather than a push payment, pointing out a number of existing consumer protection mechanisms for card payments (under both the Consumer Credit Act 1974 for credit cards and the so-called 'chargeback rules') and for direct debits (such as the Direct Debit Guarantee).

1 www.psr.org.uk/sites/default/files/media/PDF/PSR-Which-super-complaint-response-December-2016.pdf

1.7 We published our response on 16 December 2016, meeting the statutory requirement that we respond to super-complaints within 90 days of receiving them.

1.8 In that response, we set out a package of work motivated by a desire to reduce fraud and make it harder to commit. Where APP scams do occur we want to increase the chance the victim will be able to recover their funds. When we developed our proposals we took into account work other bodies were doing on financial crime, most notably projects by the Joint Fraud Taskforce and the Payments Strategy Forum.

1.9 The project covered by these ToR is one part of our proposed package of work. The other parts involve work led by Financial Fraud Action UK (FFA UK) and the Financial Conduct Authority (FCA) respectively. FFA UK agreed to lead banking industry work to understand the scale of APP scams better and improve how PSPs work together in responding to them. We are monitoring that work, and will report on progress in the second half of 2017. The FCA will take the following actions:

- Work with firms to tackle concerns around both sending and receiving banks in relation to APP fraud.
- FCA supervision will examine evidence received in relation to the super-complaint, and will address any firm-specific issues directly.
- If, following the above steps, there are unresolved sector-wide issues, the FCA will initiate further work. Any such work should consider the developments made since its thematic review of banks' defences against investment fraud in 2012.

2. The scope of this project

2.1 We have two objectives in this project:

- We will consider whether it would be effective and proportionate for operators of push payment systems to play a greater role in preventing and responding to APP scams (and possibly wider fraud). The expanded role might be in the form of actions that the operators might take, or new requirements that the operators might place on PSPs using their systems.
- If we conclude that new measures are appropriate, we will consider whether it would be best to introduce them through regulatory action or through other approaches (for example, industry-led). If we decide on a regulatory approach, we will develop proposals for consultation.

Payments included in this project

2.2 This project focuses on APP scams which target consumers; we do not plan to actively investigate APP scams which target businesses. Actions which benefit consumers would in many cases also benefit businesses; however, actively exploring APP scams specific to businesses (and potential remedies) would significantly expand the scope of this work. While we will not actively investigate business-specific issues, we will consider any business specific evidence that we identify in the course of this work.

2.3 One consequence of focusing on APP scams targeting consumers is that Bacs will be out of scope, since only businesses make push payments using Bacs. Two regulated payment systems offer push payment services to consumers, and are therefore within the scope of this project:

- CHAPS
- FPS

2.4 When we have completed this project we will consider any evidence we gather about APP scams affecting businesses, and consider whether we should do further targeted work to look at these issues.

2.5 Payments made to an account with the same bank may not go through one of these systems, as the bank may process them internally. These 'on-us' payments are out of scope of this project.

Key questions we will answer

2.6 The questions we propose to focus on in this project are:

1. How do UK practices towards APP scams compare with those in other countries?

We will identify practices around APP scam prevention and response in internationally comparable push payment systems. This will include comparing how different countries collect data on the prevalence of APP scams.

2. How do practices towards APP scams compare with practices for other UK disputed payments?

We will consider the practices of:

- other UK PSOs in fraud and scam prevention and response (in particular, Mastercard and Visa)
- all UK PSOs in relation to other disputed payment types (in particular, the Credit Payment Recovery scheme operated by FPS)

This will include considering the implications for fraud and scams of the rules schemes set for member PSPs. We will also consider the incentives and actions of proprietary payment systems, such as PayPal.

3. What can be learned from non-payment networks?

We will look at other comparable network industries (for example, telecommunications) to consider the role of central operators in setting rules about which parties take responsibility for protecting end-users under different circumstances.

4. What are the economic incentives for preventing and responding to APP scams?

We will consider the first-principle economic arguments around the incentives for different parties to prevent and respond to APP scams. This includes the lessons from historical regulatory and business interventions towards fraud. We will also consider how competition between payment mechanisms operates, including competition between payment systems.

5. What actions can we take to expand the role of PSOs in APP scams?

We will consider our ability to introduce regulatory change requiring PSOs to take on a greater role in preventing and responding to APP scams, and associated legal issues.

2.7 As part of our response to the Which? super-complaint, we also stated that we would monitor the work of FFA UK in implementing a number of agreed actions. This monitoring work is out of scope of this project; however, we will take developments in the UK payments market into account. We will also have regard to other developments already in progress that should further help to address the consumer harm caused by APP scams:

- The work of the Payments Strategy Forum in developing confirmation-of-payee capabilities, and on financial crime-related initiatives – in particular, those related to financial crime intelligence sharing and payment transaction data sharing and analytics.
- The work of the Joint Fraud Taskforce, in particular its:
    - initiatives relating to recovering funds paid out as a result of scams
    - development of further public education campaigns
    - work on developing a strategic action plan for the treatment and protection of fraud victims and vulnerable consumers

2.8 We will also take upcoming changes in PSOs' governance structures into account. This includes:

- the planned merger between Bacs Payment Schemes Ltd (BPSL), Faster Payments Scheme Ltd (FPSL) and Cheque & Credit Clearing Company Ltd (C&CCL)
- the Bank of England's consideration of alternative structures for CHAPS (including whether the Bank becomes the operator)

Possible outcomes of this project

2.9 The scope of this project is limited to:

1. identifying and evaluating potential expanded roles for operators of push payment systems in preventing and responding to APP scams
2. consulting on any proposals to introduce such measures

The detailed development and implementation of specific proposals is outside of the scope of this project. We would consult on any specific proposals separately at a later time.

2.10 Our proposals could affect PSOs in two ways: by requiring them to set rules related to fraud for their members, or by requiring them to take action themselves.

2.11 We will consider if it would be appropriate to use any of our wider regulatory and competition powers to address any concerns we identify. Possible outcomes of this project could include any combination of:

- making new directions or modifying existing directions
- making recommendations for further industry initiatives or enhanced industry self-regulation
- working with the Bank of England, FCA or Prudential Regulation Authority as appropriate
- publishing guidance
- taking no further action for the time being

This is not an exhaustive list.

2.12 Our proposals will be evidence-based. As well as examining existing research and analysing information that we already hold, we plan to collect additional information from market participants. We will engage with operators, PSPs, service-users and other interested parties over the coming months. We will use a variety of methods for this engagement, including (but not limited to) interviews, roundtables and site visits. We may gather evidence through the use of specific surveys and requests for detailed information from some participants.

2.13 We plan to publish the findings of our work in the second half of 2017.

3. Commenting on the draft Terms of Reference

3.1 Before we begin our project we are consulting on these draft ToR.

3.2 We expect to publish our final ToR by the end of March 2017. In finalising the ToR, we will review all feedback we receive to these draft ToR.

3.3 We welcome views and evidence which will help to inform our assessment of the key questions outlined in these draft ToR. We are particularly interested in answers to the following questions:

- Do you think that our scope, focusing on APP scams which target consumers, is appropriate?
- Do you agree with the key questions we want to answer, set out in section 2?
- Do you agree with the proposed timing for this project?

How to submit your views

3.4 Please send your comments to app-scam-pso-project@psr.org.uk by 21 March 2017. Or in writing to:

APP scams project team

Payments Systems Regulator

25 The North Colonnade

Canary Wharf

London E14 5HS

Disclosure of information

3.5 Generally we will seek to publish views or submissions in full or in part. This reflects our duty to have regard to our regulatory principles, which include those in relation to:

- publication in appropriate cases
- exercising our functions as transparently as possible

3.6 As such, we would ask respondents to minimise those elements of their submission which they wish to be treated as confidential – we will assume consent for us to publish material which is not marked as confidential. If respondents include extensive tracts of confidential information in their submissions, we would ask that they submit non-confidential versions which they consent for us to publish. We will also not accept blanket claims of confidentiality, and will require respondents to identify specific information over which confidentiality is claimed, and to explain the basis on which confidentiality is sought.

3.7 Despite this, we may be asked to disclose a confidential response under the Freedom of Information Act 2000. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by the Information Commissioner and the Information Rights Tribunal.

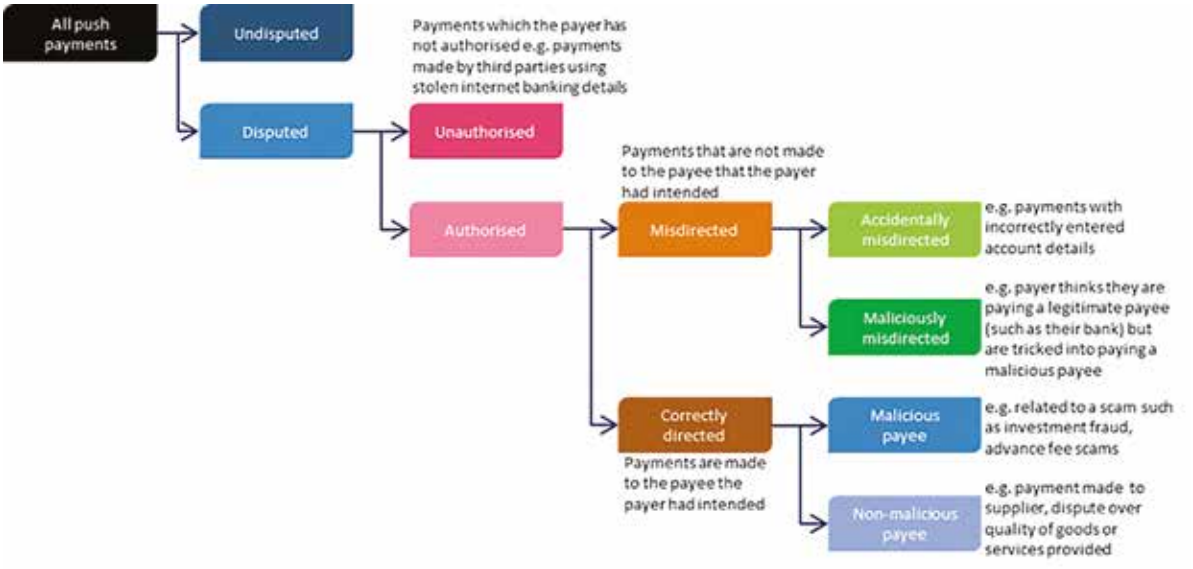
3.8 Respondents should note that we will not disclose confidential information that relates to the business or affairs of any person, which we receive for the purposes of our functions under the Financial Services (Banking Reform) Act 2013 (FSBRA), unless one of the following conditions apply:

- The information is already lawfully publicly available.
- We have the consent of the person who provided the information and, if different, the person it relates to.
- The information is published in such a way that it is not possible to ascertain from it information relating to a particular person (for example, if it is anonymised or aggregated).
- There is a 'gateway' permitting this disclosure. Among the gateways is the 'self-help' gateway whereby the PSR will be able to disclose confidential information to third parties to enable or help it to perform its public functions. Those receiving information disclosed under the gateway are still bound by the confidentiality regime.

Annex:
What are APP scams?

1.1 To understand the types of fraud within scope of this project, and the specific sub-types within those that are in scope, we present a breakdown of different reasons why a payer may make a payment and then subsequently dispute it (Figure 1).

Figure 1: Categorisation of disputed payments



Source: PSR

1.2 Of all payments (both push and pull) made from payers' payment accounts, the vast majority are **undisputed** – the payer has authorised the payment and funds are correctly credited to the intended payee, who in return provides the goods or services for which the payment was made without dispute.

1.3 Some payments, however, are **disputed** by payers and result in requests being raised with the payer's bank to recover the funds that have been paid out. Payments may be disputed for a number of reasons.

1.4 The payer may not have authorised the payment – that is, they have not provided consent for the payment. These **unauthorised** payments typically occur when a payer's payment credentials (for example, credit card or internet banking log-in details) are obtained by a malicious third party and used to withdraw or repatriate funds. For example, in a phishing/vishing scam, a fraudster calls the victim claiming to be from a credible third party such as a bank or the police. The fraudster then convinces the victim to divulge their personal or financial information.

1.5 There are a number of instances where payers have **authorised** payments (that is, they have provided consent for the payment) but subsequently dispute them:

- The first category relates to **misdirected** payments, where payments are made to payees that the payer did not originally intend. A payer may accidentally misdirect a payment by, for example, inadvertently providing incorrect payment details for the intended payee.

- Authorised payments may also be **maliciously misdirected** by third parties. In this instance, a payer intends to pay a legitimate payee but, as the result of a scam, instead pays a malicious third party due to the actions of that third party.

1.6 The second category of authorised payments that may be disputed relates to **correctly directed** payments:

- A payer may pay funds to a correctly identified payee for what they believe are legitimate purposes but then fall victim to a scam (for example, the payee may abscond with the funds without providing the promised goods or services). Authorised, correctly-directed payments that are disputed under these circumstances are referred to as relating to **malicious payees**.

- Finally, a payer may dispute an authorised, correctly directed payment relating to a non-malicious payee (for example, as part of a contractual dispute regarding payments made for goods or services).

1.7 Based on the categorisations outlined above, APP scams include **maliciously misdirected** payments and correctly directed payments to **malicious payees**.

25 The North Colonnade,
Canary Wharf, London
E14 5HS
Telephone: 0300 456 3677 or +44 20 7066 1000 from abroad
Website: www.psr.org.uk