FINANCIAL CONDUCT AUTHORITY
PAYMENT SYSTEMS REGULATOR

Report and Consultation **CP17/2**

Authorised push payment scams

PSR-led work to mitigate the impact of scams, including a consultation on a contingent reimbursement model

November 2017

This paper sets out the work we've done to reduce the harm to consumers from authorised push payment scams. As part of this, we are consulting on:

- whether UK Finance's best practice standards will be effective in addressing the issues we identified in our super-complaint response
- our view that a contingent reimbursement model should be introduced, and how this should be achieved

Please send your comments on the consultation questions to us by 5pm on 12 January 2018.

You can email us at app-scam-pso-project@psr.org.uk or write to us at the following address:

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

You can download this document from our website: www.psr.org.uk/psr-publications/consultations/APP-scams-report-and-consultation-Nov-2017

Contents

Note: The places in this document where confidential material has been redacted are marked with a [✂].

1 Executive summary

1.1 This paper explains the work we've done in the past year to reduce the harm to consumers from authorised push payment (APP) scams – where people are tricked into sending money to a fraudster.

1.2 APP scams are a crime that can have a devastating effect on the victims. They are the second biggest type of payment fraud now reported by UK Finance, in both the number and total value involved (behind card fraud).

1.3 We've worked with the payments industry to develop and progress a number of initiatives that should help prevent these scams, and improve the response when they do happen. We've also continued to explore solutions that mean victims are less likely to be out of pocket. We consider a 'contingent reimbursement model' should be introduced to reimburse victims where banks have not met the required standards – provided the victims have taken appropriate care when making the payment. We are consulting to gather views on how it should work.

1.4 We believe our work with industry to progress all of these initiatives will make a positive difference, leading to better protection from scams and better support for victims

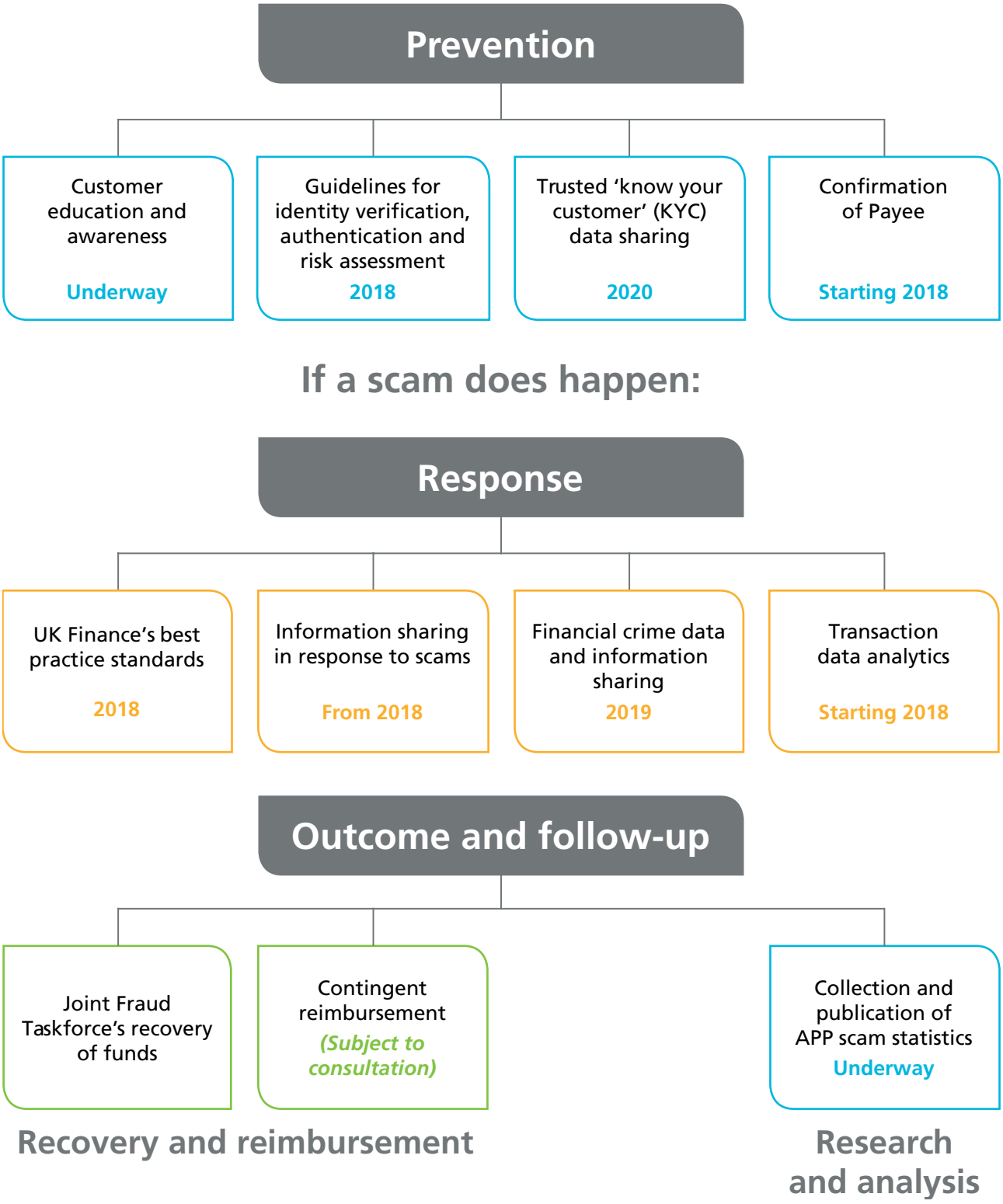
1.5 There is still no single solution, or 'silver bullet' that can prevent all APP scams. However, we believe that the industry initiatives underway, the introduction of a contingent reimbursement model, and continued efforts by all those involved should – together – have a significant impact on scams and reduce the harm they cause. Figure 1 presents an overview of all of these initiatives, broken down by those that should assist with APP scam prevention, response and outcomes. Although some of them will take time to implement, others are already underway.

Why we're publishing this document

1.6 In September 2016, the consumer body Which? submitted a super-complaint to us about APP scams, raising its concerns that victims don't have enough protection. We investigated the issue and the concerns raised, and in December 2016 published our response. We found that APP scams are a growing issue that causes significant harm to victims and that more needs to be done to address them.

1.7 We announced a programme of work to be done by ourselves and the payments industry. The Financial Conduct Authority (FCA) also agreed to do work in this area. This document sets out the progress and outcomes of this work and the next steps we propose.

Figure 1: Measures to assist with APP scam prevention and response



Preventing and responding to scams

The industry's progress

1.8 With our oversight, the industry (as represented by UK Finance) has made good progress in the three areas of work it took on:

- **Statistics:** In December 2016 we said that the data available on the scale and type of APP scams was poor. We said that there needed to be better quality reporting to help raise awareness and understanding. Industry has published the first set of robust statistics on APP scams, and from 2018 it will collect and publish more detailed data. This is essential to get a clearer understanding of the scale of the problem, as well as more insight to help develop fraud prevention measures and assess their effectiveness.
- **Best practice:** We said that payment service providers (PSPs), which include banks, could do more to assist people reporting an APP scam by being more joined up. The industry has now developed best practice standards that PSPs will follow when a victim reports an APP scam. This should improve consumers' experience and PSPs' response times. The FCA also welcomes these standards.
- **Data sharing:** We said that the industry needed to develop a common understanding of the information that could be shared under existing law and the key legal barriers to sharing further relevant information. Industry has developed a common understanding of what information PSPs can share under current law when responding to APP scam claims. This should help them respond more effectively. More work will also be done to allow for the continued sharing of information under proposed new legislation and to facilitate the recovery of victim's funds.

1.9 There are also a number of industry initiatives underway that, taken together, should help to prevent scams in the first instance, ensure PSPs respond faster when they do happen, and help in recovering the victim's money. We are driving many of these initiatives through the Payments Strategy Forum and UK Finance. Examples include introducing Confirmation of Payee, sharing financial crime data and information, and transaction data analytics.

1.10 While the industry has made significant progress on these initiatives, it is essential that this continues. To make sure this happens we have set out expected milestones for each initiative. UK Finance and the new payment system operator (which will govern the Bacs, Faster Payments and Cheque and Credit systems) will report to us every six months, starting June 2018, on each initiative's progress against these milestones.

1.11 The FCA reviewed the way PSPs handle APP scams. It found PSPs' procedures were inconsistent, their existing fraud detection systems could not easily detect APP scams, and they didn't collect enough data. The FCA considers the industry initiatives underway will help to tackle these issues.

The payment system operators' role

1.12 Payment system operators are the governing bodies that set the rules for each system and ensure that it works as it should. In December 2016, we committed to consider whether the operators of Faster Payments and CHAPS could play an expanded role in addressing APP scams. We got insights by examining practices in other payment systems, countries and sectors. We found that the industry initiatives underway in the UK will bring practices into line with those we saw elsewhere, with one exception: reimbursement. Other UK payment systems (such as card systems) and sectors have formal arrangements for reimbursement to make sure PSPs act in customers' best interests – and reimburse them if they don't. Operators play varied roles in these reimbursement models in other systems and sectors.

Reimbursing victims

1.13 We believe more can be done in the area of reimbursement, and so does the industry: Financial Fraud Action UK (now integrated into UK Finance) proposed the concept of a model that sets out the circumstances when PSPs would be responsible for reimbursing APP scam victims that have acted appropriately. Depending on the circumstances, this could be the victim's PSP or the PSP that received the money on behalf of the fraudster.

1.14 This is an example of a voluntary contingent reimbursement model, where reimbursement depends on whether the PSPs involved have met required standards, such as measures and processes that help prevent and respond to scams, and whether the victim has taken the requisite level of care.

1.15 We consider that a contingent reimbursement model should be introduced for victims of APP scams, led by industry and should be in place by the end of September 2018. In this document, we are consulting on the model and how it should be designed and implemented.

1.16 We see merit in introducing this kind of model because:

- It should increase the incentives for PSPs to invest in and maintain practices that help prevent and respond to APP scams. Consumers would continue to take care when making payments because they would need to meet a requisite level of care to be eligible for reimbursement.
- It should reduce consumer harm by reimbursing victims when they could not have reasonably prevented the scam – but their PSP, or the PSP used by the fraudster, had not met the required standards.
- Including the measures being developed by industry as part of the standards of the model should also ensure PSPs implement and use those measures.

1.17 We propose to actively monitor the industry's work on this. We also set out in this paper the high-level principles we think an effective model should meet.

1.18 In particular, we think the victim should only be eligible for reimbursement when they meet the requisite level of care. Where the victim is eligible and one, or both, of the PSPs did not the meet the standards set out in the model, then the PSP(s) at fault should reimburse the victim. As part of our consultation, we are also asking for views on the appropriate outcome in circumstances where all parties have acted appropriately and met the standards set out in the model.

1.19 We look forward to receiving responses to our consultation and then, working with industry and other key stakeholders, taking proposals for the development of a contingent reimbursement model forward as appropriate.

2 Introduction

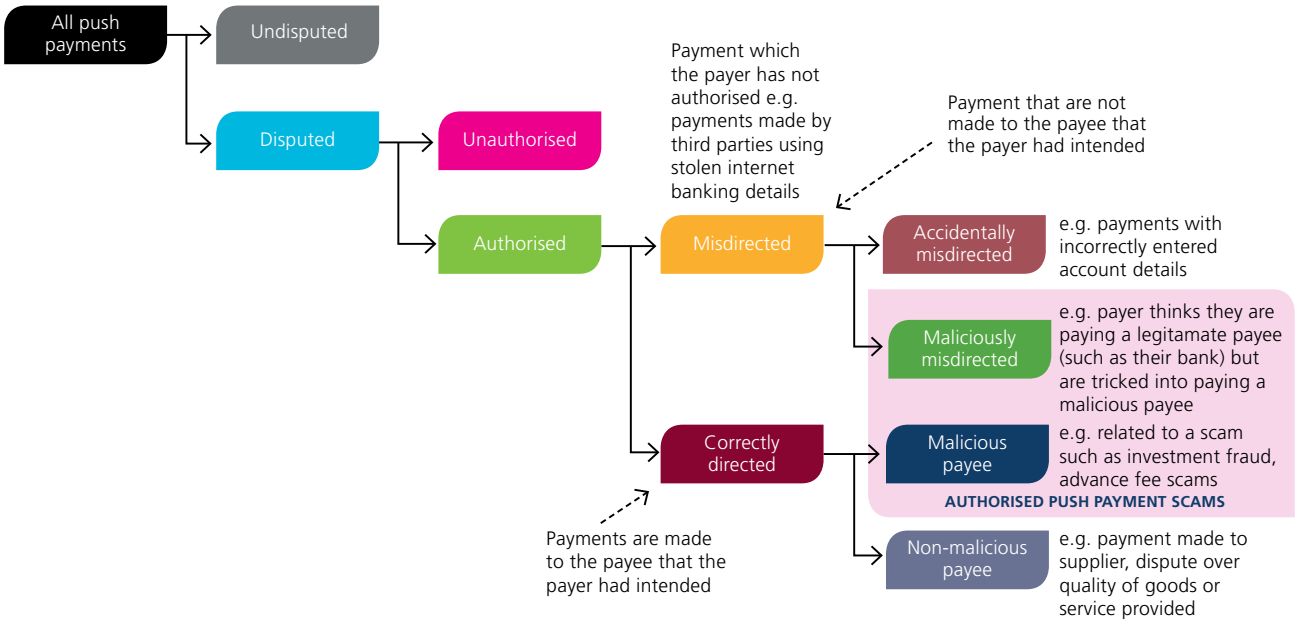
The background to our work on APP scams

2.1 On 23 September 2016, we received a super-complaint from the consumer body Which? about protecting consumers from harm caused by APP scams. Which? raised concerns that there is insufficient protection for people who are tricked into sending money to a scammer as an APP via the banking system.

2.2 Push payments are payments where payment service providers (PSPs), which include banks, are instructed to transfer money from a customer's account to another account. It is an 'authorised' push payment when the customer gives their consent for the payment to be made – this can include situations where the customer has been tricked into giving that consent. Payments related to APP scams can be made over the phone, via online banking, or in person, and most are completed instantly.

2.3 Figure 2 outlines the different categorisation of push payments and highlights which of these are related to APP scams.

Figure 2: Categorisation of push payments



2.4 After receiving the super-complaint, we investigated the problem of APP scams to better understand the issue and Which?'s concerns. On 16 December 2016 we published our response to the super-complaint, setting out our main findings and next steps.[1]

2.5 We identified that APP scams are a growing problem, and more needs to be done to tackle them. We considered wider industry and policy developments already planned or underway that had the potential to help reduce consumer harm from APP scams. We then identified three issues that needed to be addressed:

- The data available on the scale and types of APP scams is of poor quality and needed to improve.
- The ways in which PSPs work together in responding to reported APP scams needed to improve.
- Some evidence suggested that some PSPs could do more to identify potentially fraudulent incoming payments, and to prevent accounts falling under the influence of scammers.

Our work programme on APP scams

2.6 To address the issues we identified, we announced a programme of work that would be undertaken by ourselves and the payments industry (as represented by Financial Fraud Action UK, which has since become part of UK Finance). The Financial Conduct Authority (FCA) also agreed to do work in this area.

2.7 The overall work programme included several streams:

- With our oversight, the industry (as represented by UK Finance) agreed to do work that would increase understanding of the scale of APP scams and improve how PSPs work together to respond to them. We identified three specific areas for industry to work on:
  - Develop, collect and publish robust APP scam statistics, to address the lack of clear data on the scale and scope of the problem.
  - Develop a common approach or best practice standards that sending and receiving PSPs should follow when responding to APP scams.
  - Liaising with the Information Commissioner's Office (ICO) as appropriate, to develop a common understanding of what information can be shared under the current law, and the key legal barriers to sharing further relevant information
- We committed to considering the potential for the operators of CHAPS and Faster Payments Scheme (FPS) payment systems to play an expanded role in helping to minimise the consumer harm caused by APP scams. We said we would publish the findings on this work in the second half of 2017.
- The FCA took the following actions:
  - Work with PSPs to tackle concerns around both sending and receiving PSPs in relation to APP scams.
  - Examine evidence received in relation to the super-complaint to address any firm-specific issues directly.
  - If, following the above steps, there are unresolved sector-wide issues, the FCA will initiate further work.

1 Payment Systems Regulator (December 2016) *Which? authorised push payment super-complaint: our response:* www.psr.org.uk/psr-publications/news-announcements/which-super-complaint-our-response-Dec-2016

2.8 As part of our work we also considered other initiatives currently underway that could help address APP scams, including those proposed by the Payments Strategy Forum (the Forum).

Findings and outcomes

2.9 In this report we present the findings and outcomes of the work programme and the next steps. This includes our consultation on a voluntary contingent reimbursement model that, alongside other developments, could help better protect consumers from the harm caused by APP scams.

2.10 This document is structured as follows:

- **Chapter 3** sets out our assessment of the industry's (as represented by UK Finance) progress in the three areas of work it took on following the super-complaint.
- **Chapter 4** outlines our work through the Forum and other industry and regulatory developments that can help address APP scams. This includes the findings and outcomes of the work the FCA undertook following the super-complaint.
- **Chapter 5** provides a summary of our work considering the role of the operators in APP scams and our findings.
- **Chapter 6** presents our consultation on a voluntary contingent reimbursement model.
- **Chapter 7** outlines the next steps we will take regarding the consultation.
- A **glossary** is also included at the end of this document.

2.11 There are four annexes to this report that are in a separate document. The first sets out the consultation questions. The remaining three annexes outline further considerations relating to our work on the role of the operators in addressing APP scams.

3 Our assessment of the industry's progress against agreed actions

Key points

- The industry has made good progress against the three key areas of improvement we identified in our super-complaint response.
- For the first time, robust and clear statistics have been published that show the extent and nature of APP scams in the UK. More detailed data will soon be published. This will help raise awareness of the problem among industry and consumers.
- Industry has developed and started to implement common standards that should see people with APP scam complaints dealt with more quickly, kept better informed and provide a better chance to recover their money.
- There has been progress in developing a common understanding of what information can be shared between PSPs to help process scam claims, but there is more that needs to be done on information sharing. Addressing this could depend on how legislative proposals develop.

3.1 In this chapter we consider UK Finance's progress in the three areas identified in our super-complaint response.[2]

3.2 At the time, we agreed these actions with Financial Fraud Action UK (FFA UK), the body responsible for leading the collective fight against financial fraud on behalf of the UK payments industry. Its membership includes the major banks, credit, debit and charge card issuers, and card payment acquirers in the UK. In July 2017, FFA UK became a constituent part of UK Finance, the new trade association representing the UK financial services industry. We refer to the latter in the rest of this chapter, unless specified. UK Finance's work on APP scams has been done with those FFA UK-member PSPs that provide push payment services to consumers – these PSPs are UK Finance's retail bank members. These PSPs collectively account for a significant majority of the retail banking market.[3] We now outline the agreed actions.

3.3 In their super-complaint, Which? highlighted the lack of public data on APP scams to reliably to estimate the current scale of the problem. We agreed that there was very limited public data available. We asked UK Finance to **develop, collect and publish robust APP scam statistics**, to address this problem and enable monitoring of the issue over time.

3.4 Another of our conclusions was that PSPs need to **improve how they work together in responding to reports of APP scams from customers**. We asked UK Finance to develop a common approach or best practice standards that sending and receiving PSPs should follow when responding to instances of reported APP scams. We agreed with UK Finance that they would work on improvements in the speed with which PSPs respond, the information they exchange with each other to address the complaint, and the way in which they keep the complainant informed. This should improve customers' experience when their claims are being processed (by having a single PSP managing the improved process and keeping them informed). It should also help PSPs get the information they require to respond to reports of APP scams.

2 Payment Systems Regulator (December 2016) *Which? authorised push payment super-complaint: our response:* www.psr.org.uk/psr-publications/news-announcements/which-super-complaint-our-response-Dec-2016

3 As measured by market share of personal current accounts. FFA UK's membership includes all of the banks that were part of the CMA's recent analysis of market shares in the personal current account market. See Table 5.1 of CMA (2016) Retail banking market investigation – Final report: https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

3.5 We also noted in our super-complaint response that there was no industry consensus on what information could be shared between PSPs when examining APP scam claims. The PSPs' varied interpretations of the law appeared to have led to inconsistent practices; this frustrated the actions of public authorities in taking action against scammers, and made it harder for consumers to get their money back. We therefore agreed with UK Finance that it would **develop a common understanding of what information can be shared under the current law**, and the key legal barriers to sharing further relevant information.

APP scam statistics

3.6 Following our response to the super-complaint, UK Finance began collecting figures on the volume, value and victims of APP scams. It split the data into 'personal accounts' and 'non-personal accounts', as well as the value returned to victims. It has published these figures for the first half of 2017, which are shown in Table 1.[4]

Table 1: APP scam statistics, January to June 2017

	Personal	Non Personal	Total
Total cases	17,064	2,306	19,370
Total victims	16,993	2,244	19,237
Total value	£51,664,722	£49,526,924	£101,191,645
Total returned to victim	£9,813,650	£15,404,140	£25,217,791

Source: UK Finance

3.7 From January 2018, UK Finance will also begin collecting data on a significantly larger set of categories, including the type of scam (including categories within maliciously misdirected and malicious payee[5]), the payment system used, the channel (online, in-branch etc.) and the time taken in the various steps of scam investigation.

3.8 These published figures give a clearer idea of the scale of the problem. They also allow us to compare APP scam losses to those from other financial fraud. For example, according to UK Finance, fraud losses on UK-issued payment cards (the largest type of reported fraud) totalled £287.3 million across 918,000 cases in the first half of 2017.[6] While APP scams are clearly much less prevalent than card fraud (roughly 20,000 compared to 918,000) they still amount to a significant loss and appear to be a growing problem. APP scams are now the second biggest type of payment fraud, in both volume and value terms, reported by UK Finance. They are larger in both volume and value terms than unauthorised online banking fraud. The level of unauthorised online banking fraud in the first half of 2017 was approximately 11,700 cases, amounting to losses of £55.5m.[7]

3.9 The figure for the money returned to APP scam victims – around 25% of the total value – is made up of partial or total recovery of funds, as well as goodwill payments made by PSPs in some cases. While this indicates that some money is returned to victims, it also shows the considerable improvement that can be made from the various initiatives being implemented throughout the industry. It will also provide a baseline from which to assess the success of those initiatives.

4 www.ukfinance.org.uk/authorised-transfer-scams-data-h12017/
5 We describe the different types of APP scams in Figure 2 at paragraph 2.3.
6 Financial Fraud Action UK, *2017 Half year fraud update*, p2.
7 Financial Fraud Action UK, *2017 Half year fraud update*, p7.

3.10 We consider that collecting and publishing detailed and robust statistics should provide an understanding of the current APP scam landscape (and how this changes over time), greater insight for fraud prevention measures, and greater transparency for monitoring of APP scam prevention and response measures. For example, collecting statistics on the type of APP scams will help understand the magnitude of maliciously misdirected APP scams that Confirmation of Payee should help prevent (we describe how this works in Chapter 4). The inclusion of more detailed categories will enhance this value further and allow the evaluation of specific anti-fraud measures. We are therefore satisfied with industry's progress on this issue so far.

Best practice standards

3.11 In order to address our conclusion that the industry needed to improve the way it works together in responding to APP scams, UK Finance drafted a set of best practice standards that sending and receiving PSPs should follow when responding to instances of reported APP scams. UK Finance developed and discussed at length these standards with its PSP members that are retail banks and offer push payment services. The standards were finalised with the agreement of these members.

3.12 UK Finance has published a summary of these best practice standards (called the APP claim reporting standards).[8] The standards cover 16 steps in the processing of an APP scam claim, and address issues such as 24-hour availability of fraud specialists, processes for notifying and assessing claims, and blocking funds between PSPs. The steps include:

- actions taken when the victim contacts their PSP, including the victim's PSP assessing the claim type (whether it is a scam or other disputes, for example about goods and services), capturing details of the alleged scam, and notifying the PSP that received the funds
- actions taken by the receiving PSP, including assessing the notification and information provided by the victim's PSP and taking any appropriate action (such as freezing an account). It will recover funds where possible and appropriate, and reimburse the victim if it can

3.13 The PSP of the customer making the APP scam complaint will remain their sole point of contact and will administer the process of the claim. This should reduce instances of the customer being inadequately informed or 'passed around' different organisations when trying to find out the status of their claim. The standards also include a clearly defined set of information that the victim's PSP should provide to the receiving PSP so it can assess the claim, as well as 'service level' timings for the various steps of the process, where these are within the control of the PSPs involved.

3.14 UK Finance's PSP members that are retail banks and offer push payment services agreed to fully implement these standards by Q3 2018. These PSPs collectively provide a significant majority of personal current accounts.[9] Some of these PSPs are already fully implementing the standards ahead of time (notwithstanding issues around some legal aspects – see below).

3.15 In developing these standards, UK Finance has addressed many of the issues around the need for a common understanding of what customer data can be shared in dealing with APP scam complaints. This is on the basis of current data privacy laws. There are outstanding issues around information sharing, which UK Finance considers is not in the power of the organisations involved to address at this stage. We discuss this in paragraphs 3.19 to 3.24.

8 The summary of the best practice standards – the APP Claim Report Standards – can be found in Notes to the Editor 3 in UK Finance's press release: www.ukfinance.org.uk/authorised-transfer-scams-data-h12017

9 As measured by market share of personal current accounts. FFA UK's membership includes all of the banks that were part of the CMA's recent analysis of market shares in the personal current account market. See Table 5.1 of CMA (2016) Retail banking market investigation – Final report: https://assets.publishing.service.gov.uk/media/57ac9667e5274a0f6c00007a/retail-banking-market-investigation-full-final-report.pdf

3.16 As a result of this standardisation, customers who contact their PSP to complain about a possible APP scam should have their issue dealt with more quickly, be kept better informed, and could have a better chance of recovering their money. This should significantly improve the consumer's experience when reporting APP scams. The standards should mean that PSPs respond to scams faster and have better information, limiting the time available for scams to be fully executed. This may mean more accounts are identified and frozen, and more money ultimately returned. We are therefore satisfied with industry's progress on this issue and welcome the implementation of these standards. The FCA also welcomes these standards as a first step in tackling some of the issues it has identified – we outline the FCA's findings and actions in paragraphs 4.14 to 4.20.

3.17 To ensure these standards are effective, we also want your feedback on whether the standards (published by UK Finance) will address the issues we identified in our response to the super-complaint and improve how PSPs respond to APP scam claims. We will consider these responses and whether UK Finance should make changes to improve the standards. (Annex 1 is a list of our consultation questions.)

3.18 We will also want to see how these standards work in practice and, in due course, we may look for changes and enhancements, where appropriate, to ensure these standards are effective.

Question 1: In your view, will the best practice standards developed by UK Finance be effective in improving the way PSPs respond to reported APP scams? Please provide reasons.

Improved information sharing

3.19 The industry has made good progress in developing a common understanding of what information can be shared between PSPs under the current law, for the purposes of processing APP scam claims. This is on the basis of the provisions of the Data Protection Act 1998. This common understanding on information sharing underpins the best practice standards.

3.20 However, there is still work to be done on other aspects of information sharing and in relation to the recovery of victim's funds. Addressing these issues may require legislative change or developments.

3.21 UK Finance is seeking to ensure that PSPs can continue sharing relevant information under the best practice standards when the new Data Protection Bill becomes law. The new provisions are due to come into force by May 2018 and will replace the Data Protection Act 1998.

3.22 UK Finance has stated that, in the immediate future, it will be seeking to agree a privacy impact assessment and put in place a data-sharing agreement between its member PSPs (with the involvement of the Information Commissioner's Office (ICO) as appropriate). The data sharing agreement is intended to set out the basis upon which the PSPs will share information and the processes they will follow when doing so. UK Finance has also agreed to explore and progress any legal changes or developments that they believe are needed to continue to share relevant information when the Data Protection Bill becomes law.

3.23 In relation to the recovery of victim's funds, the Joint Fraud Taskforce, and UK Finance as part of it, is developing a framework for a funds repatriation scheme – so that stolen money can be tracked across payment systems, frozen, then returned to the victim of the crime (see the box on page 25 regarding the recovery of victim's funds). This may require legislative change.

3.24 We acknowledge that addressing these potential legal barriers will require efforts from outside industry. However, we think UK Finance is well placed to progress these issues and to collaborate with other industry and government work in these areas, including any initiatives for legislative change. We will support UK Finance initiatives where we agree with the proposals.

Our overall assessment

3.25 We consider that the industry, through UK Finance, has made good progress on the issues we asked it to address. However, there is still work to be done – both in continually assessing the effectiveness of the measures put into place to address APP scams, and to seek to address the longer term legal issues it has identified.

3.26 As outlined in Chapter 4, we have agreed with UK Finance that it will report to us every six months on the progress of each of these initiatives. If progress slows or is not sufficient to achieve the outcomes we expect, then we will consider appropriate regulatory action.

4 Our work through the Forum and other industry and regulatory developments

Key points

- Existing initiatives by the Payments Strategy Forum and payments industry should have a strong collective impact on reducing the incidences and harm caused by APP scams.
- We have set milestones that we expect industry to meet; UK Finance and the new payment system operator have agreed to report to us every six months. The first report is due in June 2018.
- In its work, the FCA found that PSPs' procedures for responding to APP scams were inconsistent, their existing fraud detection systems could not easily detect APP scams, and they didn't collect enough data. The FCA considers the industry initiatives underway will help to tackle these issues. It will continue to consider the impact of these initiatives.

4.1 Over the past year, there have been a number of developments that are underway or planned that should have a significant impact on APP scams.

4.2 The Payments Strategy Forum (the Forum) and other industry bodies are leading a number of initiatives, most of which we have overseen. These include measures to help prevent APP scams, alleviate the problems they cause, and return as much money as possible to the victims.

4.3 There have also been regulatory developments, with the Financial Conduct Authority (FCA) doing important work with PSPs that will help better protect consumers from APP scams.

4.4 We set out here the wider industry developments and the outcome of the FCA's work.

Our work through the Forum, UK Finance and other industry developments

4.5 The payments industry is undertaking a range of initiatives that we think should help give consumers better protection from APP scams. Many of these initiatives have been driven by the Forum, which we have close oversight of. We also include here the work of UK Finance that we have overseen, which came out of our work on the super-complaint (see Chapter 3), and work by the Joint Fraud Taskforce.

4.6 Most of the measures, and greater concentration of resources, are aimed at preventing APP scams. We recognise that stopping scams from happening in the first place is the best protection for consumers. There are also initiatives to develop measures to improve how PSPs respond to scams if they do occur. Finally, there are initiatives in place aimed at helping recover the funds of victims, and to better understand the scams so industry can continually improve its ability to stop them.

4.7 We consider that, collectively, these initiatives should have a strong impact on reducing consumer harm from APP scams. We set out below each of the initiatives, some of which are already in place, and describe how these will help protect consumers. Figure 1 in the executive summary shows how these measures, along with a voluntary contingent reimbursement model which we propose in Chapter 6, work together to help protect consumers against APP scams.

4.8 It is important that these initiatives we have identified – specifically, those being led by the Forum and UK Finance – are delivered in a timely manner. We therefore also set out below milestones for these initiatives that we expect industry to meet, and how these will be monitored.

Overview of measures to address APP scams

4.9 We present an overview of measures to address APP scams broken down into three categories:

- prevention
- response
- outcomes and follow-up

Prevention measures

Consumer education and awareness

Led by: The Forum, UK Finance and Joint Fraud Taskforce

Timing: Underway

What problem does it address?

Consumers are being tricked by scammers.

How will it help?

Consumers should be able to better spot and avoid scams.

The Forum handed over its work on improving consumer education and awareness through a joined-up industry approach to UK Finance for implementation earlier this year.[10]

UK Finance is coordinating with the Home Office's Joint Fraud Taskforce on a national programme raising awareness of financial crime and fraud called *Take Five to Stop Fraud*.[11] The first phase was launched in September 2016, and the second phase in September 2017. UK Finance and the Home Office are monitoring the effectiveness of the programme. Both the Joint Fraud Taskforce and the Forum are tracking the progress of this work.

Efforts to educate consumers about financial crime and fraud will be made more effective by better industry collaboration and coordination. This will give consumers the tools to help protect themselves against APP scams – by identifying and avoiding scams, and avoiding the risk of scammers using their accounts as 'mule accounts'.

10 Payments Strategy Forum (November 2016) *A payments strategy for the 21st Century: supplementary documents – solution descriptions*, page 32: consultation.paymentsforum.uk/final-strategy
11 takefive-stopfraud.org.uk

Guidelines for identity verification, authentication and risk assessment

Led by: The Forum

Timing: 2018

What problem does it address?

PSPs could have a more consistent approach to identity verification.

How will it help?

Criminals should find it harder to set up accounts to use for scams.

The Forum handed over to UK Finance the development of best practice guidelines for PSPs when verifying a user's identity. The guidelines will also cover how identity verification is managed across different types of payments.[12]

These guidelines should make identity verification more effective and reduce the potential risk when transferring money using different payment types. This should make it harder for fraudsters to open accounts to use for scams.

UK Finance is expected to produce a first draft of the guidelines by the end of 2017, and publish the final guidelines by the end of June 2018.

12 Payments Strategy Forum (July 2017), *Supporting paper 9: Guidelines for Identity Verification, Authentication and Risk Assessment:* implementation.paymentsforum.uk/consultation

Trusted 'Know Your Customer' (KYC) data sharing

Led by: The Forum

Timing: 2020

What problem does it address?

KYC fraud prevention measures are difficult and costly for PSPs, and sharing data on this could be more efficient.

How will it help?

PSPs should more quickly and easily spot scammers – and help stop them opening accounts to use for scams.

The Forum is developing industry collaborative standards and rules for a data sharing framework that PSPs (and possibly other participants) will use to store and share KYC data, initially focusing on business customers (small and medium sized enterprises).[13] KYC checks are part of the fraud prevention measures PSPs are required to take individually.

The industry said that currently it can be difficult and costly for PSPs to get enough information for their KYC checks on new customers, particularly business customers. The KYC data sharing framework should give PSPs quicker access to more robust data. It should also enable a competitive market to develop for KYC value-added products for PSPs to use. This should result in more efficient and effective KYC and anti-money laundering checks, giving PSPs a better chance of detecting fraudsters – which should make it harder for fraudsters to open accounts to use in scams.

The Forum has consulted on this work and is due to consider by whom and how this work is taken forward. The Forum has proposed that the KYC data sharing framework standards and rules are published in the second half of 2018, with competitive KYC value-added products to launch in 2020.

13 Payments Strategy Forum (July 2017), *Supporting paper 7: Trusted KYC Data Sharing*

Confirmation of Payee

Led by: The Forum and the New Payment System Operator (NPSO)

Timing: Progressively to 2021

What problem does it address?

Payee names on accounts are not checked before a payment is sent.

How will it help?

Customers can verify that they're paying the person they intended.

When a person is sending money to a new payee, Confirmation of Payee will check that the sort code and account details entered match the intended payee.[14] The person would be notified if the details don't match the name they've entered, and they can choose not to proceed with the payment.

While PSPs ask for the account name when making a payment, they do not currently check if it is correct. Using Confirmation of Payee before sending a payment will help stop maliciously misdirected APP scams (for example, where the scammer is pretending to be someone you know). It will also help stop fraudsters using the new Request to Pay[15] service for these types of APP scams.

By the end of 2017, the Forum will finalise the industry collaborative rules and requirements for a Confirmation of Payee solution that multiple providers can then offer to PSPs. These will be passed over to the NPSO so that Confirmation of Payee solutions can be used in the New Payments Architecture (NPA) that will be implemented in 2021. The rules and requirements can be used to implement solutions in the interim.

The NPSO is the governing body of the new payment system that will launch in 2018, combining the existing Bacs, FPS and Cheque and Credit systems.

14 Payments Strategy Forum (July 2017), *Blue print for the Future of UK payments: A consultation paper*, page 32
15 Payments Strategy Forum (July 2017), *Blue print for the Future of UK payments: A consultation paper*, page 24

Response measures

Best practice standards for responding to APP scam claims (APP claim reporting standards)

Led by: UK Finance

Timing: 2018

What problem does it address?

PSPs could respond more consistently and efficiently to scams.

How will it help?

Sets out how PSPs work together to respond to scams faster and more effectively.

As we noted in Chapter 3, UK Finance has developed a set of standards that sending and receiving PSPs will follow when processing an APP scam claim. The adoption of these standards should greatly improve the experience for victims, with better information flows between PSPs and faster response times on APP scam claims. A more effective response to APP scam claims may also mean PSPs identify and freeze more accounts, which could mean they can return more money to victims.

UK Finance members that are retail bank PSPs and provide push payment services agreed to adopt these standards. Some of these are already fully implementing the standards. UK Finance has committed to having all of its retail bank members that provide push payment services implement them by Q3 2018 (see Chapter 3 for more details).

Information sharing in response to APP scams

Led by: UK Finance

Timing: 2018

What problem does it address?

No industry consensus of what information could be shared between PSPs when responding to scams and recovering victims' money.

How will it help?

A better understanding can help PSPs work together to respond to scams faster and more effectively.

As we noted in Chapter 3, UK Finance has been leading work to clarify what information PSPs can share with each other under the current law when responding to an APP scam. It has also identified potential legal barriers to sharing relevant information under future data privacy legislation and in relation to the recovery of victim's funds. UK Finance is assisting in addressing these barriers and we will continue to monitor UK Finance's progress. A better understanding of what information can be shared should improve the process for recovering victims' money.

UK Finance has used a large part of this work to develop the best practice standards, which will be fully implemented by its retail bank members that provide push payment services by Q3 2018.

Financial crime data and information sharing

Led by: The Forum and UK Finance

Timing: 2019

What problem does it address?

Data sharing on financial crime and information is limited, making it hard to detect and prevent criminal activity.

How will it help?

More effective data sharing will make it harder for scammers to open or take over accounts.

The Forum has handed over to UK Finance work to:

- create a more effective model and roadmap for financial crime data and information sharing
- examine options for stronger industry capacity and capability on financial crime data and information
- work with the government to develop a more effective legal framework on data and information sharing for the purposes of detecting and preventing all types of financial crime[16]

Historically, data sharing between PSPs has been limited, incomplete and inconsistent. More sharing of financial crime intelligence will help detect and prevent criminal activity. It should make it harder for fraudsters to get access to money mule accounts that they use for scams.

UK Finance is carrying out detailed analysis and planning for these activities over the next two years. We understand that elements of this work are now being taken forward by government. We recognise that progress will depend in some part on the extent to which legislative changes may be required.

16 Payments Strategy Forum, *Supporting paper 11: Financial crime data and information sharing* (July 2017)

Transaction data analytics

Led by: The Forum and the NPSO

Timing: Progressively to 2021

What problem does it address?

Participants in the payment chain do not have the ability to analyse network-level data to assist with APP scam prevention and response.

How will it help?

Better ability to shut down mule accounts, and to spot potential fraudulent payments.

This is an initiative that analyses network-wide payment transaction data to help identify money mule accounts and the flow of funds related to fraudulent activity.[17] It can help protect consumers against APP scams because it should lead to a reduction in mule accounts, thereby making it harder for fraudsters to use them. It could also potentially be used for more efficient recovery of victims' funds (work is underway on this) after the scam occurs, and for real-time prediction of payments that may be fraudulent – which could help prevent more APP scams. This solution would also be beneficial for PSPs' wider financial crime prevention practices.

By the end of 2017, the Forum will finalise the industry collaborative rules and requirements for the transaction data analytics solution. It can then be competitively offered by multiple providers to PSPs. The Forum expects to hand these rules over to the NPSO so that solutions can be made available progressively, with competing solutions available when the NPA is implemented in 2021. We understand that industry participants are looking to implement a transaction data analytics solution in the interim that would cover FPS and Bacs transactions.

17 Payments Strategy Forum (July 2017), *Supporting paper 6: Payments Transaction Data Sharing and Data Analytics*

Outcomes and follow-up

APP scam statistics

Led by: UK Finance

Timing: Underway

What problem does it address?

There was little authoritative data available about APP scams.

How will it help?

More accurate and comprehensive statistics will help the industry analyse and combat scams better.

As we noted in Chapter 3, UK Finance has started collecting statistics on APP scams and has now published the first set of these and it will begin collecting more detailed data on scams from 2018. Previously, the data available on the scale and types of APP scams was of poor quality. Regular, ongoing collection and publication of robust statistics will provide a better understanding of current APP scams issues and how they change over time. It also allows for monitoring the performance of fraud prevention measures in place, and for greater insight for improving fraud prevention measures over time. For example, collecting statistics on the type of APP scams will help understand the magnitude of maliciously misdirected APP scams that the Confirmation of Payee solution will help prevent, and how effective it is at preventing that type of scam.

UK Finance has committed to publishing these statistics on a six-monthly basis.

Recovery of victims' funds

Led by: Joint Fraud Taskforce

Timing: Potentially 2 to 3 years' time

What problem does it address?

It can take time for PSPs to trace a victim's money, determine if they can get their money back and, if they can, for the money to be returned.

How will it help?

PSPs should more quickly and easily trace a scam and, if possible, return money to victims.

The Joint Fraud Taskforce is developing a framework for a funds repatriation scheme – so that stolen money can be tracked across payment systems, frozen, then returned to the victim of the crime. This should also stop criminals from getting the money.

The work being done by industry participants on using transaction data analytics for funds repatriation will help inform the design and implementation of this repatriation framework and what legislative changes may be required. It is envisaged that this framework will form part of the Forum's transaction data analytics solution (see box above).

The Joint Fraud Taskforce will take a phased approach to introduce the scheme. It could take between 24 and 36 months to fully implement the scheme, but this depends on delivery of the transaction data analytics solution and legislative requirements.

Monitoring the progress of industry initiatives

4.10 Each of these measures will help better protect consumers against APP scams – so it is important that they are delivered as soon as possible. Industry has committed to delivering these measures and has made significant progress on them to date. We want to make sure that they continue to do so, specifically those measures overseen by UK Finance and those that the NPSO will take over from the Forum.

4.11 We therefore set out the milestones that we expect industry to meet for each initiative of UK Finance and the NPSO. UK Finance and the NPSO's Chief Executive Officer have agreed to monitor these and report to us on a six-monthly basis on the progress of their initiatives. They will provide their first report in June 2018. If progress slows or is not sufficient to achieve the outcomes we expect, then we will consider appropriate regulatory action.

4.12 Table 2 sets out the initiatives that UK Finance will monitor and our expected milestones.

Table 2: UK Finance's initiatives and expected milestones

Initiatives	Milestones
Customer education and awareness	We expect to see a rise in consumer awareness of fraud by the end of 2018. Evidence of this should be provided in the progress reports.
APP scam statistics	We expect UK Finance to continue publishing these statistics on a six-monthly basis. This includes collecting and publishing the more detailed statistics – such as the type of scam (the categories within maliciously misdirected and malicious payee) – as soon as possible. We also expect UK Finance to analyse the statistics to monitor trends in APP scams and the effectiveness of the fraud prevention measures being put in place.
Financial crime data and information sharing	We expect detailed planning to be completed quickly, and a high-level plan to be delivered by mid-2018. We expect that practical actions – those not dependent on legislative changes – will be completed quickly.
Best practice standards (APP claim reporting standards)	We expect that the PSPs that are retail bank members of UK Finance that provide push payment services will fully implement these standards by Q3 2018. We expect that all PSPs that offer push payment services to consumers will fully implement these standards by the end of 2018.
Information sharing in response to APP scams	We expect the outcomes of this work that have been incorporated into the best practice standards will be implemented with those standards by Q3 2018. We will monitor and support, where appropriate, any legislative changes or developments required to address any legal barriers identified in the follow-up work.
Guidelines for identity verification, authentication and risk assessment	We expect that a significant proportion of UK Finance members that provide push payment services to consumers (at least 75% of market share) will have implemented the guidelines by mid-2019. By mid-2020, all PSPs that provide push payment services should follow the guidelines.
Trusted KYC data sharing	We expect the standards and rules are published in the second half of 2018. We expect that KYC value-added solutions are in place by the end of 2020.

4.13 Table 3 set outs the initiatives that the NPSO will monitor and our expected milestones.

Table 3: NPSO's initiatives and expected milestones

Initiatives	Milestones
Confirmation of Payee	We expect the rules and requirements to be in place by 2018 allowing PSP to offer Confirmation of Payee solutions from then. We expect any necessary infrastructure and solutions to be in place so solutions are available when the NPA is implemented in 2021.
Transaction data analytics	We expect the rules and standards to be in place by 2018 allowing transaction data analytic solutions to be offered from then. We expect competing transaction data analytic solutions are available when the NPA is implemented in 2021.

The FCA's regulatory developments

4.14 As part of our response to the Which? super-complaint, the FCA committed to undertake work to identify if there were any firm-specific or sector-wide shortcomings in the way PSPs handle APP scams. In particular, the FCA undertook to:

- work with PSPs to tackle concerns around both sending and receiving PSPs in relation to APP scams
- examine the evidence received in relation to the super-complaint and address any firm-specific issues directly

4.15 Over the past year, the FCA has proactively engaged with a number of PSPs (specifically, the major retail banks) to understand their policies and procedures for handling APP scams – both as sending and receiving PSPs. This also included a review of the measures they have in development to improve their ability to prevent APP scams.

4.16 The FCA has found the following:

- While PSPs provide staff training and have procedures in place for dealing with victims of APP scams, the underlying procedures for handling cases of APP scams are often unclear and inconsistently applied. In practice this can lead to poor communication with customers, delays in PSPs taking action once a scam has been reported, and inconsistent approaches to customer vulnerability.
- APP scams seek to circumvent PSPs' existing financial crime systems and controls, including those to detect fraud and to identify and monitor customers for anti-money laundering (AML) purposes. PSPs are working to improve their capabilities to detect instances of APP scams and identify potential money mule accounts; some PSPs have made more progress on this than others.
- Insufficient data has been collected by PSPs in order to understand the scale of APP scams. If further information was collected by PSPs, it could help to better identify money mules, for example.

4.17 The FCA found that PSPs are actively engaged on the issue of APP scams, and most are taking forward their own initiatives to improve their capabilities to prevent and respond to APP scams.

4.18 The FCA is supportive of the industry-led initiatives set out in this chapter, as well as introducing a contingent reimbursement model that we discuss in Chapter 6. It considers these initiatives to be a natural starting point to tackle the issues it identified and should significantly reduce consumer harm arising from APP scams.

4.19 The FCA welcomes the introduction of UK Finance's best practice standards for responding to APP scam claims – the APP claim reporting standards (as set out in Chapter 3) which is a key initiative in tackling APP fraud. The FCA will also be writing to members of UK Finance to ask them to consider the following[18]:

- Whether the SMF Manager with responsibility for the firm's policies and procedures for countering the risk that the firm might be used to further financial crime is ensuring that adequate measures are being taken to address payment services fraud (including APP scams).
- If they have committed to adopt the best practice standards, how they will incorporate them into their policies, procedures and target operating model.

4.20 Successful adoption of UK Finance's best practice standards by the industry should prevent the need for the FCA to take a more interventionist approach to tackling APP scams. The FCA will continue to consider the impact of UK Finance's standards and other industry initiatives in this area. It will seek to take further action if it deems that these are not delivering the expected benefits for consumers in preventing and responding to scams.

18 www.fca.org.uk/news/statements/fca-response-psr-paper-authorised-push-payment-scams

5 The role of payment system operators

Key points

- During our work on the role of the payment system operators, a stakeholder suggested a concept for reimbursing victims of APP scams – we are keen for this option to be progressed further (see Chapter 6).
- A study of the fraud handling in push payment systems outside the UK shows that only two countries (Japan and South Korea) have specific APP scam detection procedures; in all the markets we studied the legal financial liability for APP scams falls on the payer.
- The industry initiatives underway in the UK should have significant benefits to preventing and responding to APP scams, and will bring practices into line with those used in other UK and international payment systems and other sectors.

5.1 In our response to the Which? super-complaint, we committed to considering the potential for the operators of CHAPS and FPS to play an expanded role in helping to minimise the consumer harm caused by APP scams.

5.2 In the terms of reference for this work[19], we set out that we would focus on the following questions:

- How do UK practices towards APP scams compare with those in other countries?
- How do practices towards APP scams compare with practices for other UK disputed payments?
- What can be learned from non-payment networks?
- What are the economic incentives for preventing and responding to APP scams?

5.3 To investigate these questions we:

- commissioned a study of fraud practices in comparable international push payment systems
- issued and received responses to information requests from the operators of both FPS and CHAPS
- issued and received responses to a 'call for input' from PSPs and other interested industry stakeholders
- held a range of meetings with various parties including card payment system operators, other payment industry stakeholders, and regulators of other network industries

5.4 In this chapter, we present the key findings from our work on each of these questions.

5.5 Before doing so, however, we highlight in particular one of the call for input responses we received as part of this work – from FFA UK, which has since been integrated in the new financial services trade body, UK Finance. We refer to the latter in the rest of this chapter.

19 PSR (2017) *Authorised push payment scams: the role of payment system operators – final Terms of Reference:* www.psr.org.uk/psr-publications/policy-statements/authorised-push-payment-scams-role-of-operators-final-terms-reference

5.6 As part of its response, FFA UK set out its view that there was potential for operators of UK push payment systems to act as administrators of a new 'funds repatriation scheme' that would 'establish a common approach and standards for processing, investigating and where applicable returning the proceeds of confirmed fraud/APP scams to victims.' The proposed scheme introduced the concept of an 'equitable liability model', whereby PSPs would be responsible for reimbursing victims of APP scams in instances where it was not possible to trace and recover the underlying funds and the PSP had failed to meet the relevant standards set out in the scheme.

5.7 We refer to this model as a 'contingent reimbursement model' to avoid potential confusion with potential shifts in the underlying legal liability for fraud related to authorised payments.

5.8 In our view the introduction of such a model has strong merit. In particular:

- Currently, APP scam victims could bear all the loss in any circumstance if their PSP cannot recover their money, or decides not to reimburse them. Making reimbursement contingent on agreed standards should increase PSPs' incentives (particularly where they are the receiving PSP) to adequately invest in and maintain practices that help prevent and respond to APP scams. This should reduce the number of APP scams. The model should not reduce the care consumers take when making payments because they would need to meet a requisite level of care to be eligible for reimbursement (we discuss this in Chapter 6).
- It should reduce consumer harm by reimbursing victims when they could not have reasonably prevented an APP scam but their PSP, or the PSP used by the fraudster, has not met the required standards. We found similar models in other UK payment systems and the rail sector.
- It should support the other measures that the industry is developing to help prevent and respond to APP scams (these are set out in Chapter 4). Including these measures as part of the standards of the model should give PSPs an incentive to implement and use those measures. However, the contingent reimbursement model would not be a substitute for these developments.

5.9 As a result, we have decided to support the further exploration, development and implementation of this kind of model. Our first step is to consult on its potential merit, scope and characteristics. Our consultation, and wider discussion of the model, is set out in the next chapter.

5.10 FFA UK's proposed concept of a similar model suggested that payment system operators may be best placed to administer the model. However, we think operators may not necessarily be the most appropriate entity to do so. As set out in the next chapter, we think that there is merit in exploring whether the model could be operated by other parties, such as industry trade bodies, with us actively monitoring their work on this.

5.11 Regarding the other industry initiatives outlined in Chapter 4, we do not consider the operators of CHAPS and FPS need to play an expanded role at this time beyond those initiatives that the new payment system operator will take over – that is, overseeing the rules and requirements for Confirmation of Payee and transaction data analytics.

5.12 In our terms of reference we also said that, if appropriate, we would consider the actions we could take to expand the role of operators in APP scams. Given our decision to explore and support the proposal to develop a contingent reimbursement scheme (see Chapter 6), we have not sought to respond to this question in any detail at this time.

Fraud practices in international push payment systems

5.13 We commissioned specialist payment consultants to study the fraud practices used in push payment systems comparable to CHAPS and FPS in 12 international jurisdictions.[20] The study considered the fraud practices used in these markets that could help prevent or respond to APP scams, the role of payment system operators in these practices, and the relevant wider legislative and regulatory frameworks in these markets.

5.14 The summary findings of this work are published separately alongside this report.[21] The key findings are set out in the remainder of this section.

5.15 Overall, the study found that in most of the markets analysed, fraud practices in the relevant payment systems – and associated legislative and regulatory frameworks – do not focus on APP scams specifically. They focus on fraud more generally or specifically on unauthorised fraud. The exceptions are Japan and South Korea; they have implemented fraud practices and legislation to address APP scams as the problem is more common in these markets.

5.16 In the following sections we consider both the key fraud **prevention** and **resolution** processes that the study identified.

Fraud prevention processes

5.17 The majority of fraud prevention processes found in international markets are similar in principle to those being developed in the UK: specifically, the Confirmation of Payee and transaction data analytics technical solutions, and information sharing processes (see Chapter 4). These were implemented to address fraud more generally or to improve the customer experience, but can also help to address APP scams. Many of the markets use beneficiary account name verification services (which are similar to the Confirmation of Payee solution being developed in the UK). Around half of the markets have network-level transaction analytics for monitoring and scoring transactions from sending accounts and into receiving accounts. A few markets have established information sharing services to collect, disseminate and, in some instances, analyse fraud-related data for the community.

5.18 South Korea and Japan have specific APP scam prevention processes in place. South Korea uses a withdrawal delay system. This prevents the cash withdrawal of a transfer of funds for up to 30 minutes if the transfer value exceeds 3 million Korean won (~£2,000). In Japan, people are not able to make ATM-initiated credit transfers above 100,000 Japanese yen (~£700). These measures address the main characteristics of the scams used in those markets, and there is some evidence they have been effective in reducing consumer harm from APP scams.

5.19 The operators' role in these processes varies, while other stakeholders – regulators and PSPs – tend to play a significant role. In general, the centralised solutions and processes exist to extend and augment the PSPs' own fraud processes or consumer service offerings. The operators tend to play a role in processes that are centralised or are incorporated into the central payments infrastructure (for example, network-level transaction analytics and beneficiary verification solutions). In one market, the use of beneficiary account verification is mandated in the payment system rules but can be procured from a group of preferred suppliers. In another market, the centralised information sharing service is provided by an organisation separate to the operator.

20 The countries in the study are Australia, Denmark, India, Japan, Nigeria, the Netherlands, the Single Euro Payments Area (SEPA), Singapore, South Africa, South Korea, Sweden, and the United States.

21 Lipis Advisors (2017) *Fraud prevention and resolution in push payment systems: Comparative analysis:* www.psr.org.uk/psr-publications/consultations/Lipis-report-on-international-fraud-practices

5.20 There is a mix of mandatory and voluntary use of these processes. Beneficiary account name verification services are generally offered as value-added services. In Japan, South Korea and some less developed countries, regulators have mandated APP scam-specific processes and network-level transaction analytic solutions. In more developed markets, the transaction analytic solutions are generally offered as value-added services.

5.21 In all the markets considered, the consumer fraud prevention processes are used in retail push payment systems comparable to FPS. They are not used in high-value (wholesale) systems. This reflects the limited scope for consumers to initiate payments in these systems.

Fraud resolution processes

5.22 In all of the markets in the study, the legal financial liability of APP scams falls on the payer, similar to the legislation in the UK. No evidence was identified to suggest that these countries have considered whether the allocation of financial liability of APP scams should be changed.

5.23 Japan and South Korea have implemented specific legislation regarding APP scam resolution. They set out the framework for when PSPs can freeze a scammer's account and for redistributing the funds to victims. The operators do not have a role in these resolution processes. The authorities in each market said that these resolution frameworks have been effective tools in reducing consumer harm from APP scams.

Practices for disputed payments in UK payment systems

5.24 We considered what practices UK payment system operators follow for fraud and other types of disputed payments. Specifically, we considered practices in the four-party card payment systems (focusing on Mastercard and Visa), Bacs, the new Cheque Imaging Clearing System (ICS), proprietary payment systems and payment overlay services. We also considered FPS' and CHAPS' current practices for other types of disputed payments.

5.25 Our detailed analysis is presented in Annex 2. Our key findings in this area are set out in the remainder of this section.

5.26 The system rules set out liability models for disputed payments in payment systems that provide pull payments – card systems (Mastercard and Visa), Bacs and ICS. These are used for disputes over fraudulent payments and, in card payment systems, other commercial disputes.

5.27 In card payment systems, liability (and therefore the party which bears the loss) depends on whether the parties involved have met certain responsibilities or acted appropriately. The responsibilities are linked to practices that help prevent the fraud from happening. Liability can apply to all parties involved under different circumstances – PSPs, the merchant and the consumer – who are all expected to have taken a certain amount of care over the payment.[22] Where the victim has acted appropriately, they are reimbursed.

5.28 Card payment systems and the ICS have dispute resolution mechanisms in place. For cards, it is the operator that acts as an arbitrator and for ICS it is an independent third party.

22 The card systems' scheme rules place liability on the issuers and acquirers that, in turn, can place responsibility on the cardholder or merchant through their respective commercial relationships.

5.29 In payment systems where liability models are used, we recognise there are some distinct differences compared to the way APP scams occur. These are:

- Fraud prevention and resolution is generally focused on unauthorised fraud, whereas APP scams relate to payments that are explicitly authorised by the consumer.
- The payments are person-to-merchant/corporate. This is a more limited network of participants compared with push payments (which include person-to-person payments), and so it may be easier to monitor fraudulent payees (the businesses). An exception is the ICS liability model, which also covers person to person payments.
- Pull payments generally take a longer time to settle (and for the scammer to move the funds) than real-time push payments.

5.30 While there are differences, we note that these liability models give consumers confidence and trust in those payment services, by reimbursing them when they fall victim to a fraud that they could not reasonably prevent. Furthermore, these models can be used to incentivise all the parties involved to take actions to prevent the fraud from occurring in the first place, where they are best placed to do so, or risk bearing the loss. We consider it is important that consumers have trust in all UK payment systems and services, and as outlined in Annex 4, it is important to ensure PSPs have the appropriate incentives to address APP scams. We consider how similar practices – reimbursement and incentivising participants – could be used to address APP scams in Chapter 6.

5.31 In the responses to our call for input there was very limited support from PSPs for a full chargeback-like process (similar to that used in card systems) for push payments. Most PSPs that responded said the operators could play a greater role in reducing harm from APP scams, but there were varying views on what this should be. Several respondents supported the Forum's initiatives for Confirmation of Payee and transaction data analytics. Many PSPs said legal issues with data sharing could limit the operators' role; in contrast, one PSP [✂] said PSPs could submit additional information in their fraud reporting (for example, recipient details) and that the operators could require this as part of the system rules.

5.32 The use of penalties is another measure that can be used to incentivise participants, specifically PSPs, to use practices for preventing fraud. This concept is used in the card systems. Penalties can include fees or audits. A comparable practice for APP scams could be to penalise PSPs that are the beneficiary PSP for a high proportion of APP scams. These PSPs could be required to improve their monitoring and detection capabilities and/or face a financial penalty. To implement this process, the standards would need to be determined and a body established to monitor and enforce compliance.

5.33 We also find there are certain practices used for fraud and other disputed payments – such as misdirected payments – in UK payment systems that are similar, in principle, to those measures being developed by industry that will help prevent or respond to APP scams.

- **Transaction data analytics at the network level:** While these are used in the card systems for generally detecting and preventing unauthorised fraud, the Forum is developing standards for data analytics solutions that could identify money mule accounts used by scammers.
- **Payee verification in Paym:** This is used to verify the payee before making a payment. The Forum is currently developing rules for Confirmation of Payee solutions that can be used for other push payments.
- **The credit payment recovery principles in place for FPS, Bacs and CHAPS:** These set out clearly how PSPs should interact when responding to an accidentally misdirected payment. With our oversight, UK Finance has developed best practice standards for how PSPs respond to APP scam claims.

Practices in non-payment network industries

5.34 We also considered the practices used in other network industries that face challenges comparable to APP scams – where the actions of one network participant can impose costs on other participants in the industry. These included challenges in telecommunications (misuse of premium rate services and Calling Line Identification spoofing), rail (delays affecting other train companies) and electricity supply (electricity theft).

5.35 Our detailed analysis in this area is presented in Annex 3. The key findings in this area are set out in the remainder of this section.

5.36 The industries we identified have taken approaches to these problems that are similar in principle to measures that have already been implemented in the payments industry. These are broadly comparable to:

- PSPs having the ability to analyse data to monitor and possibly detect transactions for their own customers that may be linked to fraud
- a trade body which focuses on addressing the issue; for APP scams this is UK Finance
- regulating access to the payments network – PSPs are required to undertake KYC checks for customers

5.37 Other approaches used in these industries are similar in principle to measures that the payments industry is now implementing. These are:

- transaction data analytics, which will use centralised data analysis to provide insights not available to individual PSPs
- Confirmation of Payee, which can help customers check they are sending money to the account they intend to

5.38 However, there are some notable processes used in the rail industry that are not used in payments for addressing APP scams. The rail industry has formal arrangements in place for compensation payments between train operating companies and Network Rail, and to compensate passengers when trains are delayed or cancelled. These schemes are designed to give train companies an incentive to act in the best interest of all passengers, and to compensate passengers for the harm they may have suffered. There is a process in place for resolving disputes between train companies, which is run by an independent third party.

5.39 There are different organisations in each industry overseeing the approaches used to address the challenges. Some approaches have been led by central operators. However, for other approaches it is the network participants, trade bodies and regulators that play the most important role. The role of the central operator tends to reflect its ability to view the whole network, but there are other examples where this can be done by another organisation.

Economic incentives for preventing and responding to APP scams

5.40 We considered the economic incentives for different parties to prevent and respond to APP scams. Our detailed analysis in this area is presented in Annex 4. The key findings in this area are set out in the remainder of this section.

5.41 When considering APP scams individually, consumers, followed by their PSPs, have the strongest incentives to limit harm from APP scams. Incentives are weaker for receiving PSPs and the payment system operators.

5.42 No single party involved in the scam payment chain has complete visibility over the whole chain and the other parties involved. For example, a victim's PSP has a commercial relationship with the victim of an APP scam, and can see which PSP received the payments. They do not, however, have any visibility of the payee at that scammer PSP. The operator has visibility of the sending and receiving PSPs for payments relating to APP scams (and some details of the accounts involved at those PSPs). However, they have no information on the payer (the victim) or payee (the scammer).

5.43 Equally, no one party is able to exert influence, or to coordinate activity, over the whole chain. Moreover, the influence that each party in the scam chain is able to exert in relation to scam prevention and response could, in general, complement (rather than substitute) that of other parties in the chain.

5.44 Distinguishing between sending and receiving PSPs is relevant for individual APP scams. When considering APP scams in aggregate, however, many PSPs (especially larger PSPs) will be in the position of having been used by both victims and scammers. As a result, when considered in aggregate there may be stronger incentives on PSPs to prevent and respond to APP scams. This will likely hold only if individual PSPs expect their efforts to be reciprocated by other PSPs. Given the potential for free-riding on investments of other parties in scam prevention and response, this may not occur without outside intervention.

Key insights

5.45 The key insights that we take from this work are:

- The industry initiatives underway in the UK should have a significant impact in preventing and responding to APP scams, and will bring practices into line with those used in other UK and international payment systems and other sectors. It is important the industry has good incentives to deliver and adhere to these initiatives.
- Industry has proposed a model that would see PSPs provide contingent reimbursement to victims of APP scams. We see merit in this proposal, and are consulting on introducing such a model. There is no clear evidence at this stage that the payment system operators **need** to play an expanded role in introducing a voluntary contingent reimbursement model. We explore this further in our consultation.

6 Consultation on the development of a contingent reimbursement model

Key points

- We consider there is merit in an industry-led contingent reimbursement model. We are consulting on this and want feedback on how it should be further developed, implemented and administered.
- An effective model would give both PSPs and consumers the incentive to help prevent APP scams, and to respond to them effectively when they occur. The right solution would be pragmatic and fair – consumers would still need to be vigilant and sensible, but if PSPs could have done more, then they would reimburse victims.
- If a contingent reimbursement model is introduced, its first iteration should be implemented by the end of September 2018.

6.1 One initiative that could help APP scam prevention and response is a contingent reimbursement model. This is a process that sets out the circumstances when the victims of APP scams would get their money back and whether it would come from either their PSP (the sending PSP) or the PSP that received the money on behalf of a fraudster (the receiving PSP). Reimbursement would be contingent on whether these PSPs had met the required standards, and whether the victim had taken a requisite level of care. The standards that PSPs need to meet would include processes – such as use of technology, rules and procedures – that help prevent and respond to APP scams.

6.2 In this chapter we consider voluntary contingent reimbursement as an additional measure for tackling APP scams. It is set out as follows:

- Introducing a contingent reimbursement model
- Designing and implementing the model, including our role in this
- Potential barriers to implementation
- Other details to consider

6.3 We want your feedback on our current view that a voluntary contingent reimbursement model should be introduced, and how it should be implemented and administered. We will take this feedback into account in reaching our final view on this.

Introducing a contingent reimbursement model

6.4 As part of our combined work on APP scams, FFA UK (which has been integrated into UK Finance) outlined a proposal for a 'funds repatriation scheme' that introduced the concept of a model that has characteristics of contingent reimbursement (see from paragraph 6.17 and Chapter 5 for more details).

6.5 A contingent reimbursement model would complement existing informal arrangements where PSPs voluntarily compensate some victims of APP scams. PSPs that adopted the model would agree to reimburse victims under specified circumstances.

6.6 We consider that, for a number of reasons, there is merit in introducing a voluntary contingent reimbursement model:

- Currently, APP scam victims could bear all the loss in any circumstance if their PSP cannot recover their money, or decides not to reimburse them. Making reimbursement contingent on agreed standards should increase PSPs incentives (particularly where they are the receiving PSP) to adequately invest in and maintain practices that help prevent and respond to APP scams. This should reduce the number of APP scams. The model should not reduce the care consumers take when making payments because they would need to meet a requisite level of care to be eligible for reimbursement.
- It should reduce consumer harm by reimbursing victims when they could not reasonably have prevented an APP scam but their PSP, or the PSP used by the fraudster, has not met the required standards. We found similar models in the other UK payment systems and the rail sector.
- It should support the other measures that the industry is developing to help prevent and respond to APP scams. Including these measures as part of the standards of the model would give PSPs an incentive to implement and use those measures. However, the contingent reimbursement model would not be a substitute for these developments.

6.7 In this section, we set out our high-level principles for a voluntary contingent reimbursement model. We also set out FFA UK's concept. We then set out some variations for a reimbursement model and explain why these are inappropriate. Finally, we discuss the potential costs of introducing a contingent reimbursement model. We welcome stakeholders' views on all of these issues.

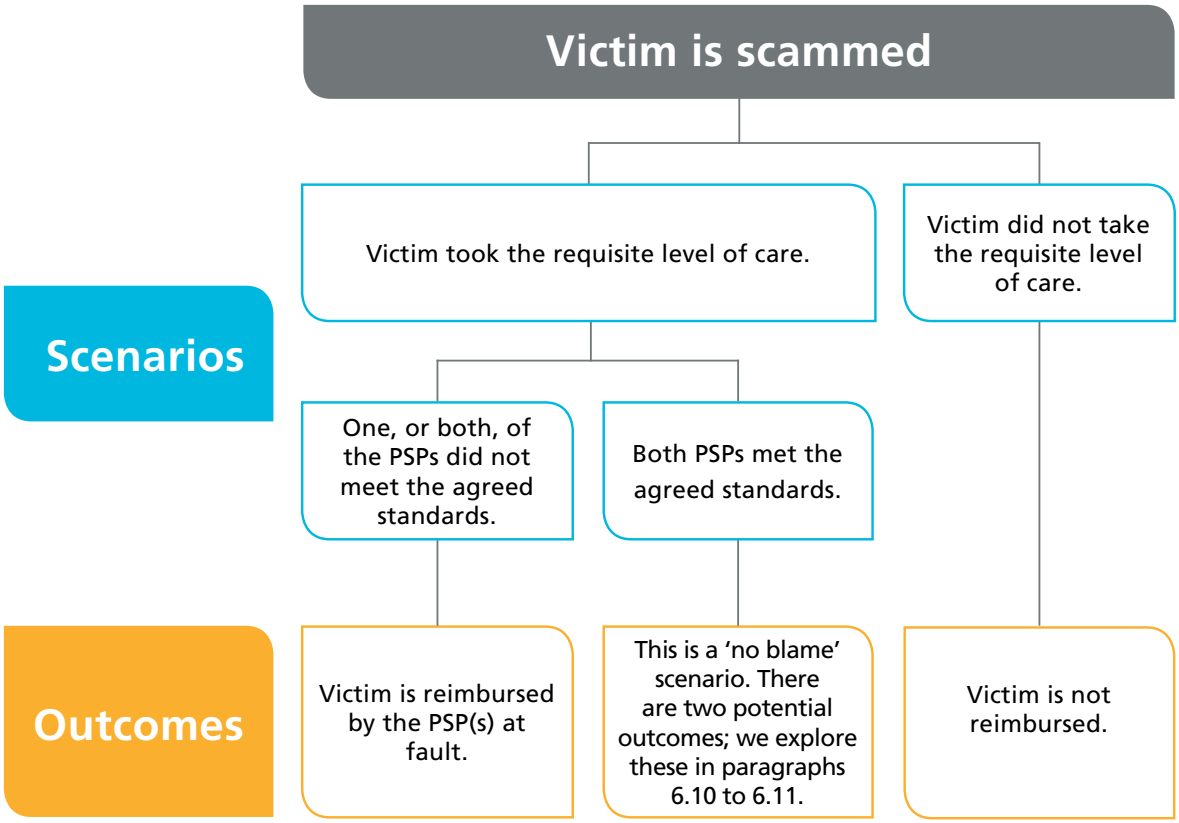
Our high-level principles of a contingent reimbursement model

6.8 An effective reimbursement model would give all parties involved – PSPs and consumers – the incentive to help prevent APP scams, or to respond to one if it occurs, where they are best placed to do so:

- Consumers must have an incentive to take whatever steps they reasonably can to avoid becoming a victim of an APP scam. This can be achieved by defining the requisite level of care victims are expected to meet to be eligible for any reimbursement (we discuss defining the level of care in paragraph 6.36).
- PSPs must have an incentive to implement and adhere to agreed standards that help protect consumers from APP scams – for example, stopping misdirected payments and better identifying mule accounts used by scammers. This can be achieved when PSPs are expected to meet agreed standards or risk needing to reimburse the victim (where the victim is eligible).

6.9 Figure 3 shows the potential scenarios and outcomes of an effective contingent reimbursement model.

Figure 3: Potential APP scams scenarios and outcomes



6.10 In a 'no blame' scenario, the victim and the sending and receiving PSPs have all acted appropriately and met the required standards, but a scam still occurs. There are two potential outcomes for this scenario:

- **Focus on consumer protection:** In this outcome, the victim is reimbursed, either by the PSPs directly involved, or from a central fund to which all PSPs contribute. Here, the consumer is always protected as long as they have taken an appropriate level of care. However, this outcome could weaken PSPs' incentives to prevent and respond to APP scams because they would have to contribute to a central fund or bear the cost of reimbursement even in instances where they have met the required standards. This could mean that it is not as effective for preventing APP scams as it could be.
- **Focus on incentives:** In this outcome, the victim is not reimbursed and bears the loss. The PSPs do not pay anything because they met the required standards. This outcome ensures strong incentives for all to act appropriately. However, it means there will be instances where two consumers behave in the same way, but one is reimbursed (because the PSP(s) failed to meet the standards) and the other is not (because the PSPs did meet the standards).

6.11 We would like feedback on the relative advantages and disadvantage of each option, and which outcome is most appropriate in a 'no blame' scenario.

6.12 Regardless of whether the victim has taken the requisite level of care, in any scenario where a PSP has not met their required standards, it might be appropriate that the model includes some form of fine or penalty on the PSP to ensure it is appropriately incentivised. The funds could potentially be put into a central fund for reimbursing victims such as in the 'no blame' scenario.

6.13 We consider that, in any scenario where the victim is eligible for reimbursement, the reimbursement should not depend on their money being recovered. This is because it will not always be possible to recover the money.

6.14 The contingent reimbursement model should not prevent PSPs choosing to give 'goodwill' payments to victims – for example, where the victim did not take the requisite level of care set out in the model but where a PSP considered other mitigating factors were relevant. Some sending PSPs already offer varying degrees of goodwill payment.[23] An example of this is where a PSP did not meet its own internal guidelines so it reimburses the victim, even though it is not required to. A contingent reimbursement model should set out more clearly the circumstances when a victim should be reimbursed and which party should do it. However, either PSP should be able to reimburse the victim if it chooses to – for example, to improve its reputation or demonstrate good customer service.

6.15 It is important that the standards of the model – those that PSPs must meet – ensure that PSPs use effective processes that help protect consumers against APP scams. We therefore believe that the measures being developed by industry (specifically UK Finance and the Forum) that we identified in Chapter 4 – such as consumer awareness campaigns, Confirmation of Payee, transaction data analysis, and the best practice standards for dealing with APP scam claims – should be included as required standards in the model. These measures should significantly improve prevention and response to APP scams. Incorporating these measures as the required standards to meet will increase the incentives of PSPs to implement and use these measures, which would help reduce the harm caused by APP scams. The model could also incorporate other measures developed specifically for the purpose. We propose to monitor the design of the model, including the required standards that are used (see paragraph 6.30).

6.16 In addition, the model should take into account regulatory developments, such as the new categories of industry players entering the market following the introduction of the second EU Payment Services Directive (PSD2). Specifically, payment initiation service providers (PISPs) as a type of third party provider (TPP). The model should also consider how it will interact with reimbursement for other types of fraud and misdirected payments.

FFA UK's proposal

6.17 FFA UK proposed a 'funds repatriation scheme' that incorporates a concept for a framework with similar characteristics of a voluntary contingent reimbursement model, which it suggests could be administered by the payment system operators (see paragraphs 5.5 to 5.6).

6.18 FFA UK's concept sets out early views on potential scenarios and outcomes for reimbursement, which would be dependent on whether the victim had acted appropriately, and whether the PSPs involved had adhered to certain standards – for example, the best practice standards for responding to APP scams. [✂]

23 *Which? authorised push payments super-complaint – PSR Response* (Dec 2016), paragraphs 5.23 to 5.25: www.psr.org.uk/sites/default/files/media/PDF/PSR-Which-super-complaint-response-December-2016_0.pdf

Other reimbursement models

6.19 We considered two alternative reimbursement models, which we believe are inappropriate.

6.20 The first model always puts responsibility for reimbursement (where the victim is eligible) entirely on either the victim's PSP or the receiving PSP. We consider this is inappropriate because both the victim and receiving PSPs have a role to play in APP scam prevention and response. The PSP that does not have any responsibility for reimbursement would have much weaker incentives to help prevent and respond to APP scams (a 'free rider' problem – see paragraphs 5.40 to 5.44). For this reason, we consider the responsibility for reimbursement should be contingent on the actions of both the sending and receiving PSPs.

6.21 The second model guarantees that victims are reimbursed in any circumstance, even if they have not taken reasonable care to avoid the scam. In our response to the Which? super-complaint we explained why we consider this would be inappropriate:[24]

- If consumers knew there was no risk to themselves, they could change their behaviour in ways that would make APP scams more common. According to the Commissioner of the Metropolitan Police Service in 2016, consumers could become less vigilant in identifying and preventing APP scams.[25]
- There is also scope for an increase in 'first-party fraud', where consumers falsely claim they were victims of APP scams in order to claim reimbursement from their PSP.
- Knowing that PSPs would reimburse victims of APP scams could also embolden existing scammers and prompt more criminals to start operating scams.

The cost of adopting a contingent reimbursement model

6.22 We believe an effective contingent reimbursement model, together with the other measures discussed in Chapter 3, should reduce APP scams and benefit victims. However, it will also cost money to develop, operate, monitor and arbitrate – and the costs could ultimately be passed on to consumers. An effective contingent reimbursement model should help minimise the total system cost associated with APP scams, by reducing the number of APP scams occurring in a cost effective way.

6.23 Different variations of the model would have different cost implications, and different benefits, and these will need to be taken into account.

Question 2: Should a contingent reimbursement model be introduced? Please provide reasons.

Question 3: Do you agree with our high-level principles for a contingent reimbursement model? Please provide reasons.

Question 4: In your view, what are the relative advantages and disadvantages of each alternative outcome for a 'no blame' situation (the victim is reimbursed by PSPs, or the victim bears the loss)? Please provide reasons.

Question 5: Do you agree that the measures being developed by industry (specifically UK Finance and the Forum) should be included as the required standards of the contingent reimbursement model that PSPs should meet? Please explain your reasons.

24 *Which? authorised push payments super-complaint – PSR Response* (Dec 2016), paragraph 8.23.
25 The Guardian, *Met chief suggests banks should not refund online fraud victims* (24 March 2016):, www.theguardian.com/uk-news/2016/mar/24/dont-refund-online-victims-met-chief-tells-banks

Designing and implementing a contingent reimbursement model

6.24 If a voluntary contingent reimbursement model is introduced, an organisation would need to be responsible for ensuring that PSPs adopt the model, and that it is effective in reducing APP scams.

6.25 To be effective, we consider that a contingent reimbursement model would need to continually evolve to adapt to changes in the ways APP scams are run, as well as industry developments and approaches to preventing APP scams.

6.26 We believe that industry should lead the design and implementation of the model; industry has the appropriate expertise and capabilities to take this forward in the most efficient way (we set out our proposed role in the process in paragraph 6.30 onwards).

6.27 There are a number of industry organisations which could take responsibility for design and implementation:

- **UK Finance:** UK Finance is an industry body for businesses that provide financial services. Financial Fraud Action UK (FFA UK), which has recently been integrated into UK Finance, has significant expertise and knowledge of fraud prevention and response. It is responsible for leading on financial fraud initiatives, including most of those measures being developed that we think should help address APP scams (see Chapter 4). It has also proposed a voluntary framework for tackling APP scams which has similar characteristics and principles to the voluntary continent reimbursement model we think is appropriate (see paragraphs 6.17 and 6.18).
- **The New Payment System Operator (NPSO):** The NPSO will consolidate Bacs Payment Schemes Ltd, the Cheque and Credit Clearing Company and Faster Payment Scheme Ltd.[26] The NPSO will also introduce the New Payments Architecture (NPA).[27] Fraud prevention is not a core competency of the NPSO, or of the companies it will replace, and so it may not be well placed to design and implement processes which address APP scams. The NPSO will have a high workload in the medium term, and so may not have the capacity to develop a contingent reimbursement model. Whether or not the NPSO develops the model, it could implement it by including the model in its scheme rules that NPSO participants would need to follow. However, payments in APP scams can be made outside FPS (through CHAPS or as 'on-us' payments, where the consumer's and recipient's accounts are held at the same PSP). This would need to be considered if the model was implemented this way.
- **The Joint Fraud Taskforce:** The Joint Fraud Taskforce is a partnership between the Home Office and industry that was established to address fraud. The Taskforce has access to a wide range of fraud expertise, and includes UK Finance, Cifas and the Home Office among its members. As the members include government and industry bodies, there could be many ways the Taskforce could implement a model. Being led by the Home Office, the Taskforce works closely with government and so may be able identify and potentially address any legal barriers to implementing a contingent reimbursement model (we discuss these in paragraphs 6.33 to 6.34). However, for the same reason, the Taskforce's leadership could dampen industry's sense of ownership over the model. We consider that it would be beneficial for industry to lead this work (see paragraph 6.26).

26 www.psr.org.uk/psr-focus/payment-system-operator-delivery-group
27 implementation.paymentsforum.uk/working-groups/npa-design-hub

6.28 An alternative option could be for stakeholders to establish a new association to operate the model and manage its adoption by PSPs.

6.29 In our view, UK Finance (with FFA UK within it) is best placed to design and implement a contingent reimbursement model. UK Finance has access to the expertise to develop and operate a model. It would need to make sure its development process included any stakeholders who would need to participate in the model, or would be materially affected by it. We propose to actively monitor its work on this, which we set out in the next paragraph.

Question 6: If a contingent reimbursement model is introduced, which organisation should design and implement it? Please provide reasons.

The PSR's role

6.30 If a voluntary contingent reimbursement model is introduced by industry, we propose to work with the industry organisation to establish a working group for the design and implementation. This working group must have terms of reference and agreed delivery dates. We propose to take the role of 'active observer' on this working group. We have taken a similar role in our relationship with the Payments Strategy Forum, which has enabled us to be informed of developments and, where appropriate, steer its direction in the interests of service-users. We would monitor industry's progress in designing and implementing the model, with particular regard to:

- the high-level principles we would expect the model to meet, including which measures are included as standards in the model
- the speed of implementation
- whether the chosen implementation options are in the best interests of end users

6.31 If it is appropriate for industry to introduce a voluntary contingent reimbursement model, we would expect this model to be implemented by the end of September 2018 (see paragraphs 6.57 to 6.63).

A potential PSR model

6.32 We would consider using our statutory powers if the voluntary contingent reimbursement model is not delivered in a timely manner, subject to any constraints imposed by PSD2. One option may be for the PSR to mandate a model which would require PSPs to comply with prescribed processes – including technology, rules and procedures. If a PSP failed to meet these prescribed processes, it would be required to pay a penalty. The funds accumulated in this way could potentially be used as a central fund to pay victims of APP scams through a separate mechanism.

Barriers to implementation

6.33 To the extent that standards of a voluntary contingent reimbursement model are linked to other industry or regulatory developments, or regulatory changes, implementation could partly depend on the timing of these developments. Phasing the introduction of the model could help address these issues (see paragraphs 6.58 to 6.59).

6.34 In setting out its proposal, FFA UK said there are legal barriers to funds repatriation (where the proceeds of APP scams are given back to the victims) which need to be addressed before its funds repatriation scheme can be implemented. As noted in paragraph 6.13, we consider the reimbursement of victims does not need to be dependent on the repatriation of funds, and so we consider that these potential barriers should not prevent the adoption by industry of a contingent reimbursement model in some form.

Question 7: In your view, are there any barriers to the adoption of a contingent reimbursement model which we have not considered? Please provide reasons.

Other details to consider

6.35 In this section we outline some additional details of a contingent reimbursement model that need to be considered, if one is introduced. We welcome your feedback on these.

Victims' eligibility for reimbursement

6.36 A contingent reimbursement model would need to define the requisite level of care from consumers to determine when a victim would be eligible for reimbursement. The requisite level of care should be high enough that consumers have an incentive to be careful of scams, but should not be unreasonable for them to meet. We consider that it is important that the organisation designing the model balances these considerations when developing the definition. Clearly, where a customer fraudulently claims to have been a victim of an APP scam (and is therefore committing first-party fraud), the customer should be ineligible for reimbursement.

6.37 For example, the definition of eligibility could cover these factors:

- Whether the victim's PSP had warned the victim about the transaction, for example through a phone call.
- Whether Confirmation of Payee (once implemented) had informed the victim that the recipient of funds did not match the name the victim had entered. This development is discussed in Chapter 4.

6.38 Vulnerability may play a role in defining the requisite level of care from consumers, and so the level could vary. The model may therefore need to consider consumer vulnerability

Question 8: Please explain, if relevant, how your organisation currently decides whether to reimburse a victim of an APP scam. Does this include an assessment of vulnerability?

Question 9: Are there any factors that should be considered when defining the requisite level of care victims should meet?

The scope of a contingent reimbursement model

PSPs involved

6.39 We consider that, to be effective in reducing consumer harm, a contingent reimbursement model must capture a significant majority of, if not all, PSPs that provide push payment services for consumers. This will ensure more consumers are protected. Also, PSPs that did not adhere to the model would risk becoming a main target for APP scammers, and their consumers would not be protected. Because of this, it is possible that if PSPs did not adopt the model, it could affect their reputation with consumers. PSPs may therefore have an incentive to adopt the model.

6.40 We would expect the organisation that administers the contingent reimbursement model to set relevant rules for its establishment and operation of the model. We do not believe the membership of this organisation should limit non-member PSPs from adopting the model. To ensure this:

- a trade association, such as UK Finance, would have to consider how non-members might participate
- the NPSO would have to consider how to capture both direct and indirect participants

Question 10: Do you think it is necessary for a significant majority of, if not all, PSPs that provide push payment services to consumers to adopt the contingent reimbursement model for it to be effective? If yes, please explain if you think the model would need to be mandatory for PSPs

Personal and business victim accounts

6.41 A contingent reimbursement model should protect consumers who have been scammed. We would therefore expect it to apply to payments made from consumer accounts. In FFA UK's concept, the model could possibly cover payments made from consumer accounts as defined under PSD2, which includes small businesses. We do not see any issues with using the PSD2 definition, given that small businesses typically demonstrate similar behaviour to consumers.

Geographic scope

6.42 A contingent reimbursement model should cover APP scams made between UK payment accounts. We consider that including payments made to or from overseas accounts would add significant complexity to the model and would therefore not be appropriate to include at this stage. FFA UK's concept also proposed the model could possibly cover UK payment accounts.

Payment systems involved

6.43 APP scams which target consumer accounts are made over FPS or CHAPS, or as on-us payments where a payment system is not used (because the payer and payee use the same PSP). In our view, a contingent reimbursement model itself does not need to be linked to a payment system; instead it should set standards and processes which apply whenever an APP scam occurs. FFA UK's concept is not specific to any payment systems.

6.44 If the model is administered by the NPSO it would need to consider how victims would have recourse when an APP scam payment is made through CHAPS or as an on-us payment.

Scammers using multiple receiving accounts

6.45 Once an APP scam payment has reached the first account controlled by a scammer, the scammer often moves the money on to other accounts. These additional accounts may not be held at the same PSP as the first recipient account.

6.46 A contingent reimbursement model could cover these additional accounts and PSPs. However, this adds complexity for allocating responsibility. Assigning responsibility where there are an increasing number of accounts and PSPs becomes more difficult, and disputes between PSPs may become more complex.

6.47 FFA UK's concept suggested the model could possibly cover the first transaction only. For the above reason, we agree.

Timing of eligibility

6.48 We recognise that having a time limit for claiming reimbursement for an APP scam is likely to be appropriate. We see this for card payments, where there is a time limit for disputing a payment and seeking reimbursement through the chargeback process.

6.49 We do not expect a contingent reimbursement model to involve retroactive reimbursement (for scams that happened before the model was introduced). This is because we recognise that PSPs cannot retrospectively implement or adhere to the standards of the model. PSPs would continue to be able to offer goodwill payments in these circumstances.

Question 11: What are your views on the scope we have outlined for the model? Please describe any other factors you think we should consider.

Resolving disputes

6.50 Under a contingent reimbursement model there is the potential for parties to disagree about the outcome of a case. The model will need a dispute resolution mechanism to address these disagreements.

6.51 Dispute resolution is used in similar models used elsewhere, such as the chargeback process for cards, the new Cheque Imaging Clearing System and payment between train companies in the rail sector (see Chapter 5). [✂].

6.52 The design of the dispute resolution mechanism will need to consider how it would relate to consumers' rights to appeal to the Financial Ombudsman Service (FOS) – the public body that handles complaints between consumers and PSPs, including APP scams disputes.

6.53 The effectiveness of the dispute resolution mechanism would have an impact on the effectiveness of the contingent reimbursement model. Therefore, dispute resolution must provide consistent, timely, and accurate responses.

6.54 In the chargeback process, the organisation which manages disputes is the same as the organisation which manages the rules that set out the liability model. This can allow for efficient interaction between the rules and disputes, such as updating the rules to reflect developments and outcomes of disputes. There is a risk of disconnect between the rules and dispute resolution if these roles are performed by separate organisations. However, separating these roles may be appropriate as some organisations are well placed to manage the rules but not disputes. Similarly, some organisations may be well placed to manage disputes but not rules – in some of the examples of liability models we considered, an independent third-party is responsible for resolving disputes.

6.55 A number of bodies could potentially oversee the dispute resolution:

- **UK Finance:** UK Finance does not currently resolve disputes and would need to acquire the relevant resources to do so. UK Finance could draw on its experience and knowledge of fraud when arbitrating disputes.
- **The NPSO:** Dispute resolution will not be one of the NPSO's core competencies. Unlike card systems, interbank payment systems do not play a key role in resolving disputes between members about specific payments. The businesses which will be consolidated into the NPSO do have some experience in addressing fraud; in particular, the system rules for cheques set out which PSP is responsible for cheque fraud under different circumstances. The NPSO has a high workload in the medium term, so it may not be practical for it to arbitrate disputes as well.
- **Independent third-party arbitrator:** In this model both parties appoint a single arbitrator of their choice and inform the operator (or another third party) of the outcome. There is no fixed arbitrator. This would enable parties to choose an organisation with appropriate experience in resolving disputes, that understands financial crime and has the capacity to resolve the dispute. This process, however, could lead to lack of standardisation in dispute resolution outcomes. It could also cost more than the other options.

6.56 We currently have no preference for which entity operates the dispute resolution process.

Question 12: In your view, how should the dispute resolution mechanism work and which organisation should oversee this? Please provide reasons.

Approach and timeframe for implementing a contingent reimbursement model

6.57 If a contingent reimbursement model is introduced, it is important that it is done in a timely manner. This will minimise the harm caused by APP scams as soon as possible. We recognise that developing and implementing the model would take time. The industry would need to agree and implement changes to business practices. In particular, it would need to agree a definition of the level of care consumers should take, and the arbitration process it would follow.

6.58 Implementation could also depend on the timing of the industry measures and developments that might be incorporated into the model as the standards that PSPs need to meet. Some of the measures for preventing and responding to APP scams that could be used as standards will be developed and implemented earlier than others (such as those depending on legislation changes). We note that many of the standards and initiatives should be in place by the second half of 2018 – for example, UK Finance's best practice standards for responding to APP claims will be implemented by its members by the end of September 2018.

6.59 It is therefore possible to use a phased approach for implementing the model. The model could incorporate those standards that are developed first, then as each additional standard is developed, or as appropriate changes to legislation occur, these could be incorporated into the model.

6.60 Alternatively, a transitional approach could be used if it might take time to agree the standards PSPs should meet. In this approach, reimbursement would not initially be linked to the PSPs' standards. Instead, if a victim had met a requisite level of care and should be reimbursed, both PSPs involved would share the responsibility for reimbursing the victim, regardless of how they acted. As the standards of the contingent reimbursement model are developed, responsibility for reimbursement by PSPs could be specifically linked to these standards. Over time, it would transition from the more general initial approach to a contingent reimbursement model.

6.61 We note that, regardless of which implementation approach is used, we believe that it is not necessary to wait until all standards and new initiatives are in place for the model (and victim reimbursement) to commence.

6.62 Taking these considerations into account, we propose that, if a contingent reimbursement model is introduced, its first iteration should be implemented by the end of September 2018. This would mean that the model is in place and enables consumers to be reimbursed where appropriate.

6.63 We would monitor the timeframe for the introduction of the model. If a suitable model had not been introduced by the end of September 2018, we would consider using our statutory powers to introduce an alternative model (see paragraph 6.32).

Question 13: Do you agree with our view that a contingent reimbursement model, if introduced, should be in place by the end of September 2018? Please explain.

Question 14: Should a phased or transition approach be used to implement a contingent reimbursement model? Please explain.

7 Next steps

Responding to our consultation

7.1 We want to hear your views on:

- Whether UK Finance's best practice standards will be effective in addressing the issue we identified in our super-complaint response and improve how PSPs respond to instances of reported APP scams.
- Our current view that a voluntary contingent reimbursement model should be introduced, and how this should be achieved. We are also asking for your views on the high-level principles we have set out and other key characteristics that a potential model should have.

7.2 A full list of the consultation questions can be found in Annex 1.

7.3 Please send your comments by 5pm on 12 January 2018 in electronic Word or PDF format to app-scam-pso-project@psr.org.uk or in writing to the address on page 2.

7.4 When we have received the responses to this consultation, we will consider:

- if UK Finance should make any changes to the best practice standards
- if it is appropriate to proceed further with the development of the contingent reimbursement model concept and, if so, which organisation is best placed to take it forward

7.5 If changes should be made to the best practice standards, we would expect to share with UK Finance the consultation responses (where appropriate in an aggregated, anonymised form) which will help it to make enhancements to the standards.

7.6 If a contingent reimbursement model should proceed, we would expect to share with the identified organisation:

- the high-level principles we would expect the model to meet
- the consultation responses (where appropriate in an aggregated, anonymised form) which will help the organisation when developing the model

7.7 As mentioned in Chapter 6, if it is appropriate to take the model forward, we propose to take an 'active observer' role in the design and implementation.

7.8 We expect to publish a statement on the outcome of this consultation and, if appropriate, the next steps for the best practice standards and the development and implementation of the model (including the name of the entity that would take it forward and the high-level principles). We will also look to publish the consultation responses.

Disclosure of information

7.9 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

7.10 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.

7.11 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.

7.12 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.

Glossary

Term or abbreviation	Description
authorised push payment (APP) scam	Scams in which people are tricked into sending money to a fraudster by making a payment from their bank account to another bank account.
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	CHAPS (Clearing House Automated Payment System) is 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.
Cifas	Cifas is a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime.
Data Protection Act 1998	The Data Protection Act 1998 is a United Kingdom Act of Parliament which defines the law on the processing of data on identifiable living people and is the main piece of legislation that governs the data protection.
Data Protection Bill	The Data Protection Bill 2017 will change data protection laws to reflect increasing amounts of data.
FCA	Financial Conduct Authority
Financial Fraud Action (FFA UK)	Financial Fraud Action UK (FFA UK) is the body responsible for leading the collective fight against financial fraud on behalf of the UK payments industry. Its membership includes the major banks, credit, debit and charge card issuers, and card payment acquirers in the UK. In July 2017, FFA UK became a constituent part of UK Finance, the new trade association representing the UK financial services industry.
Financial Ombudsman Service	The Financial Ombudsman Service is an alternative dispute resolution service. They were set up by Parliament to resolve individual complaints between financial businesses and their customers. They can look into problems involving most types of money matters – from payday loans to pensions, pet insurance to PPI. If they decide someone's been treated unfairly, they have legal powers to put things right.
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.
FSBRA	Financial Services (Banking Reform) Act 2013.

Term or abbreviation	Description
Image Clearing System (ICS)	Cheque imaging is the process that enables images of cheques to be exchanged between banks and building societies, through the Image Clearing System (ICS), for clearing and payment. This significantly speeds up the clearing process.
Information Commissioner's Office (ICO)	The UK's independent body set up to uphold information rights.
Joint Fraud Taskforce	The Joint Fraud Taskforce is made up of key representatives from government, law enforcement and the banking sector and has been set up to tackle fraud.
know your customer (KYC)	Know your customer (KYC) is the process of a business, identifying and verifying the identity of its clients.
malicious payee	A type of APP scam. 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).
maliciously misdirected payment	A type of APP scam. 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.
New Payment System Operator (NPSO)	The NPSO will consolidate Bacs Payment Schemes Ltd, the Cheque and Credit Clearing Company and Faster Payment Payments Scheme Ltd. The NPSO will also introduce the new payments architecture (NPA).
New Payments Architecture (NPA)	The Payments Strategy Forum has been planning new payments 'architecture' that is simpler, more accessible and more responsive to future user needs and innovation than the current model. This will be introduced by the NPSO.
'on-us' payment	Payments where the payee's PSP/payer's PSPs are the same entity.
payee	A person who is the intended recipient of transferred funds.
payer	A person who holds a payment account and allows instructions to be given to transfer funds from that payment account, or who gives instructions to transfer funds.
payment service provider (PSP)	A PSP, in relation to a payment system, means any person who provides services to consumers or businesses who are not participants in the system, for the purposes of enabling the transfer of funds using that payment system. This includes direct PSPs and indirect PSPs. Banks are one type of PSP.
Payment Systems Regulator (PSR)	The Payment Systems Regulator Limited, the body corporate established by the FCA under section 40(1) of FSBRA.

Term or abbreviation	Description
Payments Strategy Forum (the Forum)	The Payments Strategy Forum was announced by the PSR in its Policy Statement published in March 2015. The Forum is an industry-wide group consisting of representatives from consumer organisations and PSPs. It 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.
pull payments	Pull payments are payments where the person who is due to receive the money instructs their bank to collect money from the payer's bank.
push payments	Push payments are payments where a customer instructs their bank to transfer money from their account to someone else's account.
receiving PSP	The PSP that holds the payment account that receives money paid as part of an APP scam and which is under the control of a fraudster.
second EU Payment Services Directive (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.
sending PSP	The PSP that holds the payment account of the victim of an APP scam.
UK Finance	The trade association for the UK banking and financial services sector that represents around 300 firms providing finance, banking, markets and payment-related services.

PUB REF: CP17/2

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