FINANCIAL CONDUCT AUTHORITY
PAYMENT SYSTEMS REGULATOR

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

Final Terms of Reference

March 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?.[1] These 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 consumers 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 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

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

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 consumers 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).

1.7 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.

Stakeholder input to this terms of reference

1.10 We published draft ToR for this work on 28 February 2017 and asked stakeholders to provide us with feedback. We received a total of 15 responses to this consultation. We thank all respondents for taking the time to provide feedback on the draft ToR.

1.11 The majority of respondents were supportive or broadly supportive of the proposed work. A summary of the feedback we received is provided at Annex 2. These final ToR reflect our consideration of, and response to, the feedback we received.

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 proposals) 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 further targeted work to look at these issues should be undertaken.

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 direct 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, and compare these to the UK. This will include comparing how different countries collect data on the prevalence of APP scams. We will consider the relevant domestic legal and regulatory context when comparing international practices around 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, and of payment system overlay services (such as PayM).

   When comparing practices, we will consider differences in payment characteristics and the underlying legal and regulatory context for different payment systems.

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. **If appropriate, 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 In answering these questions, we will seek to identify evidence on the effectiveness of specific practices – in different jurisdictions, payment systems, and industries – in addressing their targeted issue (for example, how effective certain practices may be in reducing the incidence of fraud).

2.8 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. While out of the direct scope of this project, we will consider potential interactions and, where appropriate, coordinate with FFA UK's work.

2.9 We will 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, including the development of confirmation-of-payee capabilities, and its work 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

2.10 We will take upcoming changes in PSOs' governance and operational structures into account. This includes:

- the proposed consolidation of Bacs Payment Schemes Ltd (BPSL), Faster Payments Scheme Ltd (FPSL) and Cheque & Credit Clearing Company Ltd (C&CCL), and development of the new payments architecture (NPA)
- the Bank of England's consideration of alternative structures for CHAPS (including whether the Bank becomes the operator)

2.11 We will take wider relevant developments in the UK payments sector into account, including the implementation of the second EU Payment Services Directive (PSD2) and the development of Open Banking.

Possible outcomes of this project

2.12 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.

2.13 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.

2.14 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.

3. Next steps

Information gathering

3.1 Following publication of these final ToR, we will begin to gather information to inform our work. As well as examining existing research and analysing information that we already hold, we plan to collect additional information from market participants.

3.2 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, which may include interviews, roundtables and site visits. We may also gather evidence through the use of specific surveys and requests for detailed information from some participants.

Indicative timetable

3.3 Our current proposed broad timings for this work are as follows:

- **Q2 2017:** Information collection, including bilateral meetings with key stakeholders and issuance of any information requests.
- **Q3 2017:** Analysis of information and identification and development of any initial proposals.
- **Q3/Q4 2017:** Publication of our report setting out our findings. This report may include proposals for consultation.

3.4 In the event that we need to alter these timings, we will provide a revised timeline on the PSR website.

Input to this work

3.5 We welcome views and evidence that will help us inform our assessment of the key questions outlined in this ToR. Please send any comments to app-scam-pso-project@psr.org.uk. Or in writing to:

APP scams project team
Payment Systems Regulator
25 The North Colonnade
Canary Wharf
London
E14 5HS

Disclosure of information

3.6 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

3.7 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.

3.8 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.

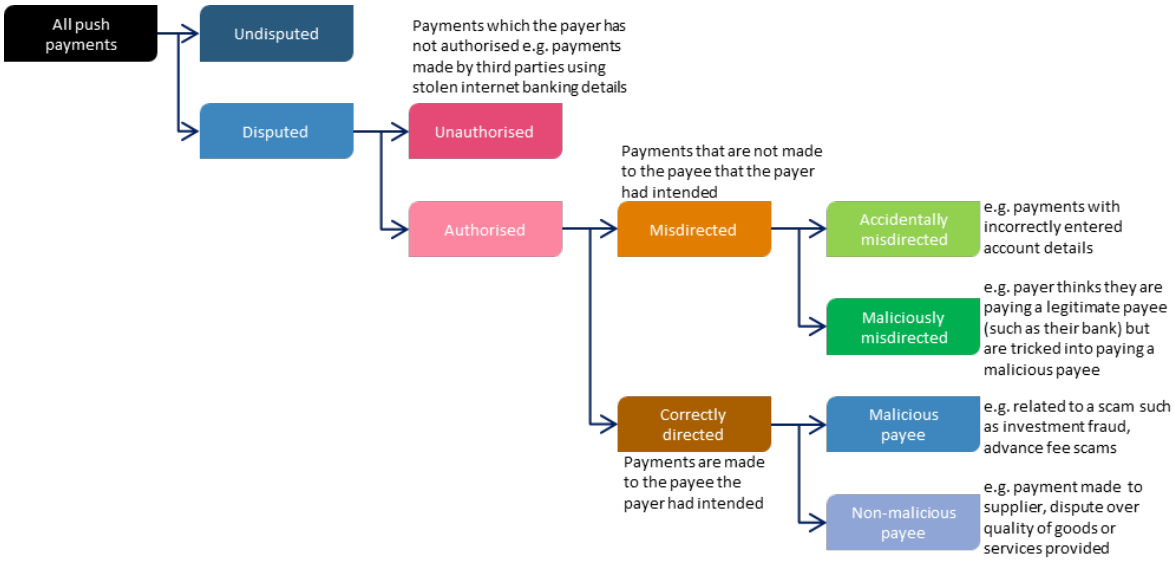
3.9 Respondents should note that we will not disclose confidential information that relates to the business or affairs of any person, which we receive for the purposes of our functions under the Financial Services (Banking Reform) Act 2013 (FSBRA), unless one of the following conditions apply:

- 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 1:
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 below).

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, APPs scams include **maliciously misdirected** payments and correctly directed payments to **malicious payees**.

Annex 2:
Summary of consultation responses

Summary

2.1 We received a total of 15 responses to our consultation on the draft ToR for this work, including eight responses from PSPs and two from PSOs (see Annex 3 for a full list of respondents). The majority of respondents were supportive or broadly supportive of this work and our proposed scope.

2.2 In this Annex we present a summary of the main issues raised in the responses we received. Issues are grouped based on the three questions we posed in the consultation. We then discuss a number of additional issues raised by respondents.

2.3 The three questions we asked were:

i) **Scope:** Do you think our scope, focusing on APP scams which target consumers, is appropriate?

ii) **Key questions:** Do you agree with the key questions we want to answer?

iii) **Timing:** Do you agree with the proposed timing for this project?

Scope

2.4 In our 2017/18 Annual Plan we set out that one of the key areas we plan to explore during the year is consumer protection and education in the payments sector. Our aim is to see what wider issues there are and whether it would be appropriate for us to respond to them. Where we have decided to not include areas of focus proposed by stakeholders within the direct scope of the project covered by these ToR, we will instead consider these issues as part of this wider work.

Focus on consumers as victims of APP scams

2.5 We received mixed views on our proposal to limit the direct scope of this work to APP scams involving consumers only. Several respondents explicitly supported the consumer-only focus. Two respondents thought that we should extend our scope to also include small businesses, noting that small businesses demonstrate similar payment behaviours to consumers, and also benefit from similar consumer-type protections under certain payments legislation (such as the Payment Services Regulations 2009). Two other respondents thought we should extend our scope to include businesses more generally.

2.6 We are of the view that our proposal to limit the direct scope of this work to APP scams involving consumers remains appropriate. Actions which benefit consumers would in many cases also benefit businesses. However, actively exploring APP scams specific to businesses (and potential proposals) 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. When we have completed this project we will consider any evidence we gather about APP scams affecting businesses, and consider whether further targeted work to look at these issues should be undertaken.

2.7 In developing any potential proposals, we will also consider what the appropriate beneficiaries should be for the given proposal (for example, consumers and small businesses).

Payment systems within scope

2.8 One respondent asked us to consider whether cheques should be in direct scope of this work, or in scope of a future review once the cheque imaging system has been implemented. They argued that excluding cheques could mean missing a vulnerable group of consumers who fall victim to scams by writing multiple cheques. As the direct focus of this work is on APP scams and given that the characteristics of cheque payments are significantly different to electronic push payments, we do not view it as appropriate to bring cheques into scope for this work at this time.

2.9 Another respondent argued that, given the upcoming consolidation of interbank payment systems in the UK (which will include Bacs), any proposals from this work may also impact on Bacs payments. As a result, they argued Bacs payments should be bought into direct scope for this work. The focus of this work is on scams relating to authorised push payments initiated by consumers. As consumers no longer make push payments using the Bacs system, we have excluded Bacs from the direct scope of this work. We will consider the potential interactions of any potential proposals we may make as a result of this work with the upcoming consolidation of interbank payment system operators.

2.10 One respondent, while agreeing with the direct scope being limited to CHAPS and Faster Payments, thought that consideration should also be given to how funds are finally withdrawn from UK payment systems and the ability to recover funds from fraudsters based outside the UK. While not central to the direct scope of this work, we agree that this is an important consideration and will consider it as part of developing our understanding of the wider context around APP scams.

Exclusion of 'on-us' payments from scope

2.11 Respondents expressed mixed views on our proposed position to exclude on-us payments from this work. Two respondents explicitly supported their exclusion from scope. One respondent recommended caution in excluding them, based on the view that customers should receive consistent treatment regardless of whether they are making an 'on-us' payment or not. As the focus of this work is on the potential expanded role of PSOs in preventing and responding to APP scams, 'on-us' payments are almost by de facto out of direct scope (as, by definition they do not flow through the central payment infrastructure). In developing any potential proposals we will, however, consider the implications for the relative treatment of 'on-us' payments.

Types of disputed payments in scope

2.12 The proposed scope of our work is limited to two types of disputed payments that result from APP scams –maliciously misdirected payments and correctly directed payments to malicious payees (see Annex 1 for a detailed discussion of the types of disputed payments).

2.13 One stakeholder suggested that we also include accidentally misdirected payments *within scope*, as potential solutions for maliciously misdirected payments may also address accidentally misdirected payments. Another stakeholder requested that we explicitly confirm that accidentally misdirected payments are *out of scope* of this work. Given the focus of this work is on APP scams, and that accidentally misdirected payments are not related to APP scams, we are not proposing to bring these types of disputed payment into scope. We will, however, consider the wider impact on other types of disputed payments of any potential proposals that emerge from this work.

2.14 A stakeholder suggested that we should exclude correctly-directed malicious payee payments from the scope of our work. They argued there is often limited distinction between correctly-directed malicious payee payments and correctly-directed, non-malicious payee payments (for example, what circumstances differentiate alleged scams or fraud from standard commercial disputes?). While we acknowledge the complexities of distinguishing between types of disputed payment in some circumstances, we are of the view it is not appropriate to exclude correctly-directed malicious payee payments from the scope of this work. Our work on the Which? super-complaint response showed that scams associated with these types of disputed payments are a significant source of consumer harm.

Key questions

General observations on our key questions

2.15 One respondent argued that, in answering our proposed key questions, our focus should be on observed outcomes (for example, relative levels of fraud incidence) as opposed to inputs alone. To clarify, we have added a statement in the ToR that we will seek to identify evidence on the effectiveness of specific practices in different jurisdictions, payment systems, and industries in addressing their targeted issue.

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

2.16 Several respondents emphasised the importance of considering the relevant domestic legal and regulatory context when comparing international practices around APP scams. We agree and have now made this explicit in the ToR.

2.17 Two respondents made proposals for relevant jurisdictional comparators. One respondent suggested an intra-EU comparison would be appropriate, given the maximum harmonisation requirements under the EU Payment Services Directives (PSD and PSD2). Another respondent suggested we consider the new instant payment systems under development in the EU and US. We will consider these suggestions as we develop the detailed approach to answering this question.

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

2.18 Several stakeholders highlighted the importance of considering differences in payment characteristics and underlying legal and regulatory context when comparing practices between different disputed payment types. We agree and have now made this explicit in the ToR.

2.19 Two stakeholders suggested that there may be relevant insights to gather from the PayM payment overlay service. We agree and have now explicitly included PayM within our scope.

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

2.20 One respondent emphasised that as scams evolve over time, any potential actions need to be effective at addressing both current and future APP scams. We agree and will take into account how to 'future-proof' any potential actions we consider.

2.21 One respondent argued that the wording of this question pre-supposed that actions to expand the role of PSOs in APP scams were required. They suggested prefixing this question with 'if appropriate'. We agree and have updated this question.

Timing

2.22 Two respondents argued that, given the harm being caused to consumers by APP scams, the PSR should undertake this work as swiftly as possible. We acknowledge the ongoing consumer harm caused by APP scams. We have developed our timetable to ensure we are able to come to a robust, evidence-based and proportionate decision about the appropriate role for PSOs in preventing and responding to APP scams.

2.23 Several respondents requested that we provide a more detailed timetable for this work to enable them to plan when their input may be required. Several other stakeholders urged that we allow stakeholders sufficient time to respond to any requests for information. In response to this feedback, we have now included an indicative timetable in the ToR (see Chapter 3). We will be mindful to allocate appropriate response times for any requests for information we make and, by using information we already have or which is in the public domain, to minimise the burden of any such requests.

2.24 Three respondents noted that interactions and timing of any actions following on from this work should have regard to other ongoing relevant industry and regulatory initiatives and developments. These include the Payments Strategy Forum's strategic plan (including development of the new payments architecture), PSD2, the CMA's Open Banking remedies, ring-fencing, and cheque imaging. We confirm that we will be mindful of these factors when developing any proposals as part of this work.

Other issues raised

2.25 Respondents raised several other issues on our draft terms of reference:

- One respondent suggested that any proposals resulting from this work should focus on facilitating market provision of competitive solutions, rather than picking specific solutions. As an economic regulator, we have a statutory objective to promote effective competition in the markets for payment systems and services. While we cannot prejudge the nature of any potential proposals resulting from this work, a high level of importance will be attached to the furtherance of this objective in developing any potential proposals.

- One respondent thought that we should be more explicit that the scope of this work is limited to considering the potentially expanded role of PSOs in preventing and responding to APP scams, rather than on other industry participants. For the avoidance of doubt, we confirm that the core focus of this current work is on the potentially expanded role of PSOs only.

- Stakeholders argued that if the PSR finds that action is needed to be taken by the PSOs in scope, then it would be helpful for this to be captured and adopted by other PSOs to ensure a consistent approach. As we develop any potential proposals as part of this work, we will take into consideration the relative costs and benefits of introducing potential cross-system consistency.

- In addition to taking into account wider industry and regulatory developments, one respondent emphasised the importance of working with all relevant stakeholders, including the Treasury, the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO) and the Open Banking Implementation Entity (OBIE). We will ensure that we undertake an appropriate level of engagement with relevant parties as our work progresses.

Annex 3:
List of consultation respondents

The table below presents a list of the respondents to our consultation on the draft ToR for this work.

Name	Category
Al Rayan Bank	PSP
Barclays	PSP
CHAPS Co	PSO
Experian	Information services company
Financial Fraud Action UK	Trade body
Faster Payments Scheme Limited	PSO
HSBC	PSP
Lloyds Banking Group	PSP
Nationwide Building Society	PSP
Private Citizen A	Private Citizen
RBS	PSP
Secure Trust Bank	PSP
Transpact	PSO
Vocalink	Payment system infrastructure provider
Which?	Consumer organisation

Annex 4: Glossary

Term or acronym	Description
Bacs	The regulated payment system which processes payments through two principal electronic payment schemes: Direct Debit and Bacs Direct Credit. The payment system is operated by Bacs Payment Schemes Limited (BPSL).
CHAPS (Clearing House Automated Payment System)	The UK's real-time, high-value sterling regulated payment system, where payments are settled over the Bank of England's Real time Gross Settlement (RTGS) system. It is operated by CHAPS Co.
CHAPS Co	CHAPS Clearing Company Ltd – the operator of the CHAPS payment system.
CMA	Competition and Markets Authority
FCA	Financial Conduct Authority
Financial Fraud Action UK (FFA UK)	An industry body responsible for leading the collective fight against financial fraud on behalf of the UK payments industry.
FPS (Faster Payments Scheme)	The regulated payment system that provides near real-time payments as well as Standing Orders. It is operated by Faster Payments Scheme Limited (FPSL).
FPSL	Faster Payments Scheme Ltd – the operator of the FPS payment system.
Information Commissioner's Office (ICO)	The UK's independent body set up to uphold information rights.
'on us' transactions	Transactions where the payee's PSP/payer's PSPs are the same entity and where the transaction is not processed by a central payment system.
PSD (EU Directive on Payment Services)	Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC of 13 November 2007, published in the Official Journal of the EU on 5 December 2007.
PSD2	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, published in the Official Journal of the EU on 23 December 2015.
Payment service provider (PSP)	Any natural or legal person authorised to provide the payment services listed in the Annex to Directive 2007/64/EC or recognised as an electronic money issuer in accordance with Article 1(1) of Directive 2009/110/EC (PSD1).
Payment Services Regulations 2009 (PSRs 2009)	These regulations implement Directive 2007/64/EC of the European Parliament and of the Council on payment systems in the internal market (PSD1). They came into force for most purposes on 1 November 2009.

Term or acronym	Description
Payments Strategy Forum (PSF)	The Payments Strategy Forum was announced by the PSR in its Policy Statement published in March 2015. The Forum is leading on a process that identifies, prioritises and develops strategic, collaborative initiatives that promote innovation for the benefit of those who use payment systems. More information on the Forum may be found on www.paymentsforum.uk.
Payment Systems Regulator (PSR)	The Payment Systems Regulator Limited, the body corporate established by the FCA under section 40(1) of FSBRA.
Payment system operator (PSO)	In relation to a payment system, any person with responsibility under a payment system for managing or operating it; and any reference to the operation of a payment system includes a reference to its management.
the Treasury	Her Majesty's Treasury.

25 The North Colonnade
Canary Wharf London
E14 5HS
Telephone: 0300 456 3677
Website: www.psr.org.uk