FINANCIAL CONDUCT AUTHORITY
PAYMENT SYSTEMS REGULATOR

Which? authorised push payments super-complaint

PSR response

December 2016

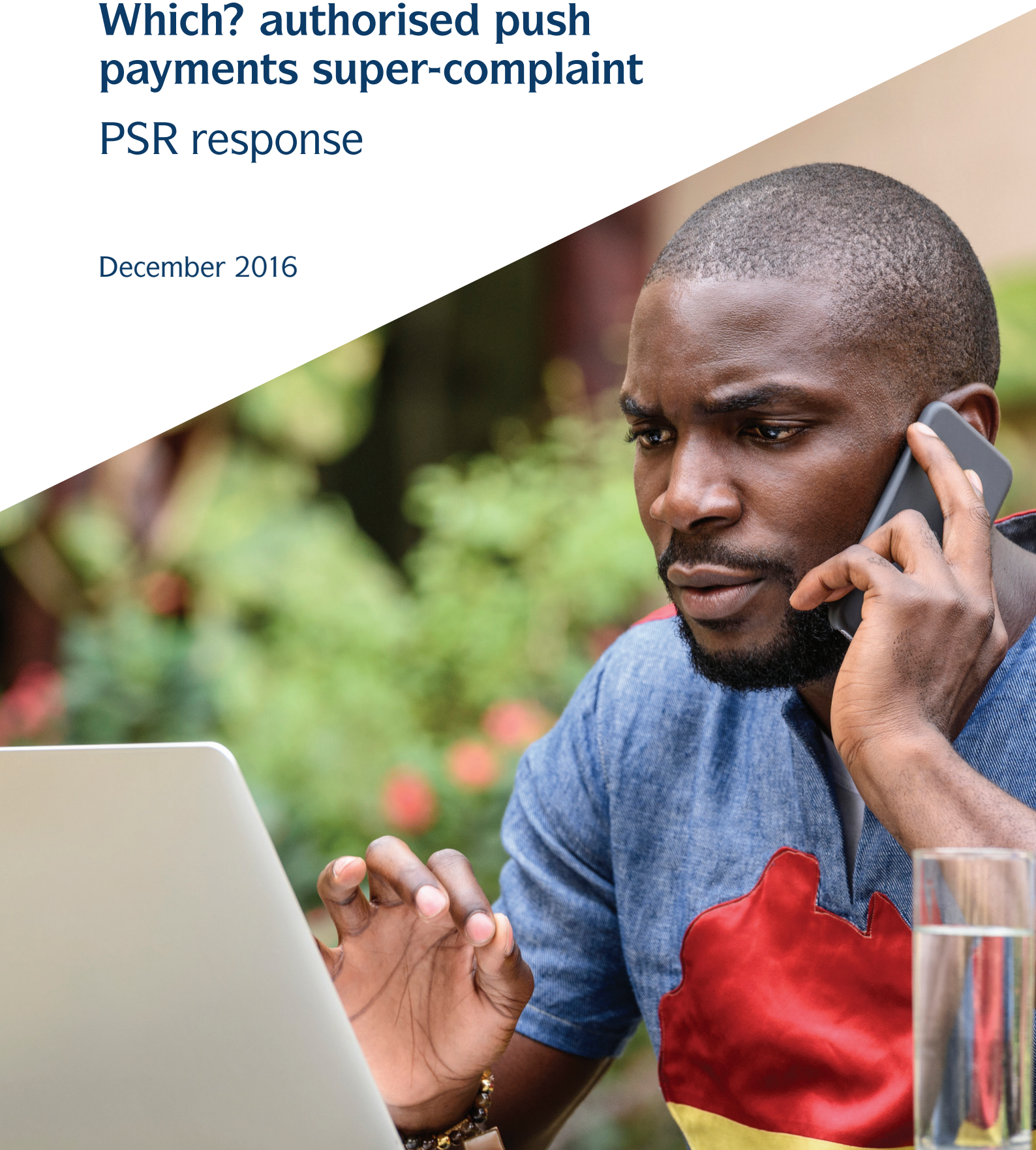


Table of contents

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

1 Executive summary

The super-complaint

1.1 On 23 September 2016 we received a super-complaint from Which? entitled *Consumer safeguards in the market for push payments*. Which? alerted the Financial Conduct Authority (FCA) to the super-complaint at the same time. This report is our response to Which? that, under statute, we are required to give within 90 calendar days.

1.2 In the super-complaint Which? argues that consumers face insufficient protection when they are tricked into making authorised push payments (APPs) as part of a scam. For example, this could be where a consumer purchasing a new house is tricked into transferring money to what they believe to be their solicitor's account, but it turns out that the account is controlled by a fraudster.

1.3 Which? further argues that consumers receive greater protections for other payment types, and that shifting liability for APP scams onto banks would better incentivise them to protect consumers. Which? asked us to investigate:

- the extent to which banks could change their conduct to reduce the harm from APP scams
- possible changes to legislation or regulation to alter incentives on banks and payment systems to ensure that more is done to manage the risks from APP scams and to protect consumers from harm

Our findings

1.4 There are three main issues that we consider need to be addressed:

1. The ways in which payment service providers (PSPs), which includes banks, currently work together in responding to reports of APP scams needs to improve.
2. There is some evidence to suggest that some PSPs could do more to identify potentially fraudulent incoming payments and to prevent accounts falling under the influence of scammers.
3. The data available on the scale and types of APP scams is of poor quality. Some of the initial evidence we have identified about the scale suggests that it may be significant and the general view held is that the prevalence of APP scams is likely to increase.

The scale of authorised push payment scams

1.5 Information on the scale of APP scams is currently limited and presents an inconclusive and uncertain picture. Estimates from the various data sources we were able to consider suggest an annual volume of APP scams in at least the tens of thousands, and possibly hundreds of thousands. In contrast, Financial Fraud Action UK (FFA UK) reported 1.5 million cases of debit and credit card fraud in 2015.

1.6 While there is uncertainty about the scale of the problem, the consensus among stakeholders is that APP scams are a growing problem. Reasons cited for the growth include the increased use of mobile and online technologies: as online banking becomes more popular, more push payments will be made; some types of APP scams utilise online platforms, such as auction and dating websites, as part of the scam; and increased online activity increases the potential for scammers to get access to personal data that they can exploit to perpetrate APP scams. Increased APP scams may also be a by-product of improvements in the payment systems – the growth of near real-time payments has made it easier for scammers to acquire and disburse the proceeds of scams more quickly, and improvements in security against other types of payment fraud mean that the consumers themselves may increasingly be seen as the weakest link in the payment chain.

1.7 The available evidence suggests that APP scams where the victim makes a payment to the intended person who subsequently turned out to be a scammer are more common than scams where the victim is duped into making a payment to the wrong account. The former appear to make up between 85% and 95% of total APP scams, although the average value of such scams tends to be smaller.

PSPs' current obligations, commercial incentives and actions

1.8 PSPs have a variety of policies and procedures in place that influence the consumer harm resulting from APP scams, policies and procedures that have evolved over time and in response to various legal obligations. We have found that it is important to distinguish between the sending PSP and the receiving PSP when thinking about whether PSPs should do more to help consumers.

1.9 While PSPs are not generally liable for APP scams, both sending and receiving PSPs are nonetheless under a range of obligations to prevent fraud. Existing legislation requires PSPs to 'know your customer', conduct due diligence, maintain appropriate records and to implement policies, procedures and training, with the aim of avoiding the facilitation of money laundering; requires PSPs to report financial crime in certain circumstances; and imposes a number of obligations on them concerning the safe use of so-called 'payment instruments' and payment instructions. The FCA's Handbook places additional obligations on certain PSPs,[1] including banks, to have adequate policies and procedures to counter the risk that they might be used for financial crime, including fraud.

1.10 Even if a PSP is not strictly liable under legislation, it may be required to compensate a customer for its losses by the Financial Ombudsman Service if the ombudsman service considers this to be fair and reasonable in the circumstances. The ombudsman service can hear any dispute arising out of the carrying on of a regulated activity. The ombudsman service has upheld complaints against both sending and receiving PSPs, though where an individual is not a customer of the PSP in question, the complaint must be sufficiently connected with the disputed payment.

1.11 The available evidence suggests that current legal obligations and commercial incentives already mean that the sending bank's interests are broadly aligned with those of the consumer. While specific practices vary, in general sending PSPs appear to have developed reasonably extensive measures to help prevent their customers from falling victim to APP scams. We also observe that sending PSPs generally appear to make reasonable efforts to assist their customers in recovering funds they have transferred as a result of an APP scam. In some instances we observe sending PSPs voluntarily refunding victims for the funds lost as the result of a scam. We

[1] The provisions of the FCA Handbook at SYSC 6 do not apply to PSPs unless they have part 4a permissions (as is the case for 'deposit takers').

do note, however, the recent findings of the ombudsman service that sending PSPs could do more to engage with victims of scams in a more sympathetic and timely fashion.[2]

1.12 The commercial incentives and obligations for receiving PSPs to ensure there are appropriate safeguards in place to protect customers of other PSPs that fall victim to APP scams are weaker than for sending PSPs. We have identified evidence of inconsistent practices among receiving banks in terms of steps taken to help prevent funds obtained as the result of scams being credited to accounts held by their customers. We also have identified indicative evidence that some PSPs may be more effective than others in preventing their accounts being opened by scammers or otherwise falling under the influence of scammers.

How PSPs interact

1.13 We have identified evidence that, in some instances, sending and receiving PSPs have problems engaging with each other in an effective and timely manner when attempting to recover payments made as the result of an APP scam. These difficulties may manifest themselves in a number of ways, including: unavailability of specialist fraud response teams at some receiving PSPs, 24 hours a day, seven days a week; inconsistent approaches to sharing information to assist in the recovery of funds; inconsistent approaches to 'freezing' alleged scammers' accounts to prevent the onward transfer of funds that may have been obtained as the result of a scam; and difficulties in agreeing indemnities to allow receiving PSPs to release funds remaining in accounts of alleged scammers.

1.14 The operators of the Faster Payments Scheme (FPS) and CHAPS payment systems, the two payment systems which consumers might use when falling foul of APP scams, do not have any rules, policies or procedures in place related to consumer protection against fraud or scams. Operators of these systems view it as outside their remit to intervene in what they view as private contractual matters between PSPs and their customers.

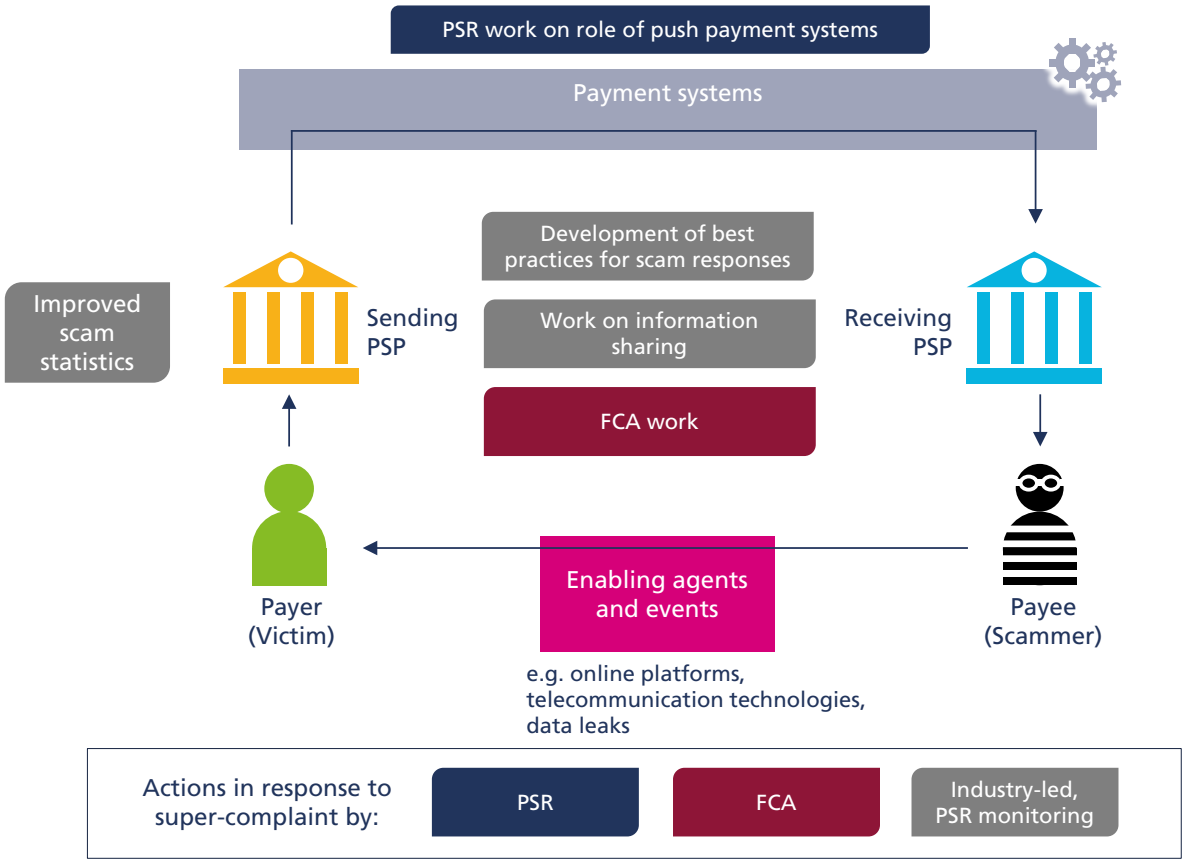
Actions to address APP scams

1.15 The package of work that we propose is motivated by a desire to make fraud more difficult and less prevalent. When APP scams do occur, we want to increase the chance that the victim will be able to recover the funds. In some cases, the work required has the potential to address fraud issues more widely than just APP scams.

1.16 There is already a range of work under way or planned for the near future that has the potential to help address consumer harm caused by APP scams. Particularly significant are the work of the Joint Fraud Taskforce and a number of the initiatives recently announced in our Payments Strategy Forum's final strategy (including the verification of payee work that should help tackle scams where the victim is duped into making a payment to the wrong account).

[2] FOS (2015) *Calling time on telephone fraud*. http://www.financial-ombudsman.org.uk/assets/pdf/vishing-insight-report2015.pdf

Figure 1: Actions in response to the super-complaint



Source: PSR

1.17 We have sought to develop proposals that complement such work, making sure the issues we have identified are addressed. To that end, we have agreed with FFA UK a programme of work that the banking industry should lead on, that will assist in both understanding the scale of APP scams and in improving how PSPs work together in responding to them:

- Industry, liaising with the Information Commissioner's Office 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 (for example, information that would help victims recover their money).

- Industry 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 would expect this to cover issues such as the availability of fraud specialists and processes for agreeing indemnity agreements between banks.

- Industry to develop, collect and publish robust APP scam statistics, to address the lack of clear data on the scale and scope of the problem, and to enable monitoring of the issue over time.

1.18 We will monitor this work on an ongoing basis, and commit to review industry progress in the second half of 2017.

1.19 The PSR will consider the potential for the operators of the CHAPS and FPS payment systems to play an expanded role in helping to minimise the consumer harm caused by APP scams. We will look to publish specific terms of reference for this work in early 2017 and look to publish the

findings of our work in the second half of 2017. We envisage this work will include consideration of how internationally comparable push payment system operators are involved in minimising risk of consumer harm around APP scams and fraud more generally.

1.20 The FCA will undertake the following actions:

- work with firms to tackle concerns around both sending and receiving banks in relation to APP fraud
- evidence received in relation to the super-complaint will be examined by FCA supervision, which will address any firm-specific issues directly
- if, following the above steps, there are unresolved sector-wide issues, the FCA will initiate further work. Any such work should consider the developments made since the thematic review of banks' defences against investment fraud in 2012.[3]

1.21 Which? presented two potential options for intervention in their super-complaint (making PSPs liable for reimbursing victims of APP scams or introducing risk management standards that PSPs must meet when executing APPs). At this stage we are not minded to directly pursue either of these as the evidence that we have been able to collect to this stage is not sufficient to justify the proportionality of either of the proposed suggestions and we are aware of possible unintended consequences. However, as our work progresses through 2017 and additional evidence comes to light, we will consider whether it is appropriate to propose changes to the obligations or incentives that PSPs have with regard to APP scams.

[3] Financial Services Authority (2012) *Banks defences against investment fraud: detecting perpetrators and protecting victims*, www.fsa.gov.uk/static/pubs/other/banks-defences-against-investment-fraud.pdf

2 Introduction

The background to the super-complaint

2.1 On 23 September 2016 the consumer body Which? submitted a super-complaint to us regarding the consumer safeguards for 'push' payments. Which? is concerned that there are no protection measures in place for people who are tricked into sending money to a fraudster via the banking system. A super-complaint requires us to respond within 90 days, under section 68 of the Financial Services (Banking Reform) Act 2013 (FSBRA).

2.2 Push payments are payments where a customer instructs their bank to transfer money from their account to someone else's account. In contrast to push 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.

2.3 Both push and pull payments can either be authorised or unauthorised. An authorised payment is one where the customer has given their consent for the payment to be made – and this can include situations where the customer has been tricked into giving that consent. An unauthorised payment is one made without the customer's consent – for example, a payment made due to a bank error or one made using a stolen payment card.

2.4 The Which? super-complaint suggests that customers have more legal protection in scams where they have paid with a pull payment rather than a push payment. Which? points out a number of existing consumer protection mechanisms for card payments (under both the Consumer Credit Act 1974 for credit cards and the so-called 'chargeback rules') and for direct debits (such as the Direct Debit Guarantee).

2.5 Specifically, Which? believes an investigation is needed to address:

- the extent to which banks could change their conduct to reduce the harm to consumers from scams that trick them into authorising payments to a fraudster
- possible changes to legislation or regulation, to change the incentives for banks and payment system operators (PSOs) to protect consumers

2.6 Which? argues that additional steps should be taken to protect consumers from push payment scams. It suggests two potential remedies:

- Make banks liable for reimbursing consumers when an APP has been made to a scammer, unless the consumer has acted fraudulently or with gross negligence
- Introduce standards for risk management that banks would be required to meet when executing APPs. If a bank had not followed these rules it would be liable to reimburse consumers who had authorised a push payment to a scammer.

The scope of the Which? super-complaint

2.7 The focus of the Which? super-complaint is on APP frauds in the UK. It focuses specifically on fraud cases involving consumers in the UK transferring money between two UK bank accounts.

2.8 Our response has consequently focused on these types of frauds. Nevertheless, it is clear that some of the issues have read across to other types of frauds. For example, businesses have also been the victims in APP frauds. Solutions designed to tackle this problem for consumers will, in many cases, also help businesses.

Our approach

2.9 In responding to the super-complaint, we sought to gain an understanding of:

- the types and scale of APP scams, including recent trends and the potential for future growth
- the legal and regulatory context that governs the protections that consumers currently receive for push payments and how this compares to other payment types
- what PSPs and payment systems currently do, and what they could do, to prevent APP scams and how they respond to protect consumers when they do occur
- changes, either from industry participants, other regulators or government, that are already under way or under consideration specifically aimed at addressing consumer harm caused by APP scams
- any other developments on the horizon that have the potential to impact – positively or negatively – APP scams that harm consumers

2.10 To gain an understanding of these issues, we undertook an extensive programme of stakeholder engagement and research. Specifically, we:

- issued information requests to the six largest providers of payment accounts to UK consumers and to the operators of the main UK interbank payment systems
- had bilateral meetings with 40 external stakeholders, including large and small PSPs, trade associations, consumer bodies, and other regulators and government bodies
- commissioned an external research agency to undertake a survey of approximately 2,000 UK adults on the scale of push payment fraud
- analysed additional evidence provided to us by Which?, including consumer views collected through their online scams reporting tool
- considered evidence submitted directly to us through our dedicated super-complaints email inbox

2.11 We are grateful to all stakeholders that have provided input to assist us in developing a robust and evidenced-based response to the super-complaint.

2.12 We have also worked closely with the FCA throughout the process of responding to the super-complaint. In particular, we have drawn on the FCA's specialist expertise where appropriate and have formed our recommendations after consulting the FCA and in awareness of its own response to the issues highlighted in the super-complaint.

The structure of this response document

2.13 Our response document is structured as follows:

- **Chapter 3** presents background to APP scams and discusses the scale, nature and trends of push payment fraud, compared to other types of payment fraud
- **Chapter 4** discusses the current legal and regulatory situation that determines consumer safeguards against APP scams
- **Chapter 5** sets out the current approach of PSPs and PSOs in providing consumer safeguards against APP scams
- **Chapter 6** discusses a number of further legal considerations around potential changes to consumer safeguards against APP scams
- **Chapter 7** presents a range of future developments that have the potential to impact consumer harm from APP scams
- We then conclude in **Chapter 8** with summarising the issues we identify and the next steps we will take.

2.14 There are four annexes. The first provides a glossary of terms. The second lists the parties we met with. The third describes some of the data sources we used. The fourth provides more details on the legal and regulatory obligations PSPs currently face.

3 Background to authorised push payment scams

Overall, the data available on the scale and types of APP scams is of poor quality. Some of the initial evidence we have identified about the scale suggests that it may be significant.

Many stakeholders have told us that the prevalence of APP scams is increasing. Several reasons have been offered for this trend: the increasing use of near real-time payments and online banking; and developments to tackle unauthorised push payment fraud leading to scammers targeting consumers directly, with some scammers viewing them as the now most vulnerable link in the chain.

APP scams can have both adverse financial and emotional consequences for victims. Wider impacts on victims may include a loss of trust and confidence in using internet banking, and online services more generally. The values involved in APP scams vary significantly but can involve significant sums.

Victims of APP scams are not confined to especially vulnerable consumers – a number of stakeholders observed that anyone could be a victim. Some stakeholders have told us that older consumers may be more vulnerable to fraud, although the evidence we have identified for this is not consistent.

While the super-complaint focuses on the harm caused to consumers that fall victim to APP scams, both small and large businesses are also targeted in APP scams.

3.1 In this chapter, we provide an overview of the information available about the scale of authorised push payment (APP) scams in the UK. We consider the factors that are driving their growth and how prevalent they are relative to other types of fraud.

3.2 Specifically, the sections that follow set out:

- an overview of different payment types
- the types of payments and scams that are the focus of the Which? super-complaint
- the scale of APP scams
- the impact of APP scams on victims
- factors contributing to the growth of APP scams
- APP scams and businesses

Overview of payment types

3.3 A **push payment** is a payment that occurs when a payer instructs their PSP to send funds to the payee's account, typically held at another PSP. Push payments initiated by consumers are typically made using three methods:

- **Faster Payments Scheme (FPS):** This is the UK's real-time, low-value retail payments system. Customers can make single immediate payments, forward-dated payments or initiate standing orders through mobile, internet and telephone banking.
- **CHAPS:** This is the UK's same-day high-value payment system. For consumers, it is most generally known as the payments system used for UK house purchases.
- **On-us payments:** These are payments where the payer's PSP and the payee's PSP are the same entity and payments do not flow through a payment system. Payments are instead completed across the internal systems of the PSP.

3.4 The super-complaint also refers to direct credit payments made using the Bacs payment system. While Bacs Direct Credit payments are a type of push payment, they are almost exclusively initiated by businesses and government, rather than consumers. PSPs do not offer Bacs Direct Credit facility to consumers. As a result, we have excluded Bacs Direct Credit payments from the direct scope of our response.

3.5 In contrast, a **pull payment** is a payment that occurs when an account holder provides details of their account to a third party (such as a utility company) and provides consent to that third party drawing funds from their account. Pull payments are typically made using three main payment systems:

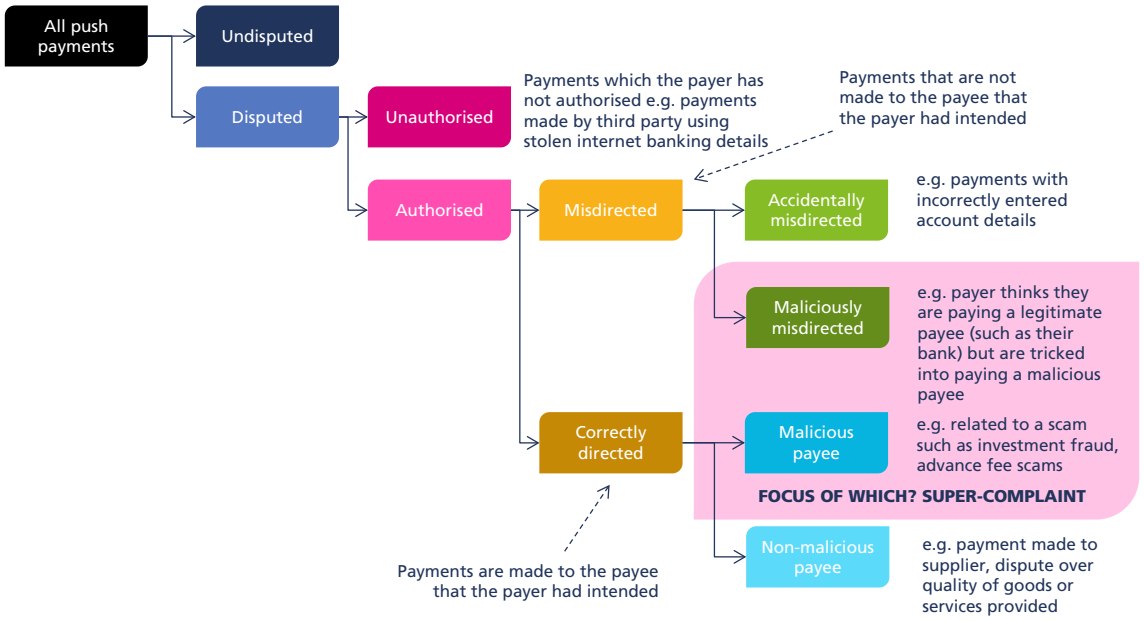
- **Card schemes:** Schemes such as Visa and MasterCard enable consumers to make payments using credit, debit and prepaid cards.
- **Bacs Direct Debit:** A direct debit is an instruction from a payer to their bank authorising a third party to collect varying amounts from their account as long as the payer is given advance notice of the collection amount and collection date.
- **Cheque payments:** The Cheque and Credit Clearing Company (C&CCC) manages the cheque clearing system in England and Wales. C&CCC processes cheques, traveller's cheques, warrants, postal orders, bank drafts and government payable orders.

The scope of the super-complaint

3.6 Which? defines the scope of its super-complaint with regard to both the payment instrument used to obtain funds as part of a fraud (push payments) and the type of fraud used to obtain those funds (*authorised* payment scams).

3.7 To understand the type of fraud within scope of the super-complaint, and the specific sub-types within those that are in scope, we present a breakdown of different reasons why a payer may make a payment and then subsequently dispute it (Figure 2 below).

Figure 2: Categorisation of disputed payments



Source: PSR

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

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

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

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

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

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

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

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

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

3.13 Based on the categorisations outlined above, the Which? super-complaint focuses on two categories of disputed APPs that involve scams:

- maliciously misdirected payments

- correctly directed payments to malicious payees

3.14 In our response, we collectively refer to these as **APP scams**. Which?'s focus on APP scams is driven by the argument that consumers do not benefit from the same level of protection that they get with other types of payments (specifically, pull payments and unauthorised push payments).[4]

Common types of APP scams

3.15 Through the course of collecting evidence to respond to the super-complaint, we have identified a range of common types of both malicious misdirection and malicious payee APP scams.

Malicious misdirection

3.16 Common types of malicious misdirection APP scams we have identified include:

- **Invoice and mandate scams**: In this scam, the victim attempts to make a payment to settle a legitimate obligation with a legitimate payee but the scammer manages to intervene to convince the victim to redirect the payment to the scammer's account.

- **Safe account scam**: This occurs when a scammer contacts the victim purporting to be from the victim's bank. The scammer then convinces the victim to transfer money to a different account in order to safeguard it but that is in fact controlled by the scammer.

- **Impersonation scam**: This occurs when a scammer contacts the victim purporting to be from a service provider (such as a broadband provider) and asks the victim to make a payment. Reasons given may be to settle a fictitious fine or to cancel out an purported erroneous refund.

[4] Which? super-complaint, Consumer Safeguards in the market for push payments, Which, 23 September 2016: http://www.staticwhich.co.uk/documents/pdf/which-super-complaint---consumer-safeguards-in-the-market-for-push-payments-453230.pdf

Malicious payee

3.17 Common types of malicious payee APP scams we have identified include:

- **Purchase scam**: This occurs when the victim pays in advance for a good or a service that they never receive. These scams may involve the use of an online platform such as an auction website. One large bank explained that of the push payment scams that it has encountered over the last 12 months, the majority (about 65%) were malicious payee versions of purchase scams. One consumer organisation told us that this is the most common type of fraud that consumers report.

- **Investment scam**: In this scam, a scammer convinces an investor to move their money to a fictitious fund offering significantly higher returns than they are currently receiving. Other instances of investment fraud involve carbon credits, land banks and wine scams. One consumer organisation told us that where consumers became victims of this type of scam the losses were particularly high.

- **Romance scam**: In this scam, the victim is convinced to make a payment to a person that they have met online and with whom they believe they are in a relationship.

- **Advance fee scam**: In this scam, scammers convince victims to pay a fee which would then result in the release of a much larger payment to the victim.

Examples of disputed APPs involving scams

We received a range of examples of APP scams from members of the public that emailed our super-complaints inbox. We present below examples we received of malicious misdirection and malicious payee APP scams:

- **Maliciously misdirected payment:** Mr B received two calls from someone pretending to be from his bank. They asked whether he authorised two transactions in Manchester and London. Mr B denied authorising these transactions and was told his account had been compromised. Mr B was then told that, in order to protect his account, he would need to transfer money into a new account which turned out to be under the scammer's control. Mr B ended up losing £18,700, which could not be recovered.

- **Correctly directed payment to a malicious payee:** Mr S attempted to buy a motorhome online. Mr S transferred £4,500 to the purported seller of the motorhome, who turned out to be a scammer. The motorhome was never provided. The police were informed but the money could not be recovered.

The scale of APP scams

Estimates from publicly-available data

3.18 In the super-complaint, Which? highlights the lack of public data sources available to reliably estimate the current scale of APP scams.

3.19 We agree that, at present, there is very limited public data available. The main public data sources on fraud are published by FFA UK and the Office for National Statistics. However, neither report data in a manner that allows the identification of the scale of APP scams.

3.20 FFA UK publishes fraud statistics[5] twice yearly based on data reported by its members (who include banks, credit, debit and charge card issuers, and card payment acquirers). However, it does not currently report data on APP scams – data reported relates to card fraud, remote banking fraud (which relates to unauthorised push payments only) and cheque fraud.

3.21 The ONS has recently added questions to its Crime Survey for England and Wales (CSEW) on fraud and computer misuse. The CSEW is a face-to-face survey which asks respondents who are residents in households about their experiences of crime in the past year. Estimates of fraud derived from answers to these questions have recently been published as experimental statistics.[6]

3.22 However, deriving the scale of APP scams from these statistics is complicated by definitional issues around the reporting categories used. These are aligned to the manner of the fraud (for example, an advance fee fraud), rather than the payment method used to effect the fraud (for example, authorised or unauthorised push payment or pull payment, cash, cheque etc.).

Estimates from other data sources

3.23 Given the lack of publicly available data, we sought to gain an understanding of the scale of APP scams using several different approaches, including using our formal regulatory information gathering powers. Specifically, we:

- issued information requests to the six largest UK PSPs and to relevant PSOs
- commissioned an independent consumer survey of a representative sample of approximately 2,000 UK adults
- considered data and evidence provided to us by other stakeholders, including the Office for National Statistics, FFA UK and Which?.

3.24 The results of our efforts to identify the scale of APP scams were ultimately inconclusive. There is currently very limited high quality data available on the scale of APP scams. In the time available to us, we have not been able to come to a definitive, consistent view on the current magnitude of APP scams. The evidence we have been able to collect suggests that the annual volume of APP scams may lie anywhere between 40,000 to 850,000. Table 1 below presents estimates of APP scam volumes from different data sources, and compares it to FFA UK and ONS data on volumes of other fraud types.

3.25 We provide further detail on these estimates in the section below.

[5] See, for example, FFA (2016) *Fraud the facts 2016*. https://www.financialfraudaction.org.uk/wp-content/uploads/2016/07/Fraud-the-Facts-A5-final.pdf
[6] ONS (2016) *Crime in England and Wales: Experimental tables.* https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/datasets/crimeinenglandandwalesexperimentaltables

Table 1: Estimates of annual volume of APP scams, compared to reported volumes of other fraud types

Source	Value (000s)
Estimated annual volume of APP scams	
Estimates from data provided by PSPs	48
Estimates provided by ONS based on CSEW data	43
Estimates based on Action Fraud data:	
FFA UK	47
ONS	10s of thousands, possibly over 100 thousand
Estimates based on results of our consumer survey	855
Reported volumes of other fraud types (for comparison)	
FFA UK (2015)	
Payment card fraud	1,487
Internet, telephone and mobile banking fraud*	33
Cheque fraud	6
*ONS based on CSEW (year ending June 2016)***	
Bank and credit account fraud	2,356
Non-investment fraud	1,028
Advance fee fraud	117
Other fraud	116
Total fraud	**3,616**

Source: PSR analysis based on data and information from PSPs, ONS, FFA UK and TNS
* Relates to unauthorised fraud only; ** APP scams may sit within any of the four categories used in the ONS CSEW

Estimates from data provided by PSPs

3.26 Only a few of the six PSPs that we asked for data were able to provide sufficiently disaggregated figures showing the recorded number of APP scams that their customers had suffered during the past 12 months.[7] If the experience of these banks is representative of the industry and using a scaling approach, it would imply an annual volume of about 48,000 incidents. We would caution that this approach makes strong assumptions about the incidence of APP scams for the PSPs we have data for being representative for the industry as a whole.

Estimates provided by ONS based on data from CSEW

3.27 On our behalf, the Office for National Statistics (ONS) undertook analysis of interview data from the Crime Survey for England and Wales (CSEW). This analysis suggests that there may have been around 43,000 APP scams in 2015.[8] The ONS cautions, however, that this estimate is

[7] None of the operators of push payment system we issued with information requests collect data on the scale of APP scams.
[8] The data has been published as experimental statistics. Although the data is 2016, the survey covers incidents of fraud experienced in the year prior to the survey interview.

likely to be lower than the true level as there is likely to be a response bias against victims of APP scams participating in their survey.

Estimates based on analysis of Action Fraud data

3.28 We also considered estimates of APP scams we obtained that are based on data from Action Fraud, the fraud and cyber-crime reporting centre run by the City of London Police. Financial Fraud Action (FFA) provided an estimate based on Action Fraud data of around 47,000 cases of authorised fraud reported to police in 2015 where funds had been paid from victims' bank accounts or where funds had been taken from victims' accounts. Separately, preliminary, high-level analysis by the ONS of Action Fraud data, suggests that annual frauds reported to the police that relate to authorised push payments are likely to be in the tens of thousands, and possibly over one hundred thousand each year. An added consideration regarding data on fraud reported to the police is that some instances of fraud may not ever be reported, for reasons including embarrassment or the fraud having been resolved with the victim's PSP.

Estimates based on analysis of results of our consumer survey

3.29 Results from the consumer survey we commissioned indicate that around 2% of those surveyed report have fallen victim to an APP scam at some point within the last 12 months. If these results are representative of the UK adult population, it would suggest that approximately 855,000 people could have fallen victim to APP scams in the last 12 months.

The scale of malicious payee scams relative to malicious misdirection scams

3.30 The evidence we have seen suggests that most APP scams seem to take the form of payments made to malicious payees rather than maliciously misdirected payments:

- Our analysis of the data from the PSPs able to provide the granular data suggests that in volume terms, these malicious payee scams accounted for around 95% of all APP scam cases.

- Which? analysis of data collected through their online scam reporting tool indicates that 5% of the reported scams related to invoice or mandate scams, a type of malicious misdirection scam.

3.31 Further, evidence suggests that the average value of funds transferred as part of a malicious misdirection scam is greater than that involved in malicious payee scams:

- Our analysis of the data from the PSPs able to provide the granular data indicates the average amount involved in a malicious misdirection scams was £5,600, compared to £3,000 for a malicious payee scam.

- Which? analysis of data collected through their online scam reporting tool indicates that the median amount involved in invoice or mandate scams was £6,500, compared to £1,200 for all reported scams.

The impact of APP scams on victims

3.32 APP scams often have severe adverse consequences for victims. Several stakeholders explained that in addition to the direct financial impact on victims, they can also have a negative emotional affect, particularly on victims' confidence and trust in the financial system. Stakeholders also mentioned the disproportionate impact that fraud can have on certain vulnerable consumers (see section on vulnerable consumers later in this chapter).

The financial impact on victims of APP scams

Values involved in APP scams

3.33 The losses that victims of APP scams incur appear to vary considerably, but in many instances involve material sums of money:

- Of the respondents to our consumer survey that reported being victims of APP scams, 88% reported paying less than £1,000 as a result of the scam.
- Analysis of the granular data on APP scams provided by the limited number of PSPs able to provide it shows that the average amount involved in APP scams was around £3,000, although this is likely skewed upwards by amounts from the largest reported scams, which involved several hundred thousands of pounds. We would caution that this analysis is based on a very limited sample of PSPs and may not be representative of trends across the industry.
- Of the 670 people that reported a fraud using Which?'s online tool, the median loss was £1,200. However, the single largest loss was approximately £400,000.
- An ONS review of the cases of APP scams reported by victims through the CSEW survey also showed that the individual losses reported by victims were generally higher than those reported for other types of fraud. The review showed that typically, individuals reported losses running into several hundred or single thousands of pounds.

Recovery of funds

3.34 In terms of victims recovering money lost to APP scams, the data we have been able to identify again tells an inconsistent story:

- Of the respondents to our consumer survey that reported being victims of authorised push payment scams, 71% got all or most of their money back. 27% of victims did not get any money back from their banks.
- Which? analysis of the data they collected from members of the public using their online scam reporting tool indicates that of the 670 instances of bank transfer scams reported, 48% involved cases where victims recovered no funds.
- Analysis of the granular data on APP scams provided by the limited PSPs able to provide it shows that on average 11% of the disputed payments related to authorised push payment scams were reimbursed, although this masked significant variation between PSPs. We would caution that this analysis is based on a very limited sample of PSPs and may not be representative of trends across the industry.

APP scams and vulnerable consumers

3.35 As part of our evidence gathering process, we asked stakeholders for their views on what impact the APP scams by Which? have on vulnerable consumers.

3.36 We defined a vulnerable consumer as someone who, due to their personal circumstances, is especially susceptible to detriment, particularly when a firm is not acting with appropriate levels of care. The PSR has a duty to give due regard to the impact of its decisions on persons with a relevant protected characteristics, as defined in the Equality Act 2010, Section 149(7). Those characteristics are age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex and sexual orientation.

3.37 In our discussions with stakeholders, we found it difficult to separate out the impact on vulnerable consumers of APP scams from fraud and other scams more generally. As a result, the discussion in this section relates to overall fraud, rather than APP scams specifically.

3.38 In our discussions with stakeholders, we received two main narratives with regards to the impact of fraud on vulnerable consumers:

1. Some stakeholders explained that they had not seen evidence to suggest that vulnerable customers are more likely to be impacted by fraud. One large PSP explained that it is difficult to conclude that the features of the market highlighted in the super-complaint disproportionately affected vulnerable customers. A number of stakeholders told us that anyone, including financially and technologically literate customers, could find themselves in a position in which they could be vulnerable to fraud. For example, the Conveyancing Association explained that there was concern amongst law firms that they were being targeted by fraudsters. They explained that their members were worried about misdirection of client funds through clients being duped into sending their deposit to a fraudster's account, or law firm's misdirection of funds through similar frauds (which could lead to an action for breach of trust, as well as reputational damage) and also their own funds.

2. A number of stakeholders also explained that fraudsters prey on particular customers and those with specific vulnerabilities (for example, investment scams targeting customers looking for strong returns). One large PSP explained that there is significant industry work under way to introduce 'vulnerable customer markers' which could help to identify and prevent fraud.

3.39 Examples of types of customers perceived by stakeholders as particularly vulnerable to falling victim to fraud include:

- older customers
- low income customers
- young people (for example, through social media)
- technologically illiterate customers
- customers with poor English
- customers with disabilities

3.40 In addition to being more likely to fall victim to fraud, several stakeholders told us that fraud has a disproportionate impact on affected consumers that are vulnerable. A payment system operator explained that fraud is likely to have a bigger impact on the overall financial health of vulnerable customers. Age UK also highlighted the especially damaging impact that fraud can have on older people as victims who may not have the opportunity to generate funds to replace the financial loss that they have suffered.[9]

[9] Only the tip of the iceberg: Fraud against older people, evidence review, Age UK, April 2015, Page 6,7, 45: http://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true, Stemming the tide, older people and mass marketed fraud, December 2014, page 11: http://www.ageuk.org.uk/documents/en-gb/for-professionals/policy/consumer-issues/age_uk_stemming_the_tide_-_mass_marketed_fraud,_dec_2014.pdf?dtrk=true

Fraud and older consumers

3.41 Several stakeholders identified older customers as being particularly susceptible to falling victim to fraud. This was for a variety of reasons, including that older people:

- may have less experience with technologies such as the internet and online banking
- may be socially isolated and more willing to engage with potential scammers
- may suffer from cognitive impairment
- are sometimes overconfident in their financial skills
- write significantly higher volumes of cheques

3.42 A range of evidence we identified supported older consumers being particularly vulnerable to fraud:

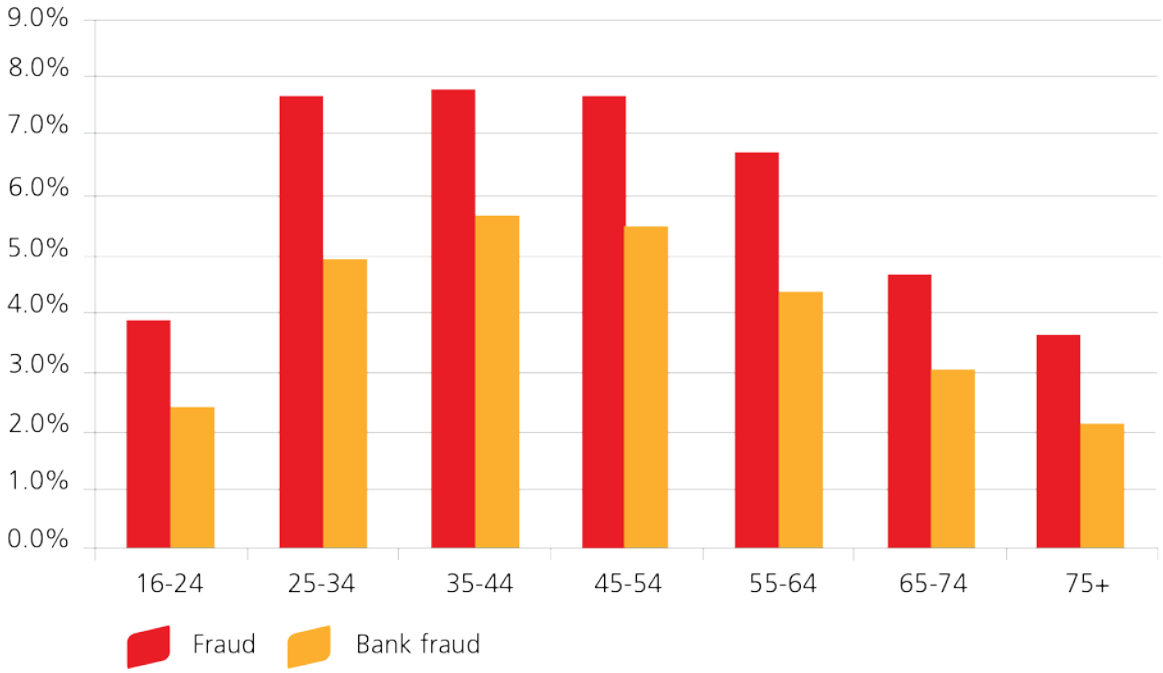
- Several PSPs identified that the average age of fraud victims were individuals over 60 or that the 'typical profile' of a fraud victim were individuals in their 60s.
- Several consumer organisations provided evidence that older consumers were disproportionately affected by fraud. Victim Support found that 35% of all fraud referrals that they received in 2015 came from victims who were over 65, despite making up only 18% of the population. Research carried out by Age UK found that older people are more vulnerable to certain types of fraud (such as doorstep fraud, pension liberation scams and investment fraud) due to particular circumstances such as social isolation or cognitive impairment. Age UK found that over half of people over the age of 65 believed that they had been targeted by fraudsters.[10] Another consumer organisation told us that the majority of people who reported cases of fraud to them were older people, but noted that fraud affects a wide range of people.
- In its insight report into telephone fraud (such as vishing), the Financial Ombudsman Service found that although this type of fraud affected a variety of age groups, older consumers were disproportionately represented in the complaints they received. In particular, the ombudsman service found that over 80% of consumers who were victims of telephone fraud were over the age of 55, with more than half of all victims were over 65 and around 25% were over 75.[11]

3.43 We considered other available quantitative data on the age characteristics of fraud victims. The ONS CSEW reports data on the incidence of fraud broken down by age group (see Figure 3 below). This evidence does not support the view that older consumers are more likely to fall victim to all fraud, at least when fraud is considered in aggregate. The incidence rate of both fraud overall and bank fraud peaks in the 35-44 age bracket, with incidence rates actually *falling* in higher age cohorts. Analysis of the results of our consumer survey by age group similarly did not indicate an increased relative incidence of APP scams among older consumers, although the limited sample sizes involved in each age category limit the robustness of this finding.

[10] Age UK, *Only the tip of the iceberg: Fraud against older people, evidence review* (April 2015), page 6, 7, 45: http://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true

[11] Calling time on telephone fraud, a review of complaints about vishing scams, Financial Ombudsman Service, July 2015, page 5, 21: http://www.financial-ombudsman.org.uk/assets/pdf/vishing-insight-report2015.pdf

Figure 3: Proportion of adults (within age group) who were victim of fraud (Year ending June 2016)



Source: ONS CSEW Experimental Tables, Table E7. Fraud includes bank and credit account fraud, non-investment fraud, advance fee fraud and other fraud.

Factors contributing to growth of APP scams

3.44 We have not been able to quantitatively identify trends in the scale of APP scams due to the absence of data and limited time available to us. However, the consensus among stakeholders seems to be that the problem is increasing. Five PSPs told us that APP scams have become increasingly common in recent years. One large PSP told us that it had seen month-to-month increases. Another PSP explained that unauthorised fraud was more prevalent in the past but that, over the last two years, they were now seeing increasing cases of APP scams.

3.45 The information and evidence that we have received from various industry stakeholders has suggested that the growth of APP scams can be attributed to two main factors:

- Increased security measures that address unauthorised payment scams driving an increase in APP scams
- The growing use of near real time payments, and online and mobile banking

Improved security measures driving increased focus on consumers

3.46 We have been told that an important driver of this recent growth has been the increased security measures introduced by PSPs around payment channels such as internet banking (for example, the use of two-factor authorisation). This has led scammers that have traditionally focused on scams involving unauthorised payments to transfer their efforts onto APP scams, with consumers themselves now viewed as the 'weakest link'.

3.47 One PSP explained that the traditional methods of phishing to obtain internet banking credentials were in decline because banks now had sophisticated software capable of detecting

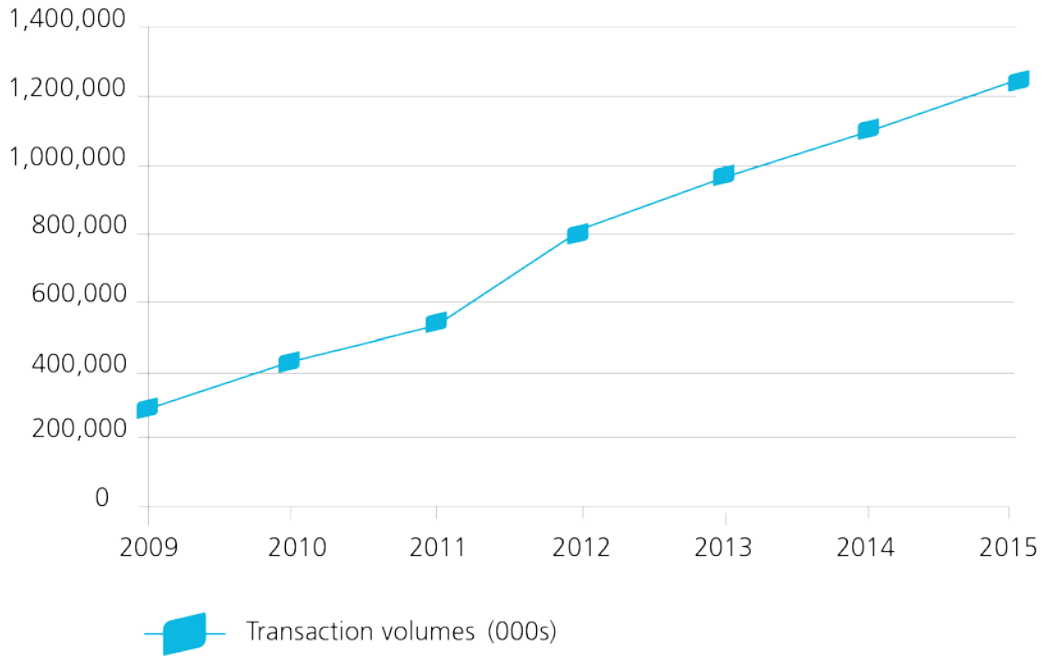
any unusual patterns. Four stakeholders explained that they have seen a recent increase in telephony-based social engineering of consumers.

Growing use of near real-time payments and internet banking

3.48 Several stakeholders cited the increasing growth and importance of near real time payments over the last few years as an important contributor to the increased prevalence of APP scams. Increased use of near real time payments has meant that scammers are able to both acquire and disburse the proceeds of scams at a much quicker rate than previously possible.

3.49 In the UK, near real time push payments made by consumers are made over the Faster Payments system. Figure 4 shows that over the period from 2009 to 2015, Faster Payment transaction volumes have been increasing year on year. Further, Payments UK forecast that the total number of payments processed using Faster Payments service will reach 2.2 billion payments in 2025.[12]

Figure 4: Faster Payments – annual payment volumes



Source: Payments UK

3.50 The increased use of the Faster Payments system is associated with the increased use of internet and mobile banking. Online banking use by UK adults has grown steadily over the last decade, with 60 per cent of all UK adults now using the internet for banking in comparison to only 30% in 2007.[13] Increasing use of internet and mobile banking services could present further opportunities for scammers to exploit online banking customers and add to the scale of authorised push payment scams.

[12] Extract from UK Payments Markets 2016, Payments UK, page 7: http://www.paymentsuk.org.uk/sites/default/files/publication-free/UK%20Payment%20Markets%20Summary%202016%20-%20Free%20Download.pdf
[13] Internet access, households and individuals, Office for National Statistics, 4/08/16: https://www.ons.gov.uk/peoplepopulationandcommunity/householdcharacteristics/homeinternetandsocialmediausage/datasets/internetaccesshouseholdsandindividualsreferencetables

APP scams involving businesses

3.51 Although the focus of the super-complaint is APP scams that target consumers, businesses (especially small and medium-sized enterprises (SMEs)) often also fall victim to APP scams.

3.52 There are two types of APP scam that specifically target businesses:

- CEO impersonation scams
- invoice redirection scams

3.53 In a **CEO impersonation scam**, employees of businesses receive correspondence from a fraudster that appears to be from the chief executive officer of the company (or someone senior such as a director), requesting that an urgent payment is made to a third party for a specific reason. The details of the correspondence, including logos, writing styles and signatures can be convincing enough to prevent recipients from following up to confirm that the payment request is genuine.

3.54 Action Fraud recently reported that over £32 million has been lost to fraudsters as a result of CEO impersonation scams between July 2015 and January 2016.[14] Of this amount, only £1 million has been recovered by the victims. This is because businesses take some time to realise that they have fallen victim to a scam. By the time they report the loss, the fraudsters have closed their bank accounts. According to Action Fraud, 52% of all companies targeted by this type of fraud are limited companies, with 22% of all victims being London-based businesses.

3.55 **Invoice redirection scams** involve scammers posing as known suppliers, contacting businesses and asking for bank account details to be amended. That way, when the business receives an invoice from that supplier and settles it, the funds are diverted to the account of the third party. According to Cifas, smaller businesses are more vulnerable to this type of fraud. In addition, they are more likely to struggle to recover from the losses incurred from such scams.[15]

3.56 Several PSPs told us that they have recently seen a significant increase in the volume and sophistication of these types of scam.

3.57 While out of the immediate scope of our response to the super-complaint, we acknowledge the wider societal harm caused by APP scams that target businesses. This wider impact of APP scams only provides additional support for the concerns and actions we outline in the remainder of our response.

Conclusions

3.58 Overall, the data available on the scale and types of APP scams is of poor quality. Some of the initial evidence we have identified about the scale suggests that it may be significant and the general view held is that the prevalence of APP scams is likely to increase.

3.59 While there is uncertainty about the scale of the problem, the consensus among stakeholders is that APP scams are a growing problem. Reasons cited for the growth include the increased use of mobile and online technologies: as online banking becomes more popular, more push payments will be made; some types of APP scams utilise online platforms, such as auction and dating websites, as part of the scam; and increased online activity increases potential for scammers to get access to personal data that they can exploit to perpetrate APP scams.

[14] Action Fraud UK, Action Fraud warning after serious rise in CEO fraud: http://www.actionfraud.police.uk/news/action-fraud-warning-after-serious-rise-in-ceo-fraud-feb16
[15] Scam warning for small businesses, Cifas: https://www.cifas.org.uk/Scam_warning_for_small_businesses

3.60 Increased APP scams may also be a by-product of improvements in the payment systems – the growth of near real-time payments has made it easier for scammers to acquire and disburse the proceeds of scams more quickly, and improvements in security against other types of payment fraud mean that the consumers themselves are increasingly seen as the weakest link in the payment chain.

3.61 The available evidence suggests that APP scams where the victim makes a payment to the intended person who subsequently turned out to be a scammer are more common than scams where the victim is duped into making a payment to the wrong account. The former appear to make up between 85% and 95% of total APP scams by volume, although the average value of such scams tends to be smaller.

4 Consumer safeguards against APP scams – current laws and regulation

PSPs are not liable for APP scams since APPs are payments that the customer has authorised (that is, the customers have given their consent for the payments for the purpose of the Payment Services Regulations 2009). A PSP is under a strict obligation to comply with its customer's mandate, which means there are legal limits to what it can do when faced with a customer who is determined to authorise a payment.

In terms of payments' liability, the principal distinction in law is between authorised and unauthorised payments – not push and pull payments. The liability regime for push and pull payments is, for the most part, the same. The protection regimes for specific types of pull payments, such as card payments and direct debits, cannot necessarily be mapped directly onto online push payments.

4.1 The super-complaint made by Which? makes two proposals as to liability for APP scams:

- Under option A, Which? proposes that there should be a change in the law making PSPs liable to reimburse a payer, who is a consumer, when an APP scam has been made to a scammer, other than where a consumer has acted fraudulently or negligently. Which? does not specify which PSP (either sending or receiving) should be liable under option A.

- Under option B, Which? proposes that risk management standards should be introduced. PSPs would then be liable in cases of APP scams if they failed to comply with those standards.

4.2 Before forming a view on those proposals, it is important to establish what the current legal framework for APP scams is. In this chapter, we therefore briefly set out PSPs' obligations to prevent fraud, before considering the current liability regime for APP scams and how it compares to other types of payments.

PSPs' obligation to prevent fraud

4.3 Both sending and receiving PSPs are under a range of legal and regulatory obligations designed to prevent fraud (see further Annex 4). For example, under law:

- The Money Laundering Regulations 2007 require PSPs to conduct due diligence at certain points (for example, account opening), to maintain appropriate records and to implement policies, procedures and training, with the aim of avoiding the facilitation of money laundering.

- The Proceeds of Crime Act 2002 requires PSPs to report financial crime in certain circumstances.

- The Payment Services Regulations 2009 impose a number of obligations on PSPs concerning the safe use of so-called 'payment instruments'.

- Under common law, a PSP is obliged not to exercise a payment instruction where it is on notice that its customer's agent is attempting to misappropriate funds.

4.4 In terms of regulatory obligations, those PSPs that come under the FCA's Handbook[16], such as banks and building societies, are obliged to have adequate policies and procedures to counter the risk that they might be used for financial crime, including fraud.[17] The same PSPs must also ensure that money laundering is taken into account in their day-to-day operations, including in their decisions as to whether to develop new products and take on new customers.[18]

Complying with a customer's mandate

4.5 To understand the current model of liability for APP scams, it is important to set these types of payments in the context of both the sending and receiving PSPs' wider obligations. PSPs are expected to comply strictly with their customers' payment orders to the extent that they comply with the agreement that authorises the PSP to make payments upon instruction ('the mandate'). Indeed, **a PSP's principal duty is to obey its customer's mandate**.[19] This position has long been recognised under the common law.[20] The consequences of this are that a sending PSP cannot debit its customers' accounts where it acts outside the mandate and, on the other hand, will be liable in damages for failing to comply with a validly executed payment order.

4.6 Indeed, under legislation, PSPs now have time frames within which they must comply with a payment instruction made in accordance with the mandate. Under the **Payment Services Regulations 2009** (PSRs 2009),[21] which implemented the Payment Services Directive,[22] the general rule is that the sending PSP must ensure that it has credited the receiving account by the end of the next business day after it received the instruction.[23] This means the PSP would have to reinstate the customer's account to the position it would have been in had the delay not occurred.[24]

4.7 A sending PSP's duty to comply with an instruction that accords with its customer's mandate is subject only to limited exceptions.

- First, a sending PSP should not comply with a customer's payment instruction where it is on notice that an agent acting for the customer (such as a company's director) is misusing its authority in order to misappropriate funds.[25]

- Second, a sending PSP should not comply with a customer's payment instruction where the sending PSP knows or suspects that a customer is engaged in money laundering under the Proceeds of Crime Act 2002 (POCA 2002). The PSP must instead disclose its suspicions to the National Crime Agency[26] and seek that organisation's consent[27] to take further action.

[16] The SYSC provisions of the FCA Handbook do not apply to all PSPs. Before the SYSC obligations apply, a PSP must be a firm with a Part 4A permission (e.g. a deposit taker).
[17] FCA Handbook, SYSC 6.1.1R.
[18] FCA Handbook, SYSC 6.3. See also the FCA's guidance entitled 'Financial Crime: A Guide for Firms', which offers practical assistance and information on money laundering prevention for PSPs.
[19] *Paget's Law of Banking,* 14th Ed., 2014: paragraph 22.51.
[20] See *Bank of New South Wales v Laing* [1954] AC 135 (subject to the requirement that the account is in credit).
[21] SI 2009/209 and amended by SI 2009/2475 and by the Payment Services Regulations 2012 SI 2012/1791.
[22] 2007/64/EC.
[23] PSRs 2009, Regulation 70.
[24] PSRs 2009, Regulation 75.
[25] *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363, per Steyn J at 3783B-J; *Lipkin Gorman v Karpnale Ltd* [1992] 4 All ER 409.
[26] POCA 2002, Section 338.
[27] POCA 2002, Section 335.

4.8 In the context of APP scams, since the customer has authorised the payment, the sending PSP's ability to prevent fraud is limited by its duty to comply with the mandate. While the sending PSP can try to dissuade a customer from making the payment in question, or notify him or her of the risks of doing so, in the end it is obliged to comply with the authorised instruction and will be liable for failing to do so. A sending PSP therefore has limited options when faced with a customer that is determined to make a payment.

Liability for payments: authorised vs. unauthorised payments

4.9 Liability for payment services is governed by the PSRs 2009.[28] While the Which? Super-complaint draws the distinction between liability for push and pull payments, the PSRs 2009 do not. Instead, in terms of liability, the principal distinction in the Regulations is between authorised and unauthorised payments.

4.10 Under the PSRs 2009, a payment will be treated as **authorised if a customer has given his or her consent** for its execution.[29] For the purposes of the payment legislation, a customer will be regarded as having consented to a transaction even where he or she was tricked into making a payment to a scammer. The fraudulent behaviour of the scammer does not mean the payment is unauthorised; it means the customer can challenge its validity upon discovery of the fraud.

4.11 Consent can be withdrawn any time until the payment order becomes irrevocable, in which case any subsequent payment would then be unauthorised.[30] Push payments become irrevocable once they have been received by the sending PSP.[31] If there is any dispute as to whether a payment was authorised, the burden of proof lies with the PSP involved in the dispute.[32] It must show evidence that the payment was authenticated in accordance with its agreement with the customer.

4.12 Under the PSRs 2009, **PSPs will generally be liable for unauthorised payments.** Unauthorised payments can include those made in error by the PSP and those made fraudulently without the payer's consent. More specifically:

- A PSP which executes an unauthorised payment is generally obliged to immediately provide the customer with a refund for the full amount and, if applicable, restore the customer's account to the state it would have been if the unauthorised transaction had not taken place.[33]

- A customer who made a payment will only be liable for an unauthorised payment:

    - Where he or she **acted fraudulently**, in which case the customer will be liable for all related losses.[34]

    - Where he or she **failed, with intent or gross negligence**, to comply with his or her obligations in relation to a payment instrument.[35] This may be the case if, with intent or gross negligence, the customer did not comply with the contractual terms and conditions or failed to notify the PSP that his or her card had been stolen.

[28] Payment Services Regulations 2009, above. SI 2009/209 and amended by SI 2009/2475 and by the Payment Services Regulations 2012 SI 2012/1791.
[29] PSRs 2009, Regulation 55(1).
[30] PSRs 2009, Regulation 55(3).
[31] PSRs 2009, Regulation 67(1), read in conjunction with Regulation 65.
[32] PSRs 2009, Regulation 60.
[33] PSRs 2009, Regulation 61.
[34] PSRs 2009, Regulation 62(2)(a).
[35] See Annex 4 for the customer's obligations to prevent fraud.

- A customer will also carry the financial burden for losses up to the point where he or she notified the PSP of the loss or theft of a payment instrument.[36]

- Where a customer's losses arise from a lost or stolen payment instrument, he or she will only have the bear the loss for the first £50, even if there was a failure to keep the payment instrument (for example, a card) safe.[37] The customer will not be liable for the first £50 if it notified the bank of the missing card before any losses were incurred.

4.13 **Where a PSP that executes a payment can establish that the payment was authorised, however, it will not be liable for the customer's losses** even if it transpires that the money was paid to a scammer. The losses will instead lie with the customer. This reflects the limited ability of the sending PSP to prevent an authorised payment because of its duty to comply with the mandate.

4.14 The Which? super-complaint raises the fact that, as it stands, the sending PSP does not **verify the payee's name** that is entered by the customer and will instead rely only on the account number and sort code to execute the payment. It suggests that since the payee's name is usually a required field for a payment, customers expect that the sending PSPs will check this information.[38] This issue was raised by other parties during our investigation. However, under the PSRs 2009, the sending PSP is only required to execute a payment in accordance with the 'unique identifier' provided by the customer.[39] Since the unique identifier need only identify the payee's account (and not his or her name),[40] a payment will be correctly executed if it matches the sort code and account number provided. The PSRs 2009 make it clear that this is the case even if additional information, such as the payee name, has been provided.[41]

4.15 The courts have refused to impose liability where a PSP has not verified the payee's name, for payments made under particular scheme rules, as long as the PSP has complied with standard banking practice. For example, in the case of *Tidal Energy Ltd v Bank of Scotland plc*[42], a company was scammed into transferring funds. It was given account details that it thought belonged to its supplier, but had in fact been switched for those of the fraudster (an example of a 'maliciously misdirected' payment). As a result, the payee name entered by the customer did not match the actual name on the account held by the receiving PSP. In accordance with the CHAPS clearing house rules, the sending PSP had checked the account number and sort code, but not the name. The court held that the sending PSP was not required to compensate the company for any resulting loss. The company was taken to have contracted with the sending PSP on the basis of the CHAPS rules, which represented standard practice, and could not therefore expect the sending PSP to verify the payee name. The courts have similarly confirmed that a receiving PSP does not owe any obligation to a non-customer payer to verify payee details.[43]

4.16 The position under the PSRs 2009, reinforced by the courts, is therefore that neither the sending nor receiving PSP will be liable for losses stemming from APP scams. However, there remains one possible route by which a PSP may yet find itself incurring liability for such payments. The Financial Services and Markets Act 2000 (FSMA 2000) provides for a dispute resolution scheme administered by the **Financial Ombudsman Service**.[44] The ombudsman service can consider all disputes arising from the carrying out of regulated activities or payment

[36] PSRs 2009, Regulation 57(1)(b).
[37] PSRs 2009, Regulation 62(1).
[38] Which? Super-complaint, page 9.
[39] PSRs 2009, Regulation 74.
[40] PSRs 2009, Regulation 2.
[41] PSRs 2009, Regulation 74(3).
[42] [2014] EWCA Civ 1107; [2015] 2 All ER 15.
[43] *Abou-Rahmah v Abacha* [2005] EWHC 2552 (QB); [2006] 1 All ER (Comm) 247.
[44] FSMA 2000, Section 225.

services.[45] The ombudsman service is not bound by the same rules of evidence as the courts and, while it is required to have regard to the law, it is not bound to follow it.[46] Instead, it is able to make its determination based on what it considers to be 'fair and reasonable' in all the circumstances.[47]

4.17 The ombudsman service has the power to make an award of monetary compensation if it sees fit. To take a complaint to the ombudsman service, an individual can be a customer of the PSP or a 'payment service user' of the PSP.[48] In cases of APP scams:

- The ombudsman service has previously held a receiving bank liable where it credited a transfer to its customer's account, and allowed the customer to transfer substantial sums out of that account, despite having identified a different transfer into the account as a security risk.[49]

- The ombudsman service has indicated that a payer cannot, however, bring a case against receiving PSP for alleged failures in account opening and closing. Where there is no banker-customer relationship, such failures are not considered to be sufficiently connected to the underlying payment that gives rise to the 'payment service user' relationship.[50]

4.18 Beyond the ombudsman service regime, however, neither the sending nor receiving PSP will be obliged to compensate customers for losses arising from APP scams.

Varying liability for pull payments: protection for card payment and direct debits

4.19 The Which? super-complaint suggests that the liability position for APP scams is different to the position for pull payments. In particular, it suggests that there is greater protection for consumers in the following situations:[51]

- First, where a scammer obtains a consumer's account (for example, card) details fraudulently and pulls unauthorised funds from his or her account.

- Second, where a consumer authorises a payee to pull funds, but the payee pulls more funds than agreed.

- Third, where a consumer authorises a scammer to pull funds but later discovers that the expected product or service did not materialise because it was a scam.

- Fourth, where a consumer makes a card payment, he or she may be protected by the '**chargeback rules**'.

- Fifth, where a consumer pays by direct debits, protection may arise from the **direct debit guarantee**.

4.20 As discussed below, specific consumer protection mechanisms apply to card payments and direct debits. Those protections do not apply in cases of APP scams. At first sight, therefore, from the consumer perspective, the position of APP scams may appear out of line with other

[45] FSMA 2000, Section 226. See FCA Handbook DISP 2.7 for the eligibility requirements for bringing a complaint.
[46] *R (IFG Financial Services Ltd) v Financial Ombudsman Service Ltd* [2005] EWHC 1153 (Admin); [2006] 1 BCLC 534.
[47] FSMA 2000, Section 228. FCA Handbook, DISP 3.6.1
[48] FCA Handbook, DISP 2.7.6R01/10/201.
[49] See FOS Decision of ombudsman Niall Taylor, dated 20 November 2012.
[50] See FOS Decision reference DRN2671069, 28 June 2016: www.ombudsman-decisions.org.uk/viewPDF.aspx?FileID=120924
[51] Which? Super-complaint, paragraph 2.1.

payment types. The consumer's primary concern is after all likely to be whether he or she recovers the lost sums, and not the intricacies of the mechanism by which that is done. However, the examples above require further consideration.

4.21 The legislation does not distinguish between push and pull payments, but rather between authorised and non-authorised payments. Notably, the first bullet point above is an example of an unauthorised payment. On the assumption that the customer was neither fraudulent nor grossly negligent, he or she would receive a refund regardless of whether the transaction involved a push or pull payment.

4.22 There is one very limited circumstance where the PSRs 2009 afford protection to pull payments specifically. A PSP will have to refund a pull payment where an exact amount is not specified in the payment instruction and the sums taken are greater than could reasonably be expected by the customer in light of the conditions of his or her contract with the PSP and the circumstances of the case.[52] This appears to be the situation referred to in the second bullet point above, and is colloquially known as the '**mini bar exception'**. It is said to be primarily aimed at preventing direct debit instruction abuse, and reflects the fact that the nature of the payment means that the payment amount is not clear at the outset. This is different from an APP scam, where the customer has specified the exact sum to be transferred.

4.23 Bullet points three to five appear to refer to the additional consumer protection associated with certain specific types of pull payments. This protection, however, stems from the particular nature of those transactions and the relationships they involve, and not from the fact that they are pull payments. The particular examples given by Which? are discussed below.

Card payments

4.24 The third example highlighted above is likely to refer to card payments, where they are covered by the **Consumer Credit Act (CCA) 1974, Section 75** (that is, credit card transactions between £100 and £30,000). Under that provision, a credit-card issuer is jointly and severally liable for a breach of contract or misrepresentation of a retailer or trader. This could potentially include fraudulent misrepresentations, as may be the case where goods purchased simply do not arrive.

4.25 However, the liability regime for APP scams and the consumer protection offered to card payments under the CCA 1974 are distinguishable for a number of reasons.

- Under the CCA 1974, the credit-card issuer is liable where it has an arrangement with the supplier of the goods or services.
- The supplier or merchant that receives payments can be required to provide an indemnity to their card acquirer.[53]
- Though there may be occasions when an acquirer cannot recover funds, recovery is far more likely than in cases of APP scams. In general, the acquirer will be seeking a refund from an established business, rather than a scammer (the latter of which will inevitably try to avoid detection).

4.26 Similar arguments also arise when considering any comparison between the liability models for APP scams and the **chargeback rules**. The chargeback process is not enshrined in law, but is part of the card scheme rules that issuers and acquirers sign up to. Where a customer makes a payment for goods or services using either a credit or debit card, he or she may be able to use

[52] PSRs 2009, Regulation 63.
[53] CCA 1974, Section 75(2).

the interbank chargeback rules to reverse a payment in certain circumstances.[54] The chargeback process can be used in a number of situations, including where goods purchased are never actually delivered. The PSP will temporarily credit the customer's account. However, he or she will not be entitled to keep that money if there is sufficient evidence to refute the claim (for example, evidence that the goods were in fact delivered). In such a scenario, the money will be credited to the seller's account.

4.27 Importantly, the liability regime for APP scams and the chargeback process differ in two ways:

- The chargeback rules do not say anything about the liability of issuers and acquirers. The rules do not impose liability on either PSP (sending or receiving). The initial credit to the customer's account is temporary, and funds to cover chargeback claims are generally held back by acquirers from the funds owed to the supplier. Under the chargeback rules there is no guarantee that the issuing bank will be able to recover money through the chargeback or that the trader will accept that the customer is entitled to a refund.

- The chargeback rules are best described as a dispute resolution mechanism between schemes' participants. Liability for payments is enshrined in laws which are applicable to push and pull payments – for example, the Payment Services Regulations 2009.

4.28 Overall, the consumer protection mechanisms for card payments cannot be mapped directly on to the liability model for APPs. This would not account for the differences between those payment methods.

Direct debits

4.29 Which? also suggests that the lack of protection for APP scams is notable when compared to the protection afforded by the **Direct Debit Guarantee** (DDG) The direct debit scheme, administered by Bacs, is a payment mechanism that enables one-off or regular payments to be made to suppliers under contract, by letting a supplier issue a direct demand for payment to the consumer's bank.

4.30 Once again, however, the enhanced consumer protection that exists for direct debits has to be viewed in the wider context of how that payment method operates. Suppliers and firms that want to collect payments via direct debit must be sponsored by a bank to do so. In practice, this means that:

- The DDG relies on a system of indemnities. While the payer's PSP will refund a customer where it is satisfied that he or she has a valid claim, it will then seek to recover those sums from the payee's PSP, which in turn would seek to recover it from the seller or supplier. In order to be sponsored for the direct debit scheme, a firm or supplier will have to provide an indemnity to its sponsoring PSP (the originator bank) for losses attributable to it and offer collaterals. The payer's PSP will therefore usually recover the money it has paid to the consumer under the DDG and will not normally itself shoulder the financial burden. A PSP will only be liable for any losses where they are due to its own acts or omissions.

- All organisations that are able to issue direct debit demands go through a careful vetting process. Such a process requires an established relationship between the PSP and the supplier. In this way, it can be distinguished from payments made via FPS, for which the recipient need only have a bank account with a 'FPS participant bank' (although of course PSPs remain under a range of obligations when opening bank accounts).

[54] The chargeback rules apply to all purchases made by a debit card, though the rules may vary between the Visa, Maestro and American Express providers. For credit cards, the chargeback rules are often of particular value for transactions under £100, where the CCA 1974 will not apply.

4.31 In any event, even under the DDG, it is unlikely that a consumer would receive a refund in a situation comparable to an APP scam, where he or she had authorised all the details of the payment in question. Under the DDG, a consumer is entitled to a full and immediate refund from his or her PSP where the supplier has not complied with the scheme rules or where he or she did not authorise the direct debit in question (for example, where a scammer has acquired the details of his or her account). However, the DDG does not cover payments that customers have been fraudulently induced into authorising, so long as they have been correctly processed by the PSP in accordance with the details provided by the supplier.

Summary on push payment protection

4.32 Overall, in terms of liability for payments, the key distinction in the payments legislation is between authorised and unauthorised payments (not push and pull payments). While the Which? super-complaint is correct that certain types of pull payments have their own consumer protection rules and that those protections may be very important from a customer perspective, this protection must be seen in context. There are features of APPs that distinguish them from the pull payments in question and suggest significant caution should be exercised before considering a transposition of the consumer protection rules from one payment method to another. The implication of this is not that it would be impossible to have greater consumer protection for push payments. Instead, what it means is that further consideration is needed to determine whether and to what extent consumer protection by way of scheme rules would be effective and workable for APP.

5 Consumer safeguards against APP scams – current role of PSPs and payment systems

The available evidence suggests that current legal obligations and commercial incentives already mean that the sending bank's interests are broadly aligned with those of the consumer. While specific practices vary, in general sending PSPs appear to have developed reasonably extensive measures to help prevent their customers from falling victim to APP scams. We also observe that sending PSPs generally appear to make reasonable efforts to assist their customers in recovering funds they have transferred as a result of an APP scam. In some instances we observe sending PSPs voluntarily refunding victims for the funds lost as the result of a scam. We do note, however, the recent findings of the Financial Ombudsman Service that sending PSPs could do more to engage with victims of scams in a more sympathetic and timely fashion.

The commercial incentives and obligations for receiving PSPs to ensure there are appropriate safeguards in place to protect customers of other PSPs that fall victim to APP scams are weaker than for sending PSPs. We have identified evidence of inconsistent practices among receiving banks in terms of steps taken to help prevent funds obtained as the result of scams being credited to accounts held by their customers. We also have identified indicative evidence that some PSPs may be more effective than others in preventing their accounts being opened by scammers or otherwise falling under the influence of scammers.

We have identified evidence that, in some instances, sending and receiving PSPs have problems engaging with each other in an effective and timely manner when attempting to recover payments made as the result of an APP scam. These difficulties may manifest themselves in a number of ways, including: unavailability of specialist fraud response teams at some receiving PSPs, 24 hours a day, seven days a week; inconsistent approaches to sharing information to assist in the recovery of funds; inconsistent approaches to 'freezing' alleged scammers' accounts to prevent the onward transfer of funds that may have been obtained as the result of a scam; and difficulties in agreeing indemnities to allow receiving PSPs to release funds remaining in accounts of alleged scammers.

The payment system operators involved in push payments currently have no involvement in managing how APP scams are prevented or managed. Operators of other payment systems, such as Mastercard and Visa, are more involved in setting out processes for managing instances of fraud.

5.1 In this chapter we discuss the safeguards against APP scams that consumers receive from the steps taken by PSPs and payment system operators (PSOs), including the obligations on these organisations. In setting out our observations on the current practices of PSPs, we distinguish between the sending PSP (the PSP acting on behalf of the victim) and the receiving PSP (the PSP acting on behalf of the scammer). We also distinguish between practices aimed at preventing APP scams in the first instance and practices PSPs follow in responding and recovering funds when APP scams are reported.

5.2 Our discussion examines:

- the role of the sending PSP
- the role of the receiving PSP
- the interaction between sending and receiving PSPs when APP scams are reported
- the role of PSOs

The role of the sending PSP

Actions taken to prevent APP scams

5.3 We have observed a significant amount of evidence that, while specific practices of individual PSPs vary, in general PSPs appear to make significant efforts to prevent their customers falling victim to APP scams.

5.4 These actions can be grouped under the following broad headings:

- Transaction monitoring, customer profiling and challenge of suspicious transactions.
- Checks, prompts and limits on functionality when initiating push payments.
- Specialised staff training to help identify and prevent APP scams.
- Education and awareness campaigns.
- Work with government and industry on other initiatives.

Transaction monitoring, customer profiling and challenge of suspicious transactions

5.5 We have seen evidence that PSPs regularly monitor outbound push payments made by their customers for suspicious patterns of activity. These systems rely on a number of different data sources to help identify and flag potentially fraudulent payments, including payments that may be related to an APP scam.

5.6 Monitoring payments to identify APP scams is relatively complicated when compared with other types of fraud. This is because in an APP scam the customer has authorised the payment themselves, which means some of the usual warning signs may not be raised.

5.7 Some PSPs have told us they augment their transaction monitoring processes with customer profiling to help identify customers that may be particularly at risk of falling victim to fraud and APP scams. Profiling may be based on customers that have fallen victim to a scam in the past, or using other factors that may increase the likelihood of particular groups of customers falling victim to scams.

5.8 When suspicious push payments have been identified, PSPs will in many instances temporarily suspend the payment and then seek to make contact with their customer to ensure the payment is indeed legitimate. We have been told that is not uncommon for PSPs to communicate to the customer their suspicion that a payment may be related to a scam, only for the customer to request the PSP to proceed with the payment. In some instances, we understand scammers will deliberately coach the victim of a scam to override these challenges

from the victim's PSP. As PSPs are legally required to follow their customer's mandate, there are limits on the further action they are able to take at this point.

5.9 Some PSPs have provided us with evidence that significant volumes of attempted scams are prevented through the interventions they make in challenging their customers over suspicious payments.

5.10 We note that, with regard to transaction monitoring, there is a need to balance the sensitivity of processes that identify potentially suspicious payments with the inconvenience caused to customers making legitimate payments that are falsely flagged as suspicious and suspended pending confirmation. This is particularly true given the overwhelming majority of push payments do not involve fraud of any type.

Checks, prompts and limits on functionality when initiating push payments

5.11 We have observed a range of different checks, prompts and limits on functionality that PSPs have variously implemented to help prevent customers make push payments as part of an APP scam. A non-exhaustive list of these steps includes:

- Presenting customers with prompts and warnings about the risks of scams, when using internet and telephone banking, where payments are made to first-time payees.
- Limiting the channels through which payments to new payees can be made and requiring additional authentication steps to make payments to new payees. These steps all make it more difficult to make payments to first-time payees, as is likely to be the case of a payment to a scammer.
- Presenting customers with the name of the sending PSP. This look-up functionality is based upon the sort code a payer provides, which is unique to individual PSPs. This may help a customer become alert to a scam if the account is held at a PSP other than they were expecting.
- Undertaking additional checks, confirmation steps or customer challenge for payments over certain values.
- Providing customers with lists of pre-populated common beneficiaries for payments using internet banking, such as utility companies.

Specialised staff training to help identify and prevent APP scams

5.12 Several PSPs told us they provide customer-facing staff with specialised training to help identify customers that may be about to fall victim to an APP scam, and the steps they should take to help prevent the customer from doing so.

Education and awareness campaigns

5.13 There is significant evidence that PSPs fund and run campaigns to educate the public against the risks of fraud, including APP scams. This takes the form of both industry initiatives and, in some cases, individual PSPs taking action.

5.14 Recent collaborative examples that the industry has been involved in include the 'Take Five' awareness campaign that aims to provide impartial advice to consumers and businesses to protect them from preventable financial fraud; the 'Out of Your Hands' initiative that provides a teaching resource which features examples of typical scams and guidance on how online payment scams can be avoided; 'Get safe online' website providing advice to individuals and businesses on how to protect themselves and their devices from fraud, identity theft, viruses

and other online problems; and the 'Hang Up on Fraud' initiative launched in 2014 to educate the public on how to avoid telephone scams. Examples of initiatives individual banks have sponsored to educate the public include the 'Think Jessica' campaign supported by Lloyds Banking Group and other bodies and 'Friends against scams' joint initiative between NatWest and National Trading Standards.

5.15 Customer education initiatives are not confined to the efforts of PSPs, with government and regulators also undertaking similar programs. Cyber Aware (previously Cyber Streetwise) is a cross-government (Home Office, Department of Culture, Media and Sport and the National Cyber Security Centre) awareness and behaviour change initiative that aims to encourage businesses and individuals to adopt simple steps to protect themselves from cyber-crime. The FCA's ScamSmart initiative aims to provide advice to the general public on how to avoid investment scams. The ScamSmart web tool provides guidance on various types of investments, enables people to search a list of known scammers or firms operating without authorisation and provides advice on how people can check that firms offering investment opportunities are legitimate.

5.16 The majority of stakeholders are in favour of these initiatives, whether funded by the banks or other parties. However, some stakeholders told us that there is little evidence that financial campaigns and consumer education are effective. It was also observed that customer education efforts can have a limited reach, and may not be reaching the groups who are at risk of being targeted by a particular type of fraud. Moreover, customers who fall victim to scams are often put in stressful situations and consequently may not apply the lessons of such education when it is actually needed.

5.17 Current incentives banks have to educate consumers against the risks of fraud include a desire to maintain confidence in the banking system, the fact that for some financial crime the banks are already liable, and the possibility that there may be competitive advantage to be had from demonstrating to customers that they take financial crime seriously.

Work with government and industry on other initiatives

5.18 We also note that PSPs frequently work with the government, regulators, law enforcement and trade bodies on wider initiatives aimed at preventing fraud, including APP scams. Recent examples include the work of PSPs with the Home Office led Joint Fraud Taskforce and the involvement of PSPs on the Payments Strategy Forum initiatives related to financial crime. We discuss this work further in Chapter 7.

Actions taken when responding to reports of APP scams

5.19 While specific practices of PSPs vary, at a high level when a customer reports to their PSP that they have made a payment as a result of an APP scam:

- the sending PSP will collect information from the customer to enable them to investigate the matter further and to confirm that the claim is genuine
- the sending PSP will then contact the receiving PSP and attempt to recover the payment on behalf of their customer
- where it is not possible to recover the payment (perhaps because the funds are already gone from the account held with the receiving PSP), in some circumstances the sending PSP may choose to provide a voluntary reimbursement to the customer

5.20 We discuss our observations with regard to the interaction between sending and receiving PSPs when APP scams are reported below. In the remainder of this section, we discuss how PSPs respond to customers' reports of APP scams and approaches to providing reimbursement when funds cannot be recovered.

Sending PSP interactions with customers reporting APP scams

5.21 We have seen some evidence that the manner in which sending PSPs respond to and manage reports of APP scams from their customers could be better. Specifically:

- We note one of the conclusions of the Financial Ombudsman Service's 2015 report into telephone fraud was that the way in which some PSPs responded to reports of fraud from customers made the situation more stressful and difficult, in particular due to delays in communication and the tone taken in communications.[55]

- In the evidence Which? collected through its online scam reporting tool and provided to us, poor responses from PSPs to reported APP scams were identified as an issue. Concerns focused mainly on the slow speed of investigation and poor levels of communication.

5.22 We emphasise the importance of PSPs engaging with victims of APP scams in a timely, compassionate and proactive manner. We understand some work is already under way in addressing how PSPs respond to victims of APP scams (which we discuss in Chapter 7). Further, we consider some of the frustrations and delays may be being caused by difficulties sending PSPs have in engaging with receiving PSPs when responding to APP scams (as is discussed further below).

Voluntary reimbursement of APP scam victims

5.23 As we have set out above, under current UK law, liability for APP scams sits with the paying customer. However, evidence we have gathered indicates that, under certain circumstances, PSPs do choose to provide voluntary, goodwill reimbursement to some victims of APP scams when recovery of funds from the receiving PSP has not been possible.

5.24 [✂]

5.25 Although we have not been able to collect conclusive data, we have seen anecdotal evidence that some sending PSPs may be more inclined than others to provide voluntary reimbursement to victims of APP scams.

Summary of role of sending PSP

5.26 While specific practices vary, in general PSPs appear to have developed reasonably extensive measures to help prevent their customers from falling victim to APP scams. Sending PSPs also generally appear to make reasonable efforts to help their customers in recovering money they have lost in an APP scam. We do note, however, the recent findings of the ombudsman service that sending PSPs could engage with scam victims more quickly and sympathetically.[56] In some instances we observe sending PSPs voluntarily refunding victims of APP scams.

[55] FOS (2015) *Calling time on telephone fraud*. http://www.financial-ombudsman.org.uk/assets/pdf/vishing-insight-report2015.pdf
[56] Financial Ombudsman Service, *Calling time on telephone fraud* (2015): www.financial-ombudsman.org.uk/assets/pdf/vishing-insight-report2015.pdf

5.27 We take our observations on sending PSPs' behaviour as evidence that their obligations and commercial incentives are generally relatively well aligned with those of their customers. It is in PSPs' interest to protect their customers from becoming victims of APP scams. Victims may lose confidence in their current PSP and stop using some of their services, or may take their business to another PSP altogether. Almost all of the checks to stop APP scams that a sending PSP might undertake will also help with detecting unauthorised payment frauds, where the PSP is liable. The PSP also has to be alive to the possibility that their customer may take a case to the ombudsman service if it has lost money to an APP scam.

The role of the receiving PSP

Actions taken to prevent APP scams

5.28 There are two main ways in which the activities of receiving PSPs can help prevent APP scams:

- Monitoring of inbound payment activity to identify activity potentially related to APP scams.
- Preventing payment accounts falling under the control of scammers.

Monitoring of inbound payment activity

5.29 APP scams can be prevented by receiving PSPs monitoring inbound payments and intervening where they identify suspect transactions.

5.30 The evidence we have collected indicates that, while receiving PSPs do monitor inbound payment activity, such monitoring is focused primarily on the prevention of money laundering, rather than identifying payments related to APP scams. This in part reflects the need for PSPs to comply with the requirements of the Proceeds of Crime Act 2002, the Money Laundering Regulations and related legislation. We understand that while transaction monitoring for anti-money laundering purposes may help identify payments related to scams, it is not specifically designed to do so.

5.31 However, some PSPs told us that they do additional monitoring of inbound payments to help identify trends that may be suggestive of fraud, including APP scams. We understand that such monitoring is typically done on a retrospective, non-real-time basis. Given that funds obtained through scams are commonly moved on very quickly, this delay may limit the efficacy of monitoring in aiding recovery of funds.

5.32 We have seen evidence of some PSPs monitoring outbound account activity to identify trends that are suggestive of an account being used by a scammer. This is seen, for example, for large and repeated withdrawals of cash.

5.33 We consider that receiving PSPs may potentially be able to do more in terms of proactively monitoring inbound payment activity to help prevent APP scams. We do note both the potential challenges of doing so and the risk of disruption to non-fraudulent payments. We are also aware that, under the FCA Handbook, certain PSPs (including banks) are under a general obligation to have adequate policies and procedures to counter the risk that they are used for financial crime,[57] and cases can be taken to the ombudsman service against receiving banks in some circumstances (discussed above, in Chapter 4).

[57] FCA Handbook, SYSC 6.1.1R.

5.34 However, we are concerned that, compared to the steps taken by sending PSPs, the measures taken by receiving PSPs to prevent customers of other PSPs falling victim to APP scams appear to be more modest. In part, this may reflect the reduced commercial incentives – as a receiving PSP, the victim of an APP scam is the customer of another PSP, so the receiving PSP does not face the prospect of losing that customer.

Preventing payment accounts falling under the control of scammers

5.35 Every fraud, including APP scams, that uses the payment system involves the fraudster having access to a bank account where they receive the funds. There are a number of ways that this might be achieved: the fraudster may have opened a bank account (possibly fraudulently); the fraudster may have identified people who are willing to act as 'mule accounts', receiving and sending on payments on behalf of the fraudster; or the fraudster may be able to hack into accounts that belong to other people, and consequently receive and make (albeit unauthorised) payments from the account.

5.36 An obvious question therefore is whether the PSPs are doing enough to stop fraudsters having access to the banking system. For unauthorised payments, the PSPs already have obligations that create incentives to stop such activities given they are liable to reimburse customers who lose money because of unauthorised payments from their account.

5.37 For the other scenarios (fraudulently opened accounts and mule accounts), the PSPs' obligations to stop such accounts operating tend to come from financial crime obligations rather than from the specific risk that they will have to reimburse other PSPs or customers because of fraudulent payments made into such accounts. Receiving PSPs do not usually provide redress to victims, except in some instances where the PSP had already identified that the account might be receiving suspicious payments.

5.38 To stop fraudsters opening accounts, PSPs mentioned several ways they vet new applications. Following a risk-based approach, PSPs are required to undertake customer due diligence checks, although the extent of these measures may vary between PSPs depending on the risk that they assess from their business. This means that some PSPs may go beyond the standard identification measures set out by the Joint Money Laundering Steering Group. These checks include verifying the customer's identity and the purpose and intended use of the account.

5.39 When vetting new applications PSPs will use a mix of internal systems and intelligence sharing systems. PSPs reported checking applications against the attributes of known beneficiary fraudsters. One PSP told us that it would make a detailed manual review of applications where there is evidence of the customer having previously been associated with fraud, or where there is a high risk of the customer committing fraud. If there is sufficient concern of a fraud risk, the PSP will decline the application.

5.40 Increasing the obligations for PSPs to do more checks before opening accounts could affect other policy goals. For example, it could conflict with efforts to increase competition in retail banking if it increases the barriers to switching bank and opening a new bank account. It is also possible that additional checks will deter some of those that are currently unbanked from opening an account. The problems faced by groups denied access to the banking system is something that policymakers, including the FCA, are keen to address.[58]

5.41 Since PSPs face ongoing duties to prevent financial crime,[59] the need to conduct customer due diligence checks does not end once the account is open. An account that passed all the appropriate checks when it was opened may be used for fraudulent purposes at a later date.

[58] See FCA Occasional paper no 17, *Access to Financial Services in the UK* (2016): https://www.fca.org.uk/publications/occasional-papers/occasional-paper-no-17-access-financial-services-uk
[59] FCA Handbook, SYSC 6.3.1 and 6.3.3. See further Annex 4.

PSPs can use external data sources to flag anomalies for further investigation, similar to data available when deciding whether to open a new account. Cifas indicated that not all PSPs routinely consult its database to check if their customers' accounts have been used in the past to facilitate frauds as the Cifas system is mainly used for fraud prevention purposes at the point of application. Some PSPs only use the database when making checks before lending money to an account holder, a situation where the PSP would stand to lose money if the account is being used by a fraudster.

5.42 Such reviews cost the receiving PSP money, and investigations can also falsely flag up genuine customers. Moreover, mule accounts may only be used on a one-off basis, such that continual review of whether an account has been used to receive funds from an APP scam may not do much to reduce fraud.

5.43 PSPs can investigate flagged accounts, which can be closed. Some PSPs told us that they would close accounts that had received fraud-related funds. In this process, some funds may be moved to a suspense account pending identification of the true owner. One PSP told us that once it had repaid funds, it will move any other funds in the account to a suspense account for safeguarding against future claims by other PSPs or a satisfactory explanation by the customer.

5.44 We have observed some limited evidence that suggests some PSPs may be more likely to be the receiving PSP used by a scammer than their market shares would suggest. This could reflect differences in the effort and ability of these PSPs to stop fraudsters gaining access to bank accounts or in their abilities to detect suspicious payments, or may instead be an artefact of the limited evidence we have received on this matter. We do note that some stakeholders told us that they thought some PSPs were better than others at stopping fraudsters receiving funds at the bank. We are of the view that the evidence is not sufficiently robust to conclude definitively on this issue at this stage, but that further investigation is appropriate.

Actions taken when responding to reports of APP scams

5.45 While the specific steps taken by different PSPs vary, we understand that, in general, the processes followed by receiving PSPs when they receive a report from a sending PSP of a customer receiving a payment allegedly relating to an APP scam are:

- The receiving PSP will request information and evidence from the sending PSP about the nature of the alleged scam. They will then conduct further investigations themselves.

- If, following analysis of the information available, the receiving PSP determines its customer may have been the beneficiary of a scam, they will typically freeze the account to prevent funds from being withdrawn from the account. They may also mark the account as suspicious so that additional inbound payments are not credited to the account while the issue is under investigation.

- If any funds remain available in the account, the receiving PSP will return the disputed amount to the sending PSP for onward crediting to the victim. Before doing so, the receiving PSP will typically require the sending PSP to provide an indemnity to protect them from any subsequent civil action brought by the intended recipient of the funds (for example, in the case the alleged scammer turns out to have been wrongly accused). If no funds are available, perhaps because they have already been withdrawn or transferred to another PSP, generally no payment is made to the victim's PSP.

- The receiving PSP will then typically close the recipient account. Any funds remaining in the scammer's account will then usually be transferred to a suspense account. Details of the scammer may then be shared using the industry's intelligence sharing facilities. This aids in preventing the scammer from opening accounts at other PSPs for use in future scams.

5.46 In practice, there are significant additional complexities to the process set out above. An example includes multiple victims of a scammer making simultaneous claim to the funds in a scammer's account that are insufficient to reimburse all parties. Scammers may also use multiple accounts held at several different PSPs to receive and quickly disburse funds obtained from APP scams. Cases such as these require further investigation and involve multiple PSPs. Where there are insufficient funds to repay all victims, the PSPs typically apply specialist legal principles to determine claims to any remaining funds available. Inevitably, these complexities lengthen the time it takes for victims to receive any available reimbursement or to even gain closure on the matter at hand. Moreover, as noted in Chapter 6, one stakeholder has also suggested that there are currently legal barriers which, in its view, make it more difficult to repatriate funds.

5.47 Some receiving PSPs have told us that they will offer refunds to the sending PSP under certain circumstances even if the scammer has already withdrawn the underlying funds. Such circumstances include instances where the PSP had allowed disputed funds to be transferred after it has been alerted to a scam.

Summary of role of receiving PSPs

5.48 We have found evidence that receiving PSPs have varying approaches to preventing money from APP scams being credited to their customers' accounts. For example, the approaches taken to monitoring inbound transactions to identify payments related to scams vary between PSPs.

5.49 There is also some indicative evidence that some PSPs may be more effective than others in preventing scammers from opening or controlling accounts that are used for APP scams, or using them for scams in other ways.

5.50 Collectively, we take these observations as evidence that the commercial incentives and obligations for receiving PSPs to ensure there are appropriate safeguards in place to protect customers of other PSPs that fall victim to APP scams are weaker than for sending PSPs. As a result, we consider that there may be capacity for receiving PSPs to do more to help prevent and respond to APP scams. We further explore this in relation to how sending and receiving PSPs interact in response to reported APP scams.

Interaction between sending and receiving PSPs when APP scams are reported

5.51 As set out above, when a consumer reports a suspected instance of an APP scam to their sending PSP, the sending PSP will then engage with the receiving PSP to attempt to recover the funds in question.

5.52 Through the evidence we have received, we are concerned that the way in which sending and receiving PSPs interact may not be functioning as effectively as possible. Specific issues that we have identified include:

- Fraud specialists at a sending PSP being unable to communicate with the equivalent team at the receiving PSP, due to a lack of 24/7 availability. This slows the response to the reported scam, gives the scammer more time to disperse funds, and results in stressful delays for scams victims.

- A lack of a standardised and consistent approach between PSPs to facilitate the recovery of funds. Examples include PSPs adopting different approaches to 'freezing' accounts of alleged scammers and taking different approaches in agreeing indemnities to allow the

release back to victim PSPs of funds remaining in accounts of alleged scammers. This can also slow the response to the reported scam.

- A lack of common understanding between PSPs on the types of information that can be shared between parties to facilitate the investigation of an alleged scam. Concerns regarding what information can be legally shared under data protection laws are frequently cited. This can not only slow the response to the reported scam, but may even make it difficult to have an effective response at all.

5.53 With regard to this last point, we understand that the issue of what information can and cannot be shared under current legislation, and whether any changes to law may be appropriate, to enable effective prevention and response to financial crime is a wider issue in the industry. It has been suggested to us that some PSPs 'hide' behind the excuse of data protection to limit engagement on sharing information to combat financial crime. We explore the implications of data protection legislation with regard to sharing information to combat financial crime in the following chapter.

5.54 We consider there is scope for the way in which sending and receiving PSPs interact when responding to reported APP scams to improve. We acknowledge that scammers often very quickly move funds onto secondary PSPs to disburse and conceal the original source. This undoubtedly complicates the funds recovery process. We understand the technical and legal issues surrounding funds repatriation involving multiple tiers of PSPs is one of the issues that the Joint Fraud Taskforce is looking into (see Chapter 7). However, we are of the view that there is scope to improve over the short term the way in which the sending PSP and primary receiving PSP interact, to both increase the chance of recovering scammed funds and provide clarity to victims on the current status of their claim.

The role of payment system operators

5.55 Consumer APP scams are conducted via one of two payment systems: Faster Payments or CHAPS. The evidence we have seen suggests that the operators of these two systems have to date not been heavily involved in tackling the problem of APP scams. They do not have any rules, policies or procedures in place related to consumer protection against fraud or scams. The PSOs tend to view the issue as something that is between the customer and the PSPs. In their view, the PSP's role is to facilitate a payment. There are also no specific obligations on the PSOs with regard to addressing fraud perpetrated using their payment system.

5.56 There are examples of PSOs taking a role in facilitating a mechanism for their members to resolve problem transactions. For example:

- The operator of Faster Payments (FPSL) administers the Credit Payment Recovery Process ('CPR') in relation to Faster Payments and Bacs. The CPR is a process for paying back certain accidentally misdirected transactions made over Faster Payments or Bacs Direct Credits. The process defines payment in error as 'a payment that should not have been sent because at the time it was not made as intended by the customer'. As the administrator of the process, FPSL gives guidance from time to time when requested by participants on the detail of the CPR process and how to apply it.

- Bacs offers a guarantee for its direct debit service. The paying PSP is responsible for making any refunds immediately if an error is made in the payment of a direct debit. If the recipient has made the error then the paying PSP must raise an indemnity claim to obtain the money back. Direct debits cannot be collected into personal accounts, so there is a higher level of 'know your customer' (KYC) and ongoing account checks for direct debit payments. If a claim is approved the payer's PSP will refund its customer, and then use the indemnity process to automatically collect the refund from the recipient. If the recipient no longer exists, their sponsoring PSP (the receiving bank) will settle the indemnity claim.

- The MasterCard and Visa card payment systems include a chargeback process. Under this system, following a disputed payment, the sending PSP (the issuing PSP) provides an immediate refund to their customer and then initiates a claim from the receiving PSP (the merchant acquirer). This is targeted at goods not delivered and fraud. The rules do not generally deal with the liability relationship between the issuer and the cardholder or the acquirer and the merchant. There are differences between card systems and push payments that may be important. For example, card payments are made to a relatively limited number of merchant accounts compared to Faster Payments, which can be sent to all PSP accounts, so monitoring of these accounts is relatively easier. But another distinction that may be important is the possibility that the card schemes have a stronger commercial incentive to develop suitable rules on chargeback arrangements. The schemes need to be attractive to acquirers and issuers, who in turn want to attract merchants and cardholders respectively.

5.57 Any actions PSOs take to become more involved in tackling APP scams may come with a trade-off. For example, the speed of clearing, one of the key attractions of both Faster Payments and CHAPS to customers, is also attractive to fraudsters. A slower Faster Payments system might, along with a requirement for member PSPs to perform more checks, tackle APP scams – but to the detriment of the overwhelming majority of transactions over the system which are legitimate.

6 Legal considerations for improving consumer safeguards against APP scams

PSPs have cited their obligations under the Data Protection Act 1998 and the duty of confidence which they owe their clients as reasons why they cannot share more information to prevent fraud and recover funds. The DPA 1998 does not amount to a blanket prohibition on information sharing for fraud prevention; indeed, it has recognised exemptions for this purpose. Nonetheless, PSPs have sometimes interpreted the DPA 1998 differently. Inconsistent practices have been harmful to consumers and hindered the efforts of law enforcement.

PSPs also cite the 'tipping off' offences under the anti-money laundering regime as a barrier to greater cooperation on fraud prevention. A PSP will not be liable for tipping off unless it knew or suspected that any disclosure would prejudice a money laundering investigation. Case law suggests that if the banks are in doubt as to their money laundering obligations, they should approach the relevant authorities and, if needs be, the courts for guidance.

PSPs believe they face new challenges in their efforts to prevent fraud from new legislation such as the requirements in the new Payment Accounts Directive. That legislation requires them to provide basic banking services to a wide range of people. The legislation, however, makes exemptions where providing a bank account would be contrary to fraud or anti-money laundering legislation.

6.1 Though PSPs are not liable for unauthorised payments, they remain under obligations, the purpose of which is to prevent and deter fraud.[60] However, a number of PSPs and representative bodies have suggested that PSPs are inhibited in their efforts to prevent and detect fraud by existing legislation. In particular, some financial institutions believe they are:

- **unable to share information and data**, either preventatively or in order to recover fraudulently obtained funds
- **constrained by their anti-money laundering obligations**
- **required to allow increased access to bank accounts,** most notably by the new EU Payments Account Directive (as transposed into UK law by the Payments Account Regulations 2015) and limited in their ability to close them

6.2 Other parties, however, including some financial institutions, believe the PSPs are adopting an overly cautious approach to their obligations and potential liability under existing legislation.

[60] For more information, see Annex 4.

6.3 PSPs have also suggested that they believe they face legal barriers which limit the extent to which they can repatriate funds originally transferred as part of an APP scam. While those concerns are briefly set out, they are not considered in detail in this response for the reasons outlined below.

Data and information sharing

6.4 PSPs have obligations with regard to information sharing under both the Data Protection Act 1998 (DPA 1998), as 'data controllers', and under their common law duty of confidentiality in light of the banker-customer relationship.

Data protection

6.5 The DPA 1998 requires PSPs to take appropriate measures to protect their customers' data.[61] If they fail to do so, they may be liable in damages for a data breach. They may also be fined by the Information Commissioner's Office (ICO), which is the UK's independent body set up to uphold information rights and is responsible for the enforcement of the Data Protection Act 1998. The maximum fine that can be imposed is currently £500,000. The highest fine handed out to date was against TalkTalk, where the data of around 147,000 customers was compromised.

6.6 The DPA 1998 requires PSPs to fulfil certain pre-conditions before they can collect or share personal data[62], including so called 'sensitive personal data', which includes data related to the (alleged) commission of a crime. The legislation allows PSPs to process data if it is 'necessary for a legitimate interest' or for the 'prevention and detection of an unlawful act' (where this is in the substantial public interest).[63] In addition, the DPA 1998 also requires PSPs to comply with a number of data protection principles, such as the requirement that they only disclose data for the purpose for which it was collected, and ensure the data shared is accurate.[64]

6.7 The legislation, however, includes a number of exemptions including one which exempts PSPs[65] from a number of obligations under the DPA if it is **necessary**[66] for '***the prevention or detection of crime***', where applying the DPA would otherwise '*be likely to prejudice*' that aim.[67] The Criminal Finances Bill may also be relevant in this field as it seeks to improve the ability of PSPs and others in the regulated sector to share information on money laundering threats (discussed further in Chapter 7).

[61] The DPA 1998 brought into effect Council Directive 95/46/EC.
[62] See Annex 4 for further information on the conditions for processing.
[63] ICO, meeting notes from second meeting, dated 18 November 2016. See Annex 4.
[64] See Annex 4 for further information on the data protection principles.
[65] The courts have recently confirmed that DPA 1998, Section 29, can be invoked by a '*private person or body*', and not only by a public body such as the police: *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB) (6 April 2016, unreported), at [36].
[66] The word 'necessary' does not appear in DPA 1998, Section 29 itself. However, the courts have recently confirmed that the provision must be read in light of Article 13 of the parent Directive, for which the exemption must be a 'necessary measure': *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB) (6 April 2016, unreported).
[67] DPA 1998, Section 29. See also *R (Lord) v Secretary of State of the Home Department* [2003] EWHC 2073 (Admin); [2004] Prison L.R. 65.

6.8 As it stands, therefore, **the DPA 1998 is not a complete bar to data sharing**. Even where the crime exemptions do not apply, the DPA 1998 does not act as a blanket rule preventing disclosure, but rather as a framework to ensure any disclosure that is made is appropriate.[68]

6.9 Different PSPs, however, appear to have interpreted the scope for information sharing for fraud prevention under the DPA 1998 in different ways. There does not appear to be a common understanding or practice amongst them, for example, as to:

- the scope of the conditions for processing (some PSPs said they believed they could not share information on the basis of a suspicion of fraud alone)
- the scope of the crime exemption[69]
- what the data protection principles themselves require

6.10 The PSPs' varied interpretations of the law appear to have led to inconsistent practices. This inconsistency, in turn, has proved harmful to consumers and has frustrated the actions of public authorities. In those circumstances, efforts can be made to agree a common, consistent approach to data sharing.

6.11 The ICO suggests that organisations should carry out a privacy impact assessment to establish the most effective way to comply with their data protection obligations.[70] In addition, where organisations seek to share data on a regular, ongoing basis, the ICO recommends that they draft a 'data sharing agreement'.[71] Such an agreement typically sets out the basis upon which the organisations will share information and the processes they will follow when doing so. While the organisations may nonetheless still fall foul of the DPA 1998, and will be required to exercise judgment on a case-by-case basis in deciding whether to share information, they may be less likely to commit a data breach where they have actively considered their information sharing obligations.

Confidential information

6.12 In addition to their obligations under the DPA 1998, PSPs owe their customers a duty of confidence.[72] The duty covers information beyond the scope of the DPA 1998, such as information on corporations and limited liability partnerships (LLPs) and information other than 'personal data'.[73]

6.13 Like the DPA 1998, however, there are recognised exceptions to the duty. In particular, PSPs will be able to disclose otherwise confidential information where there is a duty to the public to do so.[74] The extent of this exception is discussed further in Annex 4.

[68] Though any PSO or other PSP not in a contractual relationship with the individual is prohibited from disclosing information shared to them without the customer's PSP's consent: DPA 1998, Section 55.
[69] See further Annex 4.
[70] See further: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[71] See further the ICO data sharing code of practice. Available: https://ico.org.uk/media/1068/data_sharing_code_of_practice.pdf
[72] Common law: *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461; Equity: *Douglas v Hello! Ltd (No. 1)* [2001] QB 967. The courts, when deciding cases of this nature, are also required to protect individuals' rights to privacy under Article 8 of the European Convention on Human Rights, incorporated by the Human Rights Act 1998.
[73] Ibid, per Scrutton LJ at [481].
[74] See Annex 4 for further information.

Summary on information sharing

6.14 Overall, neither the DPA 1998 nor the rules at common law amount to a prohibition on the sharing of data and information for the purpose of preventing fraud and crime. Inconsistent practices have hurting consumers and hindered the chase of funds.

Anti-money laundering obligations

6.15 PSPs have also suggested that anti-money laundering legislation hampers their ability to: (a) share information on fraud; and/or (b) prevent fraudulently obtained funds from being withdrawn or transferred to other bank accounts. For example, PSPs have indicated that they are concerned that:

- if they provide information to another PSP (or its customer), they may **inadvertently 'tip off' the scammer** (tipping off is an offence under the Proceeds of Crime Act 2002 (POCA 2002))
- if one of their customers receives fraudulently obtained funds, they **may risk tipping off that customer by freezing his or her account or refusing to execute a transfer**
- if **the individual suspected of fraud is not in fact a scammer,** they may have to compensate him or her for losses caused by anti-money laundering actions they take

Tipping off: the offences

6.16 POCA 2002 requires PSPs not to disclose information related to money laundering in certain circumstances.

- It contains two so-called '**tipping off**' offences:
    - It is an offence to **disclose to another person that a disclosure of information has been made to the relevant authorities** under the legislation, where that information was acquired in the course of business in the regulated sector and relates to a money laundering offence, in circumstances in which this is likely to prejudice any investigation that might be conducted.[75]
    - It is also an offence **to disclose to another person that an investigation into money laundering** under the legislation is being contemplated or carried out, where doing so is likely to prejudice that investigation and, again, the information was acquired in the course of business in the regulated sector.[76]
- There is also a separate offence for making a disclosure likely to prejudice the investigation.[77]

6.17 The tipping off offences relate to money laundering, rather than fraud more specifically. However, there is overlap between the two. The courts have held that the original transfer of funds from a customer to a 'fraudster' does not amount to money laundering as, at the time of

[75] POCA 2002, Section 333A(1) and (2).
[76] POCA 2002, Section 333A(3).
[77] POCA 2002, Section 342.

the first transfer, the money does not *yet* represent the '*the benefit of criminal conduct*'.[78] The first transfer is not therefore considered to be a transfer of criminal property. In certain circumstances, however, the subsequent transfer of fraudulent funds may amount to money laundering.[79]

Tipping off: information sharing between PSPs and with customers

6.18 During the course of our investigations, PSPs repeatedly suggested that by sharing information based on their suspicion of fraud, they risked committing a tipping off offence. More specifically:

- First, in their capacity as the PSPs of defrauded customers, stakeholders raised the concern that they cannot provide information to their own customers to pursue missing funds or legal action.
- Second, as the PSP with which the scammer holds an account (or operates through a mule), stakeholders indicated they were sometimes reluctant to provide information to defrauded customers or their PSPs.

6.19 PSPs, however, will not be guilty of a tipping off offence for sharing information unless:

- the information **relates to money laundering**
- a **disclosure** has been made to the relevant authorities has been made or an **investigation** into alleged money laundering is under way or contemplated
- the disclosure is **likely to prejudice** any current or contemplated investigation by the National Crime Agency (NCA) or one that might occur
- it **knew or suspected** that the disclosure would be likely to cause such prejudice[80]

6.20 A number of exemptions apply to the tipping off offences. For example, there is an exemption which facilitates disclosure '*for the purpose of the* ***detection, investigation or prosecution of a criminal offence'***[81], which appears to be oriented towards public authorities. However, there is also an exception where information is shared with the other financial institution involved in a payment transaction[82], and for the '***purpose only of preventing a money laundering offence'***.[83]

6.21 The case of *C v S* considered the issue of when a PSP could share information with its own defrauded customer.[84] In that case, a company sought information from its own bank in order to trace money which it had lost to a fraudster. It had obtained an order from the courts requiring its bank to disclose documents that would help it pursue the money it had lost.

[78] R v Loizou [2005] EWCA Crim 1579; [2005] 2 Cr App R 37: in the original transfer, the money does not constitute 'criminal property' as, at that stage, it does not represent the 'benefit from criminal conduct'. The original transfer of funds is not therefore money laundering.
[79] See POCA 2002, Sections 327, 328 and 329.
[80] POCA 2002, Section 333C.
[81] POCA 2002, Section 333D(1)(b).
[82] On the condition that the other PSP is situated in the EEA and subject to equivalent duties of professional confidentiality and the protection of data under the DPA 1998 as the PSP sharing the information: POCA, Section 333C.
[83] POCA 2002, Section 333C.
[84] [1999] 1 WLR 1551.

However, the National Crime Intelligence Service did not want the company to know about its involvement in the matter. The company's PSP found itself in a position whereby it risked contempt of court if it did not comply with a court order, and at the same time, faced criminal liability for tipping off if it did. The Court of Appeal indicated that in such a scenario, the PSP should first contact the relevant authority to make it aware of its position and to establish what information, if any, it can share. If that proves unacceptable, the PSP should then seek an advisory declaration from the court.

Tipping off: action taken to prevent transfer or withdrawal of funds

6.22 PSPs have also raised concerns that they may inadvertently commit a tipping-off offence by taking action to prevent the subsequent withdrawal or transfer of fraudulently obtained funds. The High Court has held that, once a PSP has received and authenticated a transfer in accordance with the payment rules, it cannot refuse to accept the transferred funds solely on the basis that it suspects fraud.[85] If a PSP wishes to prevent any subsequent withdrawal or transfer of those funds, it may therefore feel obliged to freeze a customer's account or refuse to execute payment instructions to prevent money laundering.

6.23 In *Shah and another v HSBC Private Bank (UK) Ltd*[86]*,* the High Court held that there is an implied term in the contract between the customer and banker that the latter may refuse to provide the former with information where to do so would contravene its legislative duties and put the PSP at risk of committing a tipping off offence. However, PSPs have suggested that even the act of freezing the account without explanation may give the scammer an indication that his or her actions are being investigated.[87]

6.24 The courts have suggested that if PSPs are in doubt as to whether they should share information related to money laundering, they should seek the advice of the competent authority or subsequently the advice of the courts, as to what information they can disclose to avoid liability.[88] The courts have further indicated that '*it is unthinkable there would be a prosecution*' in circumstances where the PSP has followed clear guidance by the relevant authorities on the assurance that there will not be a tipping off prosecution.[89]

Liability for mistaken suspicions

6.25 Finally, it has been suggested that some of the reluctance to share information of suspected fraud or to freeze accounts stems from a concern that the PSPs will incur liability where their suspicions do not turn out to be correct. For example, some concern has been voiced that if a PSP shares information that results in an account being frozen or a transfer being blocked, the PSP will be liable for any associated losses if the customer in question is innocent.

[85] *Tayeb v HSBC Bank Plc* [2004] 4 All ER 1024: a PSP which suspected its customer had acted fraudulently was held liable for returning funds from its customer's account to the original sending account, as suspicion as to the origin of the funds alone was insufficient justification for returning them.
[86] [2012] EWHC 1283 (QB); [2013] 1 All ER (Comm).
[87] See *Green v Walkling* [2008] BCC 256, where the court recognised that an individual would not have been able to provide a rational reason for his refusal to sign a contract, where such a refusal would be based on money laundering concerns.
[88] *C v S* [1999] 1 WLR 1551.
[89] *C v S* [1999] 1 WLR 1551.

6.26 The courts have confirmed that a PSP will not be liable for failing to execute a payment instruction where it does so in good faith on the basis that it suspects money laundering.[90] The PSP can be required to prove its good faith suspicion,[91] and that suspicion cannot be based on a 'vague feeling' alone and must be 'more than fanciful'.[92] However, the PSP need not have reasonable grounds for its suspicion.[93]

Summary on money laundering as a barrier to fraud prevention

6.27 Overall, PSPs have raised their concerns that there is a risk that they will commit a tipping off offence under POCA 2002 if they share information or freeze accounts to prevent fraud. The POCA offences are punishable by up to two years' imprisonment and a fine, so PSPs' caution may be warranted.[94]. We note, however, that:

- the offences are subject to caveats and exemptions which reduce the risk of tipping off
- the courts have also given guidance to PSPs as to what they should do if they are in any doubt about their tipping off obligations in a particular situation
- the courts have clarified the circumstances in which PSPs will be required to compensate their customers for losses arising from a mistaken suspicion

Repatriating funds associated with an APP Scam

6.28 With regard to the repatriation of funds, one stakeholder suggested that the PSPs will face both criminal and civil liability if they return funds to a victim who has authorised a transfer. It believed that:

- PSPs may end up liable if they repatriate funds from an account holder, if it transpires he or she is not a scammer
- the law on how funds should be distributed from a scammer's account is unclear and subject to tipping off concerns

6.29 While the legal ramifications of repatriating funds transferred in an APP scam may be relevant to the issue of push payment fraud, they are not considered in further detail in this response having regard to its already broad scope and its focus on issues of liability (where the original funds have been lost), rather than the return of specific funds.

[90] See *Shah*, above.
[91] *Shah and another v HSBC Private Bank (UK) Ltd* [2010] EWCA Civ 31; [2010] 3 All ER 477.
[92] *R v Da Silva* [2006] EWCA Crim 1654; [2007] 1 WLR 303.
[93] *R v Da Silva* [2006] EWCA Crim 1654; [2007] 1 WLR 303; *K Ltd v National Westminster Bank plc* [2006] EWCA Civ 1039; [2006] 2 All ER (Comm); *Shah and another v HSBC Private Bank (UK) Ltd* [2012] EWHC 1283 (QB); [2013] 1 All ER (Comm).
[94] For conviction on indictment: POCA, Section 333A(4).

Payment Accounts Directive and regulations

6.30 The **Payment Accounts Directive** (PAD)[95], which was implemented in the UK via the **Payments Accounts Regulations** (PARs)[96], aims to improve access to basic bank accounts to ensure that all consumers legally resident in the EU have access to basic banking services.

6.31 Subject to certain conditions[97], the PARs require PSPs to offer a basic account with basic features to any consumer legally resident in the UK within 10 days of the application[98], even where the consumer has no fixed address in the UK.[99] A basic account must allow a customer to withdraw cash from the account at an ATM and execute online payments[100], and PSPs are prohibited from limiting the number of payments made.[101]

6.32 PSPs have raised concerns that one of the unintended consequences of PAD and the PARs may be increased financial crime. The PARs specifically require PSPs to refuse an application for a basic account with basic features if allowing it would be contrary to the Fraud Act 2006 or the Money Laundering Regulations 2007.[102] However, PSPs believe this provision may not allow them to refuse an application on the basis of a suspicion of fraud alone.

[95] Directive 2014/92/EU on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, adopted in July 2014.
[96] 2015/2038, brought into force in the UK on 18 September 2016.
[97] See PARs, Regulation 23(1).
[98] PARs, Regulation 24.
[99] PARs, Regulation 23(2)(a).
[100] PARs, Regulation 19(1).
[101] PARs, Regulation 19(3).
[102] PARs, Regulation 25(1). They also require the bank to refuse an application that would be contrary to the Immigration Act 2014, above, or would otherwise breach the bank's requirements for carrying out regulated activities.

7 Future regulatory and industry developments

There are a number of initiatives under way or planned that seek to tackle problems relating to financial crime. Most of the initiatives are designed to tackle fraud more generally, rather than focusing narrowly on authorised push payment scams, but should have the potential to alleviate the types of scams that the super-complaint focuses on. The two main initiatives that we are aware of are those of the Joint Fraud Taskforce and the Payments Strategy Forum. Specific measures that might help include:

- a confirmation of payee solution that may reduce the risk of payers sending funds to an account that is not in the name that they expect
- work on tracking funds through the payment systems to help identify the destination account for frauds
- improved information sharing between PSPs

Stakeholders have also alerted us to a number of legislative developments that may have implications for the problem of authorised push payment scams. In some cases, the motivation for the legislation is not primarily related to fraud, but parties suggested that it may nevertheless alleviate or exacerbate the problems associated with these types of fraud. Examples of potentially relevant legislation on the horizon include second Payment Services Directive, the fourth Anti Money Laundering Directive, the second Wire Transfer Regulations and the General Data Protection Legislation.

Introduction

7.1 In this chapter we outline key developments on the horizon that may affect the problem of authorised push payment (APP) scams. Parties alerted us to a large number of different developments that may be relevant.

7.2 Positively, there are a number of initiatives involving various stakeholders (including PSPs) already under way or in the pipeline that have the potential to tackle APP scams. We highlight some of the more relevant developments, providing a brief summary of what is planned and how it may help.

7.3 We also discuss legislative developments on the horizon that may be relevant. Some of these may not have been motivated by a desire to tackle fraud, but they nevertheless may either reduce or exacerbate the problem of APP scams. Such developments illustrate the interaction between policies to tackle APP scams and policies to achieve other policy goals. There are often important trade-offs for policymakers to consider.

Industry initiatives

7.4 There are a number of industry initiatives, often involving the PSPs working with other parties, designed to tackle financial fraud. We discuss some of the initiatives that might help reduce APP scams in this section, including:

- the programme of the Joint Fraud Taskforce (JFT)
- the strategy of the Payments Strategy Forum
- account safeguards
- the Banking Protocol

7.5 The first two items – the work of the JFT and the Payments Strategy Forum – include a wide scope of activities that have the potential to contribute materially to the fight against APP scams.

7.6 We also discuss a number of industry developments that may affect the prevalence of APP scams, even though that may not be the primary motivation for the changes industry is initiating. These include:

- the API Open Banking Work
- pressure on Faster Payments thresholds
- the Financial Services Trade Associations Review

Programme of the Joint Fraud Taskforce

7.7 The new JFT established in February 2016 is made up of key representatives from government, law enforcement and the banking sector. The Taskforce includes the City of London Police, National Crime Agency, Financial Fraud Action UK (FFA UK), Cifas, Victim Support, Trading Standards, the FCA and CEOs of the major PSPs. The JFT was set up to inform the national picture of fraud, to deliver an improved tactical response to fraud and to design out the vulnerabilities in the industry which fraudsters exploit. It also aims to empower customers and to protect them from falling victim to fraud.

7.8 The Home Secretary chaired an Oversight Board of the Taskforce in September, where a forward programme was agreed that will focus on: improving the national, regional and local law enforcement response to fraud; increasing fraud awareness and prevention; introducing a system to make it much easier for the victims of fraud to have their money repatriated; and a new collective approach to better support victims of fraud. The initiatives that, in our view, have the most direct effect on prevention of APP scams are outlined below.

7.9 **Awareness campaigns and behaviour change**[103]**:** The JTF will launch a number of awareness campaigns targeting different customers. The plan is to deliver a highly visible, hard hitting campaign to better protect customers and the wider public. They anticipate a new improved Take 5 campaign to launch in the first quarter of 2017 with phase 1 running over the course of the year.

[103] See also the overview produced by the Payments Strategy Forum on the current financial crime education and awareness:
https://www.paymentsforum.uk/sites/default/files/documents/FCDS%20WG%20-%20Education%20and%20Awareness%20%28financial%20capability%29.pdf

7.10 **Funds repatriation:** This initiative will help banks to trace funds being moved across multiple accounts. If implemented, it will allow banks to trace payments through the UK payment system and enable them to identify and return funds to customers who contact them to say they have been a victim of fraud.

7.11 There are three limbs to the work:

- **Technological solution:** The appropriate technology is needed to trace funds back to source through the payments network. The current proposal uses data from Bacs, FPS and banks' 'on-us' transactions. They are currently in discussion with infrastructure providers and banks will be making a decision about whether they want to fund the work.

- **Operating system:** Banks will need to agree ways of operating that allow for the freezing and return of funds between accounts and a system for dealing with disputes. FFA UK has sent a proposal to UK banks for them to consider and JFT expects initial views back by the end of the year.

- **Legal framework:** A legislative framework will be needed to allow the banks to undertake this work, in light of perceived legislative and contractual constraints.

7.12 PSPs have suggested that, where they try to pursue fraudulently obtained funds, they can only see the receiving account for the first bank transfer, and not for subsequent onward transfers. While this initiative will not help banks to return money that has already left the UK payments system, it may well protect significant numbers of customers and prevent money falling into the hands of fraudsters. The initial proposal will only identify mule accounts after fraud has happened. Further work would be necessary to enable daily retrospective monitoring and real-time monitoring. This capability would require closer integration to the central infrastructure provider or other party undertaking the data analytics.

7.13 This initiative may potentially result in some 'quick-wins' from a law enforcement angle. However, some stakeholders believe that legislative changes may be needed in order for this to work, including in the area of data sharing and funds repatriation. PSPs have also suggested that there may be legal risks associated with repatriating funds obtained via an APP scam back up the chain (as discussed in Chapter 6).

7.14 **Victims and vulnerability:** Victim Support and Trading Standards are currently developing a strategic action plan on victims and the vulnerable. This is likely to include: completion of the BSI minimum standard on the treatment of victims and the vulnerable for financial institutions; the national roll out of the Banking Protocol (discussed later) from next January; pushing for the introduction of additional opt-in account safeguards; and options for an improved multi-agency support for victims and better data sharing to support that activity.

Payments Strategy Forum

7.15 The Payments Strategy Forum (Forum) was created by the PSR in March 2015 with a specific focus on developing a strategy for the payments sector where the industry needs to work together. It published its final strategy in November 2016.[104] The Forum has defined solutions across four areas: responding to end-user needs; improving trust in payments; simplifying access to promote competition; and building a new architecture for payments.

7.16 For the first three areas, the Forum is tasked with developing the requirements and rules for each of the solutions by end 2017. Once the rules and requirements have been developed they will be made available for the competitive market to develop products and services.

[104] Available here: https://www.paymentsforum.uk/final-strategy

So products and services could be in place from 2018 onwards, although the Forum believes the new payments architecture is necessary to meet the needs fully.

7.17 Many elements of the Forum's strategy have the potential to reduce the risk or impact of APP scams. These are: confirmation of payee; guidelines for identity verification; payment transaction data sharing and data analytics; financial crime intelligence sharing; trusted KYC data sharing and storage repository; and customer awareness and education. According to some stakeholders, other elements, such as request-to-pay, may require that proper precautions be taken to avoid an increased risk of APP scams.

Assurance data – confirmation of payee

7.18 One of the solutions identified in the Forum's final strategy is assurance data, which will include both confirmation of payee and confirmation of receipt. This solution will give both payers and payees assurance, before (and after) a payment is sent, that their payment intentions were followed through. This may avoid misdirected payments and may also reduce the risk of some types of APP scams, particularly those we have labelled maliciously misdirected.

7.19 The Forum has prioritised the collaborative development of the necessary standards and rules, which are required for implementation of 'Confirmation of Payee'. The Forum has proposed a timeline of July to produce these for public consultation, with the work finalised by end 2017. Once these standards and rules are in place, the competitive market will be in a position to develop products and services for end-users, so there is a possibility that a 'Confirmation of Payee' solution could be available from 2018 onwards.

7.20 Even before the Forum's final strategy was published, a number of stakeholders commented on how a confirmation of payee concept might help with the fight against APP scams. Generally we have received positive reactions to such an initiative. However, some stakeholders warned that it is not clear at this stage what the resource requirements are or to what extent this would help prevent existing cases of fraud.

7.21 The Forum itself has identified potential risks related to data privacy and security along with potential legal issues related to the solution's use of personal data for confirming the recipient and receipt of a payment, but these will be ironed out during the design phase.

7.22 One respondent told us that payee verification could play into the hands of scammers (by encouraging customers to trust a payee without further verification) and would slow down payments. Other stakeholders told us there is no single solution to the problem. Two respondents noted that a genuine account holder could have many legitimate names (or ways of expressing a legitimate name). As such, the model needed to recognise a 'fuzzy logic' on the names used.

Guidelines for identity verification, authentication and risk assessment

7.23 The Forum has a proposal to improve PSPs' identity verification. Improved identity verification may reduce the risk of APP scams by making it more difficult for scammers to obtain bank accounts.

7.24 The Forum's proposal is to implement a non-compulsory guideline as a benchmark to determine how the identity of a payment service user is established, verified, used and relied upon by other PSPs. The aim is to establish consistent rules for identification in order to reduce the risk when transferring money using different payment mechanisms. The Forum expects that the specification would include requirements for identity assurance in account opening, re-authentication, setting up payment mandates, confirming payer and payee when initiating payments, mutual authentication (for example, a bank identifying itself to customer), and incorporating identity assurance into existing risk assessment processes.

7.25 One respondent suggested that greater due diligence measures could result in certain groups of customers being excluded from banking services. Some stakeholders told us that this option would require constant reviewing. One stakeholder also raised concerns about providing a general guidance if it leaves discretion to banks to adopt minimum standards rather than the full solution.

Payment transaction data sharing and data analytics

7.26 The Forum proposes the introduction of transaction data sharing to support collaboration and data sharing between the PSOs and PSPs who own the data; and data analytics capabilities to manipulate the data and extract insights relating to priority financial crime use cases. This could enable the identification of mule accounts, increased ability to repatriate funds to the victims of crime, and greater flexibility in how PSPs respond to fraud.

7.27 However:

- creating a central repository of data creates new risks related to how secure the data storage facility is, who has access to the data, the purposes for which data is used, and how that use is monitored

- some respondents also said the costs of making the changes could have a negative impact on some of the smaller players

Financial crime intelligence sharing

7.28 The Forum seeks to leverage the government's efforts to improve information sharing on financial crime in creating the Joint Money Laundering Intelligence Taskforce (JMLIT) and the JFT. Its proposed solution is an industry-operated intelligence capability, which is underpinned by a formal legal agreement, a code of conduct, and appropriate measures to protect data. It has been suggested that this resource will provide PSPs, in near real time and real time, with all known financial crime data records for confirmed, attempted, suspected or at-risk frauds. The aim is to provide access via a single source of data and intelligence without increasing workloads for PSPs, significantly changing working practices or increasing the security risks.

7.29 However, there may be risks to consumers from sharing this type of data. Labelling people wrongly can cause significant detriment if, for example, accounts are wrongly closed or frozen. Careful governance, in particular for intelligence sharing, would need to be created to ensure that this process delivers the outcomes anticipated, without creating additional risk. The establishment of this governance would need to involve expert groups, such as the new banking trade body, National Crime Agency, the City of London Police, and be subject to a legally robust framework.

7.30 We have been told that currently financial crime data and intelligence sharing between PSPs is inconsistent. We have also been told that there are significant differences between banks and other agencies in what is recorded, collected and reported. In particular, improved intelligence sharing could increase the probability of identifying malicious payees' accounts at an early stage. This could reduce the risk and impact of APP scams.

Trusted KYC data sharing and storage repository

7.31 The Forum proposes a mechanism for sharing KYC data between PSPs (and possibly other participants) focusing on business customers.

7.32 The solution is motivated by the hope that it will reduce the ability for scammers to open accounts and execute payments or transfers. The solution will require PSPs to agree a set of

standards for collecting and classifying KYC data for business customers. The more standardised approach will enable more dynamic anti-money laundering risk monitoring across the industry, and reporting of suspicious activity.

Customer awareness and education

7.33 As well as the responsibilities of industry in this field, there is still a role for customers to play to reduce vulnerabilities and improve security. Customer awareness and education may reduce the risk of customers falling victim to APP scams.

7.34 The Forum proposes that one of the industry bodies involved in consumer education (such as the JFT or the new banking trade body) should take the lead on delivering a more coordinated and streamlined approach, thus avoiding unnecessary duplication and cost.

Request to pay

7.35 One of the solutions identified in the Forum's final strategy is Request to Pay. This would enable government, businesses, charities and consumers to create and send payment requests. If recipients choose to respond, they could do so with a payment type of their choice. In respect of authorised push payments, it could enable the payer to verify that the request to pay comes from a legitimate payee.

7.36 One stakeholder noted that this solution could exacerbate the problem of fraudulent payments because consumers may trust that the request to pay comes from a legitimate source without verifying it.

Banking protocol

7.37 The Havering initiative is a multi-agency initiative between financial sector organisations, Trading Standards and the police. It aims to provide consistency across financial institutions around scams and a standard methodology for managing and reporting them to the police. As well as training staff to recognise fraud, the protocol ensures police will attend emergency calls by PSP staff as a priority. Currently in a pilot phase, there is a plan to roll out the protocol across London in the next few weeks and then nationally.

7.38 This initiative has some potential to improve the response to APP scams. However, a number of parties have noted that, while it is a welcome development, since it focuses on in-branch withdrawals it will not affect fraudulent payments initiated online.

Account safeguards

7.39 Banks together with fraud prevention agencies are considering developing added-on services to accounts which could be offered to customers on a commercial basis. Such services have the potential to reduce the risk or impact of APP scams. Examples of these potential services include text messages alerts, agreed individual limits on transactions, text messages sent to a trusted third party in the event of a payment transaction initiated by a vulnerable customer and 24-hour payment delays.

7.40 However, these suggested solutions also pose potential difficulties and challenges. For example:

- Adding account safeguards to reduce the risk of APP scams would represent a trade-off between risk and customer convenience. We have been told by some stakeholders that customers dislike anti-fraud tools as they slow down the payment transaction.

- One respondent noted that it would be difficult to agree on measures affecting specific customer groups due to the unintended consequences of putting a label on customers. For example, the proposals raise difficult issues concerning what autonomy you allow different customer groups.

- One large bank told us that in their experience, when they contact customers attempting to make an APP scam, 'the timing, message and method of communication greatly influences their ability to 'cut through' and encourage customers to reconsider. The kind of intervention that works for one type of scam (for example, invoice scams) may not work for another type of scam (for example, romance scams). In certain circumstances, a prompt may be enough; in more sophisticated or emotive scams, only personal and empathetic contact provides the best chance of success – and even then, the customer may still decide to go ahead'.

The Open Banking Standard and Application Programming Interface

7.41 In September 2015, an Open Banking Working Group (OBWG) was set up at the request of the Treasury to explore how data could be used to help people use their money. The OBWG has recommended the creation of an Open Banking Standard that will make it possible for banking data to be shared and used securely.

7.42 In its report the OBWG made a number of relevant recommendations.[105] It suggested that:

1. Open interfaces should be created to enable services to be built using bank and customer data. These would include shared data about bank transactions that individuals or businesses can choose to share through secure and controlled means.

2. Third parties specialising in security and the detection of fraudulent transactions may offer better quality monitoring and notification services. It noted this may be particularly compelling if the third party aggregates data across multiple accounts or products and can spot patterns that a single product provider would otherwise not see.

7.43 Stakeholders have suggested that these proposals raise a number of potential challenges in fraud prevention and detection. For example, some stakeholders believe that:

- By increasing the number of PSPs involved in the payment chain, it will be more difficult for them to identify fraud by using data analytics or by monitoring access to systems.

- Open interfaces and data sharing between organisations introduces new risks for customers as banks will be less in control of data flows. For example, one stakeholder indicated that open APIs magnify the potential for scams, as customers share sensitive data with third party organisations, which are sending credit transfers on their behalf.

[105] See https://www.paymentsforum.uk/sites/default/files/documents/Background%20Document%20No.%202%20-%20The%20Open%20Banking%20Standard%20-%20Full%20Report.pdf

- Open APIs may present cyber-criminals with a new attack vector. Attacks can come in a number of different guises – from those that target technical infrastructure to those that are socially engineered – and capitalise on lack of customer familiarity. The result of such attacks, unless appropriately mitigated, can range from intermittent service provision through to data loss, fraud and identity theft. There may be a need for better customer education in this field.

Pressure on Faster Payments thresholds

7.44 Currently banks and building societies can enable their customers to send Faster Payments of up to [✂] per payment. [✂]. A number of stakeholders believe that the pressure for increased speed in payments and increased payment limits will make it more difficult to prevent frauds, although PSPs can set their own limits for transfers on FPS by their customers that is lower than the overall scheme limit.

Financial Services Trade Associations Review

7.45 The Financial Services Trade Associations Review was an independent review into the effectiveness and efficiency of the financial services trade association landscape. On 20 November 2015 a final recommendation was published. The recommendation proposed that the British Bankers' Association, Council of Mortgage Lenders, Payments UK and UK Cards Association be integrated to create a new trade association.

7.46 One of the benefits of a combined trade association may be access to an integrated database. This may allow a more comprehensive overview of information which could be used in fraud prevention. It is expected that the new trade association would work together with FFA UK developing and delivering a fraud strategy.

Future legal developments

7.47 There are several pieces of legislation both at UK and EU level aimed at increasing security of data and electronic payments and strengthening the powers of fraud prevention agencies in combating fraud and financial crimes.

7.48 Parties have made us aware of legal developments which would be relevant to preventing fraudulent payments. We have included a number of legal developments which stakeholders consider may have some impact (positive or negative) on the issues raised in the super-complaint.

7.49 Stakeholders, including PSPs, consider the following legislative initiatives could have an effect on the risk or impact of APP scams:

- the 2nd Payment Services Directive (PSD2)[106]
- the 4th Money Laundering Directive (4MLD)[107]
- the EU Regulation on information accompanying transfers of funds[108]

[106] (2007/64/EC)
[107] Directive 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.
[108] Regulation 2015/847 of the European Parliament and the Council of 20 May 2015 on information accompanying transfers of funds.

- the General Data Protection Regulation (GDPR)[109]
- the Criminal Finances Bill 2016
- ring-fencing

The second Payment Services Directive

7.50 PSD2 updates and revises the EU rules put in place by the Payment Services Directive and comes into effect in January 2018. PSD2 will be implemented in the UK through an update to the Payment Services Regulations during 2017. The legislation introduces a number of changes which have the potential to have both a positive and a negative impact on APP scams.

7.51 Reflecting the emergence of new players in the area of internet payments, PSD2 will cover new types of payment services, known as 'payment initiation services' (PISs) and 'account information services' (AISs). PSD2 seeks to create a level playing field for firms wishing to provide these services, while also setting out standard requirements for confidentiality, liability and security of these services.

7.52 PSD2 will also introduce further protections for consumers through additional security requirements when authenticating transactions and requirements for PSPs to help customers that enter the wrong unique identifier for an account (as is the case for 'fat finger' errors). Where this occurs, PSD2 will require sending PSPs to make reasonable efforts to recover the funds involved in the payment transaction. Receiving PSPs will have to cooperate in these efforts by communicating to the sending PSP all relevant information for the collection of funds.

7.53 A number of stakeholders have indicated that they believe that features of PSD2 may increase the risk of APP scams. For example, PSD2 implementation may also see the rise of intermediaries between the bank and its customer. PSPs have suggested that this may weaken the effectiveness of their fraud detection systems. For example, several respondents expressed concerns that new players in the payment chain may make it more difficult for the PSP to carry out fraud screening, undermining the current liability regime. Stakeholders also noted that information collection by providers of AISs could exacerbate the problem of APP scams. It may, however, provide a model for information sharing for fraud prevention in the future.

4th Money Laundering Directive (4MLD)

7.54 4MLD is designed to strengthen the EU's defences against money laundering and terrorist financing, while also ensuring that the EU framework is aligned with the Financial Action Taskforce's AML and CTF standards.[110] 4MLD came into effect on 25 June 2015[111] and has to be transposed by member states by 26 June 2017.[112] In July 2016, further targeted amendments to this Directive were proposed by the EU and are currently subject to negotiation.

[109] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
[110] http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf
[111] Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC.
[112] The Treasury proposes to create a Money Laundering and Transfer of Funds (Information on the Payer) Regulations 2017 in order to transpose both the directive and the WTR2. See HMT's Consultation on the transposition of the Fourth Money Laundering Directive published in September 2016.
https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/553409/4mld_final_15_sept_2016.pdf

7.55 In the context of APP scams, the following features of the 4MLD are particularly relevant:

- There is a proposal which, if agreed, would enable national competent authority swift access to information on the holders of bank and payment accounts, through centralised registers or electronic data retrieval systems. This proposal, however, has not yet been agreed.

- 4MLD enables greater access to information on the beneficial owners associated with bank accounts and funds.

- 4MLD strengthens the sanctioning powers of the national competent authority by introducing a set of minimum principles-based rules that member states should ensure are available for systematic breaches of key 4MLD requirements.

7.56 Stakeholders have welcomed provisions that facilitate cooperation between relevant authorities and the private sector with a view to optimizing their efforts in a consistent way.

EU Regulation on information transfers of funds

7.57 The EU Parliament has approved a Regulation which will apply from 26 June 2017.[113] It replaces the Wire Transfer Regulations, which require PSPs (under certain circumstances) to ensure that electronic fund transfers include sufficient information on the person making the payment. The new Regulation extends this to include information on the payee, aiming to improve tracking for transfers of funds sent or received by an EU PSP. It introduces a system of checks, which vary in intensity according to the value of the transfer and whether it is an international or domestic payment.

7.58 In the context of APP scams, the following obligations are important:

1. The Regulation introduces a new requirement on the PSP of the payer to ensure that transfers of funds are accompanied by information on the payee. The information specified is the payee's name and payment account number or unique transaction identifier.

2. In certain circumstances, the payer's PSP may be required to verify the information of the payer before the transfer of funds.

3. The intermediary must ensure that information accompanying the transfer of funds is kept with the transfer, subject to certain technical limitations.

4. The PSP for the payee must either reject a transfer of funds or ask for complete information on the payer where such information is missing. This may also prompt a payee's PSP to make a Suspicious Activity Report.

7.59 Both the PSP of the payee and the intermediary PSPs are obliged to establish effective risk-based procedures for determining whether to execute, reject or suspend a transfer of funds that lacks the required payer and payee information. Overall, the proposals may enhance transparency of information and facilitate the work of the banks in identifying possible frauds. It may also enhance checks and controls put in place by PSPs and will increase the amount of information which needs to be attached to a payment.

[113] The Regulation of the European Parliament and of the Council on information accompanying transfers of funds – repealing Regulation (EC) No 1781/2006: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32015R0847&from=EN

The General Data Protection Regulation (GDPR)

7.60 The GDPR will have direct effect in all EU member states from May 2018. It will replace current EU data privacy laws, including the Data Protection Directive.[114]

7.61 Consent to share data under the GDPR must be 'freely given, specific, informed and unambiguous'. Where profiling of customers is the basis of automated decision-making, it will be permitted under the GDPR only if the data subject has provided 'explicit' consent; where it is necessary for the performance of a contract; or it is otherwise permitted under the applicable law. Customers will have the right to object to profiling at any time, unless the PSP can demonstrate legitimate grounds that override an individual's interests.

7.62 A large number of respondents noted that the stricter requirements introduced by the GDPR could have two different effects. They could increase consumers' protection but at the same time further limit the ability of the banks to use data for fraud prevention and to share or collect data with other market players due to the requirement to obtain clearly evidenced consent.

7.63 Under the GDPR, various sanctions can be imposed for breach of requirements. This includes fines of up to 4% of annual worldwide turnover or EUR20,000,000, whichever is highest, in respect of some serious breaches. This is a marked increase from the current maximum fine of £500,000 that the Information Commissioner's Office (ICO) can currently levy for failure to comply with data protection requirements.

7.64 Scammers have previously used widely reported data breaches as a narrative to convince customers to make APP. The GDPR will introduce mandatory data breach reporting to the supervisory authority without undue delay (72 hours where feasible), unless the breach is 'unlikely to result in a risk for the rights and freedoms' of individuals. Under the current regime, reporting a breach is voluntary. Under the DPA, there is no general obligation to report data breaches to the ICO, but the ICO would expect serious breaches to be reported, and to provide information to the affected individuals if it is appropriate to do so. Under the Privacy and Electronic Communications Regulations 2003 (PECR), telecoms companies and ISPs already must notify the ICO within 24 hours of personal data breaches, and in some cases, also inform individual users and subscribers.

Criminal Finances Bill 2016

7.65 The Criminal Finances Bill 2016 (CFB) is currently before Parliament and has not yet been enshrined in law. If enacted, however, it contains a number of provisions that could prove beneficial in the field of APP scams. Most notably, the proposed legislation would enable a PSP to share information with another PSP upon request, but only where it is satisfied that the disclosure will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering suspicions, including those relating to scams such as APP. Where such a disclosure is made in good faith, it will not constitute a breach of the DPA 1998 or the duty of confidence. In addition, the proposal Bill includes a new power to allow money held in bank accounts to be swiftly seized and forfeited where there are reasonable grounds to suspect that the funds within it are recoverable property, or are intended for use in unlawful conduct.

[114] See ICO's Overview of the GDPR, published on 11 October 2016: https://ico.org.uk/media/for-organisations/data-protection-reform/overview-of-the-gdpr-1-1.pdf

Ring-fencing

7.66 The Banking Reform Act 2013 introduced a ring-fence around retail deposits held by UK banks.[115] The aim is to separate certain core banking services critical to individuals and small and medium-sized enterprises (SMEs) from wholesale and investment banking services. The ring-fences is intended to protect the uninterrupted provision of critical banking services to retail and SME depositors.

7.67 One important change is the prohibition on ring-fenced PSPs from entering into any transaction that requires the use of services provided through an interbank payment system unless the PSP is a direct participant in the system. This means that all such PSPs will be required to become direct participants of interbank payment systems in their own right (unless there are exceptional circumstances). [✂]

[115] New Part 9B of the Financial Services and Markets Act 2000 (FSMA).

8 Our approach to addressing the issues identified

There are three main issues that we consider need to be addressed:

- The ways in which PSPs currently work together in responding to reports of APP scams needs to improve.
- There is some evidence to suggest that some PSPs could do more to identify potentially fraudulent incoming payments and to prevent accounts falling under the influence of scammers.
- The data available on the scale and types of APP scams is of poor quality. Some of the initial evidence we have identified about the scale suggest that it may be significant and the general view held is that the prevalence of APP scams is likely to increase.

We have developed a package of work to address these issues, which seeks to complement the range of work under way or planned for the near future that has the potential to help address consumer harm caused by APP scams.

We have agreed with FFA UK programme of work that the banking industry should lead on that will assist in both understanding the scale of APP scams and in improving how PSPs work together in responding to APP scams:

- Industry, liaising with the 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 (for example, information that would help victims recover their money).
- Industry to develop a common approach or best practice standards that sending and receiving PSPs should follow when responding to instances of reported APP scams.
- Industry to develop, collect and publish robust APP scam statistics, to address the lack of clear data on the scale and scope of the problem, and to enable monitoring of the issue over time.

We will monitor this work on an ongoing basis, and commit to review industry progress in the second half of 2017.

We will consider the potential for the operators of the CHAPS and FPS payment systems to play an expanded role in helping to minimise the consumer harm caused by APP scams. We will look to publish specific terms of reference for this work in early 2017, and our findings in the second half of 2017. We envisage this work will include consideration of how internationally comparable push payment system operators are involved in minimising risk of consumer harm around APP scams and fraud more generally.

8.1 In this chapter we discuss:

- the steps we will take to tackle the issues we have identified regarding PSPs' current efforts to prevent and respond to APP scams
- our views on the appropriateness of the two potential interventions proposed by Which? in the super-complaint

8.2 Before we begin this discussion, we first set out a range of important considerations we take into account in developing our proposals.

Important considerations in developing our proposed actions

The wider scam ecosystem

8.3 The Which? super-complaint is focused primarily on the conduct of PSPs and payment systems in terms of their role in preventing and responding to APP scams. However, there is a wider ecosystem of participants that have a role to play in the prevention of and response to APP scams. We consider that addressing the consumer harm caused by APP scams cannot be achieved solely through actions – taken either by industry or regulators – involving PSPs and payment systems alone.

8.4 Other relevant participants include:

- **Consumers**: Consumers have a responsibility to remain vigilant to the risk of APP scams. As far as is reasonably possible, consumers need to make efforts to understand this risk and to take steps to minimise the risk of falling victim to APP scams.
- **Enabling agents and events**: In many instances, the perpetration of APP scams involves the inappropriate use of online platforms or telecommunications technologies. Accidental leaks of large amounts of personal data enable scammers to effectively target and implement their scams. Companies whose products, services or information have the potential to be abused in such a manner have a responsibility to take steps to ensure the risk of this happening is minimised.
- **Law enforcement**: An effective and proportionate law enforcement response, both in terms of apprehending current scammers and deterring future scammers, is a key element in addressing consumer harm from APP scams.
- **Government**: The government has an important role to play in forming an appropriate overall public policy response to the issue of APP scams.

Other actions already under way

8.5 As set out in Chapter 7, there is a significant programme of work already under way that has the potential to reduce consumer harm caused by APP scams.

8.6 In developing our proposals, we have been mindful of not taking action that either duplicates existing work or that could have the effect of frustrating this work. That said, there are clear interactions between the actions we propose below and some of the initiatives already under way. In implementing our proposals, we will ensure any interactions are managed effectively.

Balancing security with convenience and innovation

8.7 Underlying the consideration of measures to tackle fraud in any payment system is the need to recognise that improved security measures could affect the extent to which payment systems provide users with fast, frictionless payments. Such measures could frustrate the user, for example by complicating the process for making payments or slowing down the time it takes for funds to reach the payee.

8.8 APP scams relate to only a small percentage of total push payments, with the vast majority of payments being completed without issue or dispute. When considering any potential action, we are sensitive of the need to minimise the harm experienced by a relatively small group of users (though significant to the individuals affected) that is caused by APP scams against the introduction of additional frictions that will adversely impact users of the large majority of payments that are made without incident.

The risk of creating adverse incentives

8.9 When considering potential changes to the liability model currently in place for APP scams, there is a need to understand the risk of any change creating adverse incentives for participants involved in a payment. For example, any change that results in consumers exercising less care in authorising push payments could result in an overall increase in the volume of APP scams. We explore this issue further in our discussion of Which?'s proposed remedies below.

The risk of creating unintended consequences

8.10 We are mindful of the potential for unintended consequences to be created by any actions we take. This is particularly the case when considering potential changes in liability for APP scams, but is also the case for any action that may introduce significant additional cost or risk to industry participants. For example, interventions that result in significant changes in cost or risk to PSPs could be met by a range of responses from the impacted PSPs, such as:

- an increase in the cost of payment services provided to consumers
- the withdrawal or scaling back of the supply of payment services to certain customer segments, for example those thought to be at particular risk of falling victim to APP scams
- the introduction of additional frictions to the use of payment services offered, or the scaling back in the capabilities of those services

8.11 There is also the risk that such changes would encourage behaviour that increases the scale of APP scams.

Our approach to addressing the issues identified

8.12 We have identified the following issues:

1. The ways in which PSPs currently work together in responding to reports of APP scams needs to improve.

2. There is some evidence to suggest that some PSPs could do more to identify potentially fraudulent incoming payments and to prevent accounts falling under the influence of scammers.

3. The data available on the scale and types of APP scams is of poor quality. Some of the initial evidence we have identified about the scale suggests that it may be significant and the general view held is that the prevalence of APP scams is likely to increase.

8.13 We have identified and agreed with FFA UK work that the banking industry should lead on:

- Industry, liaising with the ICO as appropriate, to develop a common understanding of what information can be shared under the current law, and any key legal barriers to sharing further relevant information (for example, information that would help victims recover their money).

- Industry 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 would expect this to cover issues such as availability of fraud specialists and processes for agreeing indemnity agreements.

- Industry to develop, collect and publish robust APP scam statistics, to address the lack of clear data on the scale and scope of the problem, and to enable monitoring of the issue over time.

8.14 We will monitor this work on an ongoing basis, and commit to review industry progress in the second half of 2017.

8.15 We will consider the potential for the operators of the CHAPS and FPS payment systems to play an expanded role in helping to minimise the consumer harm caused by APP scams. We will look to publish specific terms of reference for this work in early 2017 and look to publish the findings of our work in the second half of 2017. We envisage this work will include consideration of how internationally comparable push payment system operators are involved in minimising risk of consumer harm around APP scams and fraud more generally.

8.16 The FCA will undertake the following actions:

- work with firms to tackle concerns around both sending and receiving banks in relation to APP fraud

- evidence received in relation to the super-complaint will be examined by FCA supervision, which will address any firm-specific issues directly

- if, following the above steps, there are unresolved sector-wide issues, the FCA will initiate further work. Any such work should consider the developments made since the thematic review of banks' defences against investment fraud in 2012.[116]

8.17 Table 2 maps the issues we have identified to the actions that will be taken.

Table 2: Issues and proposed actions

Issue	Action	Follow-up action
Poor quality data available on the scale and types of APP scams.	Industry to develop, collect and publish robust APP scam statistics, to address the lack of clear data on the scale and scope of the problem.	PSR to monitor this work on an ongoing basis and commit to review industry progress in the second half of 2017.
The need for improvement in the ways in which PSPs currently work together to respond to reports of APP scams.	Industry, liaising with the 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. Industry 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 would expect this to cover issues such as availability of fraud specialists and processes for agreeing indemnity agreements between banks.	
Some evidence to suggest that some PSPs could do more to identify potentially fraudulent incoming payments and to prevent accounts falling under the influence of scammers.	FCA to work with firms to tackle concerns around both sending and receiving banks in relation to APP fraud. FCA supervisors will examine evidence received in relation to the super-complaint and address any firm-specific issues directly.	If, following these steps, there are unresolved sector-wide issues, the FCA will initiate further work. Any such work should consider the developments made since the thematic review of banks' defences against investment fraud in 2012.
	PSR will consider the potential for operators of the CHAPS and FPS payment systems to play an expanded role in helping to minimise the consumer harm caused by APP scams.	PSR will look to publish specific terms of reference in early 2017 and look to publish findings in the second half of 2017.

[116] Financial Services Authority (2012) *Banks defences against investment fraud: detecting perpetrators and protecting victims*, www.fsa.gov.uk/static/pubs/other/banks-defences-against-investment-fraud.pdf

8.18 In addition to the actions set out above, we emphasise the particular importance of the following developments already in train in further helping to address consumer harm caused by APP scams:

1. The work of the Payments Strategy Forum in developing confirmation of payee capabilities and on financial crime-related initiatives, in particular those related to financial crime intelligence sharing and payment transaction data sharing and analytics.

2. The work of the JFT, in particular its initiatives relating to recovering funds paid out as a result of scams, development of further public education campaigns, and its work on developing a strategic action plan for the treatment and protection of victims of fraud and vulnerable consumers.

Which?'s proposed options for intervention

8.19 In their super-complaint, Which? present two potential options for addressing the consumer harm caused by APP scams:

- **Option A**: Introduce changes that make PSPs liable for reimbursing victims of APP scams, except where the victim acted fraudulently or with gross negligence.

- **Option B**: Introduce risk management standards that PSPs must meet when executing authorised push payments. PSPs would be required to reimburse victims of APP scams in instances where they had not met these standards, except where the victim had acted fraudulently or with gross negligence.

8.20 Both options proposed by Which? would impose greater liability on PSPs for APP scams than they currently face under the Payment Services Directive (PSD), as implemented by the Payment Services Regulations 2009 (PSRs 2009), and the revised Payment Services Directive (PSD2).

8.21 We think that a wholesale shift in liability to PSPs that requires them to reimburse victims of APP scams, even with an exception where the victim has not acted fraudulently or with gross negligence, is inappropriate. We have observed little support for such a change through the course of investigating the issues raised in the super-complaint. However, some parties we have engaged with have presented more nuanced arguments that call for a shift in liability in certain circumstances to certain parties.

8.22 Making a recommendation to change the liability at the end of the 90-day process in which we have to respond would be unlikely to give proper consideration to all the potential policy and legal issues that may arise from such a decision. There are a number of possible detriments that would need to be considered.

8.23 A change in liability would likely create adverse incentives and could actually result in an increase in APP scams. This could manifest itself in several different ways:

- Consumers, knowing that PSPs faced complete liability for APP scams, could change their behaviour in ways that would make APP scams more common. For example, consumers could become less vigilant in their attempts to identify and prevent APP scams.

- There is also scope for an increase in so-called 'first-party fraud', whereby consumers could falsely claim they were victims of APP scams in instances where they were not in an attempt to gain false recompense from their PSP.

- Knowing that PSPs were liable for losses from APP scams could also embolden existing scammers and prompt new scammers to enter the market.

8.24 Such a change in liability would also likely result in changes in PSP behaviour that could have an adverse impact on consumers. Possible impacts include:

- PSPs may decide to increase the cost to consumers of making payments to recover the losses from increased liability.
- PSPs may decide to introduce additional hurdles and barriers to making payments, which would create inconvenience and friction for the large majority of payments that are currently made without issue.
- Faced with increased liability, PSPs may instead decide to withdraw from supplying certain market segments. This would result in disruption and reduced consumer choice.

8.25 Given there are a wide range of parties in addition to PSPs that have a role in preventing APP scams, an intervention that transfers liability entirely to PSPs does not appear to be appropriate where other solutions are available. These parties include consumers themselves but also, for example, companies whose legitimate products or technologies are used by scammers to enable APP scams (such as online trading platforms) and law enforcement.

8.26 The second potential intervention proposed by Which? would involve the introduction of risk management standards that PSPs must meet when executing authorised push payments. PSPs would be required to reimburse victims of APP scams in instances where they had not met these standards, except where the victim had acted fraudulently or with gross negligence.

8.27 We think there is some merit in this proposal. Indeed, the actions we are taking incorporate some characteristics of this proposal:

- We have asked industry 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 are of the view that this will contribute to the rapid recovery of funds lost to APP scams and also help reduce the stress faced by victims of APP scams.
- The work we are undertaking in considering the potential for payment systems to play an expanded role in preventing and responding to APP scams is also relevant.

8.28 We think that the programme of actions we have set out above, combined with the programme of work by other players already under way, will contribute to addressing the consumer harm caused by APP scams.

9 Annex 1: Glossary

Term or acronym	Description
Bacs	The regulated payment system which processes payments through two principal electronic payment schemes: Direct Debit and Bacs Direct Credit. The payment system is operated by Bacs Payment Schemes Limited (BPSL).
BPSL	Bacs Payment Schemes Ltd – the operator of the Bacs payment system.
British Bankers Association (BBA)	The BBA is a trade association for the UK banking sector.
CHAPS (Clearing House Automated Payment System)	The UK's real-time, high-value sterling regulated payment system, where payments are settled over the Bank of England's Real time Gross Settlement (RTGS) system. It is operated by CHAPS Co.
CHAPS Co	CHAPS Clearing Company Ltd – the operator of the CHAPS payment system.
Cifas	Cifas is a not-for-profit company working to protect businesses, charities, public bodies and individuals from financial crime.
Counter Terrorist Financing (CTF)	The package of initiatives and regulations directed at preventing terrorist financing, including the Terrorism Act 2000.
credit card transaction	A card-based payment transaction where the amount of the transaction is debited in full or in part at a pre agreed specific calendar month date to the payer, in line with a prearranged credit facility, with or without interest.
Crime Survey for England and Wales (CSEW)	The Crime Survey for England and Wales is an important monitor of the extent of crime in England and Wales. It is used by the government to evaluate and develop crime reduction policies, provides vital information about the changing levels of crime over the last 30 years.
Customer Due Diligence (CDD)	Also referred to as Know Your Customer (KYC) requirements. Certain regulated firms are required to carry out customer due diligence measures, which involve: (a) identifying the customer and verifying the customer's identity on the basis of documents, data or information obtained from a reliable and independent source (b) identifying, where there is a beneficial owner who is not the customer, the beneficial owner and taking adequate measures, on a risk-sensitive basis, to verify his identity so that the relevant person is satisfied that he knows who the beneficial owner is, including, in the case of a legal person, trust or similar legal arrangement, measures to understand the ownership and control structure of the person, trust or arrangement (c) obtaining information on the purpose and intended nature of the business relationship

Term or acronym	Description
debit card	A card enabling its holders to make purchases and/or withdraw cash and have these transactions directly and immediately charged to their accounts, whether these are held with the card issuer or not.
debit card transaction	A card-based payment transaction, including those with prepaid cards that is not a credit card transaction.
direct credit	A payment service for crediting a payee's payment account, with a payment transaction or series of payment transactions, from a payer's payment account, by the payment service provider which holds the payer's payment account, based on an instruction given by the payer.
direct debit	A payment service for debiting a payer's payment account, where a payment transaction is initiated by the payee on the basis of the payer's consent given to the payee, to the payee's payment service provider or to the payer's own payment service provider.
DPA	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.
Financial Action Taskforce (FATF)	An inter-governmental body which develops and promotes policies to combat money laundering and terrorist financing. Its website is: http://www.fatf-gafi.org/about/.
FCA	Financial Conduct Authority
Financial Fraud Action UK (FFA UK)	Financial Fraud Action UK (FFA UK) is the name the financial services industry uses to coordinate its fraud prevention activities.
Financial Ombudsman Service	The Financial Ombudsman Service is an ombudsman in the United Kingdom. It was established in 2000, and given statutory powers in 2001 by the Financial Services and Markets Act 2000, to help settle disputes between consumers and UK-based businesses providing financial services, such as banks, building societies, insurance companies, investment firms, financial advisers and finance companies.
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.
General Data Protection Regulations (GDPR)	The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Parliament, the Council and the European Commission intend to strengthen and unify data protection for individuals within the European Union (EU). It was published in the Official Journal of the EU on 4 May 2016. It will apply from 25 May 2018.
Information Commissioner's Office (ICO)	The UK's independent body set up to uphold information rights.
Joint Money Laundering Intelligence Taskforce (JMLIT)	JMLIT has been developed in partnership with the financial sector to combat high end money laundering. Its website is: http://www.nationalcrimeagency.gov.uk/about-us/what-we-do/economic-crime/joint-money-laundering-intelligence-taskforce-jmlit

Term or acronym	Description
Joint Fraud Taskforce (JFT)	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.
3rd EU Money Laundering Direction (MLD)	Directive 2005/60/EC of the European Parliament and of the Council of 26 October 2005 on the prevention of the use of the financial system for the purpose of money laundering and terrorist financing, published in the Official Journal of the EU on 25 November 2005.
4th EU Money Laundering Directive (MLD4)	Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC, published in the Official Journal of the EU on 5 June 2015.
Money Laundering Regulations 2007 (also known as MLRs 2007)	The Money Laundering Regulations 2007 (SI 2007/2157), which implements the third EU Money Laundering Directive (Directive 2005/60/EC) in the UK, as amended from time to time.
National Crime Agency (NCA)	The National Crime Agency (NCA) is a national law enforcement and police agency in the United Kingdom. It was established in 2013 as a non-ministerial government department, replacing the Serious Organised Crime Agency and absorbing the formerly separate Child Exploitation and Online Protection Centre (CEOP) as one of its commands.
National Fraud Intelligence Bureau (NFIB)	The National Fraud Intelligence Bureau (NFIB) sits alongside Action Fraud within the City of London Police which is the national policing lead for fraud.
'on us' transactions	Transactions where the payee's PSP/payer's PSPs are the same entity.
Office for National Statistics (ONS)	The Office for National Statistics (ONS) is the UK's largest independent producer of official statistics and is the recognised national statistical institute for the UK. It is responsible for collecting and publishing statistics related to the economy, population and society at national, regional and local levels.
Payment Account Directive (PAD)	Directive 2014/92/EU of the European Parliament and of the Council of 23 July 2014 on the comparability of fees related to payment accounts, payment account switching and access to payment accounts with basic features, published in the Official Journal of the EU on 28 August 2014.
Payment Account Regulations (PARs)	The Payment Accounts Regulations 2015 (SI 2015/2038), which implements the PAD in the UK.
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.

Term or acronym	Description
PSD (EU Directive on Payment Services)	Directive 2007/64/EC of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48/EC and repealing Directive 97/5/EC of 13 November 2007, published in the Official Journal of the EU on 5 December 2007.
PSD2	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, published in the Official Journal of the EU on 23 December 2015.
Payment service provider (PSP)	Any natural or legal person authorised to provide the payment services listed in the Annex to Directive 2007/64/EC or recognised as an electronic money issuer in accordance with Article 1(1) of Directive 2009/110/EC (PSD1).
Payment Services Regulations 2009 (PSRs 2009)	These regulations implement Directive 2007/64/EC of the European Parliament and of the Council on payment systems in the internal market (PSD1). They came into force for most purposes on 1 November 2009.
Payments Strategy Forum (PSF)	The Payments Strategy Forum was announced by the PSR in its Policy Statement published in March 2015. The Forum is leading on a process that identifies, prioritises and develops strategic, collaborative initiatives that promote innovation for the benefit of those who use payment systems. More information on the Forum may be found on www.paymentsforum.uk.
Payments UK (formerly known as Payments Council)	An industry trade association representing the UK payments industry. Historically, it was a membership organisation set up following the OFT's Payment Systems Taskforce, which included a focus on payment systems.
Phishing	Phishing is the attempt to obtain sensitive information such as usernames, passwords, and credit card details (and, indirectly, money), often for malicious reasons, by disguising as a trustworthy entity in an electronic communication.
Proceeds of Crime Act 2002 (POCA)	The Proceeds of Crime Act 2002 (POCA) sets out the legislative scheme for the recovery of criminal assets. It was given Royal Assent on 24 July 2002.
Payment Systems Regulator (PSR)	The Payment Systems Regulator Limited, the body corporate established by the FCA under section 40(1) of FSBRA.
Suspicious Activity Report (SAR)	A report made to the Serious Organised Crime Agency (SOCA) in respect of transactions or behaviour that give the financial institution grounds to know or suspect that the activity is linked to criminality. Sometimes also referred to as a disclosure.
the Treasury	Her Majesty's Treasury.
The Wire Transfer Regulations 2 (WTR2)	The Regulation of the European Parliament and of the Council on information accompanying transfers of funds – repealing Regulation (EC) No 1781/2006.
Vishing	Vishing is the act of using the telephone in an attempt to scam the user into surrendering private information that will be used for identity theft. The scammer usually pretends to be a legitimate business, and fools the victim into thinking he or she will profit.

10 Annex 2: Sources of evidence

The sources of evidence we rely upon in forming our response to the super-complaint are:

- meetings and calls with 40 external stakeholders (see Annex 3 for list) and, in some instances, further information provided to us by stakeholders subsequent to those meetings
- responses we received to our formal section 81 information requests (we issued information requests to six PSPs and six payment system operators)
- a written submission we received from FFA UK
- emails we received from members of the public into our super-complaint email inbox
- a survey of 2,096 UK adults on payment fraud, undertaken on our behalf by TNS
- additional evidence provided to us by Which?, including information collected through their online scams reporting tool
- desk research

11 Annex 3: Organisations we met with

The table below sets out with organisations we met or spoke with during the course of our work in responding to the super-complaint.

Category	Organisations
Payment system operators	Bacs Payment Schemes Ltd CHAPSs Co Faster Payments Scheme Ltd Mastercard Inc. Visa Europe
Payment service providers	Barclays Bank Plc HSBC Bank Plc Lloyds Bank Metro Bank Plc Nationwide Building Society Santander UK Plc Svenska Handelsbanken AB Royal Bank of Scotland
Trade associations and industry representatives	British Bankers Association The Conveyancing Association Financial Fraud Action UK Fraud Advisory Panel Payments UK Payments Strategy Forum Financial Crime Working Group
Consumer interest groups	Age UK Citizens Advice Bureau FCA Consumer Panel Money Advice Service Victim Support Which?
Government, regulators and law enforcement	Bank of England City of London Police Competition and Markets Authority FCA Financial Ombudsman Service Home Office Joint Fraud Taskforce Information Commissioner Office Ofcom Office for National Statistics Trading Standards
Other organisations	4Keys International Behavioural Insights Cifas PSR Panel VocaLink Ltd

12 Annex 4: Fraud prevention – legal and regulatory requirements

Further information on the application of the DPA 1998 and the duty of confidence in fraud prevention

12.1 The DPA 1998 requires PSPs to take appropriate measures to protect their customers' personal data.[117] It does so by setting down certain pre-conditions for the processing (including the sharing) of personal data, as well as a number of data-protection principles with which the PSPs are required to comply. If a PSP breaches the DPA 1998, it may be liable for damage, including for any resulting distress.[118] In addition, it may receive an enforcement notice from the Information Commissioner's Office (ICO), with which failure to comply is a criminal offence.[119]

12.2 There is no blanket rule which prevents a customer's PSP from sharing his or her information.[120] Instead, the DPA 1998 acts as a framework for information sharing, to ensure personal data is not shared inappropriately. **Personal data** is defined as data which relates to an individual (as opposed to a company or LLP) which allows a PSP to identify him or her (DPA 1998, Section 1(1)). This is likely to include customer names, and may include other information (such as telephone numbers) which enables the PSP to identify the individual in conjunction with other information held. IP addresses and cookies, described as 'non-obvious identifiers', can constitute personal data if the associated electronic device can be reliably linked to a particular customer.[121]

12.3 A PSP must identify certain **conditions** in order to process personal data**.** A full list of those conditions can be found in the DPA 1998, Schedule 2. Potentially relevant conditions include:

- **Customer consent**[122]**:** Any consent must be a '*freely given specific and informed indication of his wishes by which [the customer] signifies his agreement…'.*[123] The ICO Data Sharing code of practice indicates that customers must know '*precisely what data sharing they are consenting to and understand its implications for them'* and must have '*genuine control over whether or not the data sharing takes place'.*[124] The ICO guide to data protection also indicates that there must be '*some active communication'* between the PSP and its customer and that the former should not infer consent.[125] In any event, the likelihood of a scammer consenting to the use of his or her data is low and consent can be withdrawn at any time.[126]

[117] The DPA 1998 brought into effect Council Directive 95/46/EC.
[118] DPA 1998, Section 13.
[119] DPA 1998, Section 40 and Section 47.
[120] Though any PSO or other PSP not in a contractual relationship with the individual is prohibited from disclosing information shared to them without the customer's PSP's consent: DPA 1998, Section 55.
[121] See ICO personal information online code of practice (page 32). In the case of C-582/14 *Patrick Breyer v Bundesrepublik Deutschland*, the CJEU held that 'dynamic IP addresses' could be personal data.
[122] DPA 1998, Schedule 2, Section 1.
[123] European Data Protection Directive, Article 2(h).
[124] ICO Data Sharing code of practice, page 15.
[125] ICO Guidance on Data Protection (page 101). This accords with the common law approach under *Interfoto Picture Library Ltd v Stiletto Visual Programmes Ltd* [1989] QB 433.
[126] ICO's Guide to Data Protection, page 102.

- **Disclosure is necessary for a specified purpose:** Those purposes include:
    - the individual's contract (or required in order to enter into it)
    - a legal obligation, or
    - a 'legitimate interest'[127]

12.4 Fraud prevention and detection, in certain circumstances, may fall into the 'legitimate interest' category.[128] Importantly, however, this alone is insufficient to share '**sensitive personal data**'.[129] This includes personal data relating to the (alleged) commission of an offence.[130] Before a PSP can consider sharing personal data on the (alleged) commission of a fraud, in addition to satisfying one of the conditions for processing above, it would have to ensure it had also satisfied one of the conditions in the DPA 1998, Schedule 3, which apply to sensitive personal data.

Potentially relevant conditions include:

- **explicit** consent – as noted above, it may be unlikely that a scammer would provide this consent and any consent previously given can be withdrawn[131]
- disclosure is in the substantial public interest, is necessary for the prevention or detection of any unlawful act **and** must necessarily be carried out without explicit consent[132]
- disclosure is in the substantial public interest, is necessary for the discharge of any function designed for protecting members of the public against dishonesty or improper conduct **and** must necessarily be carried out without explicit consent[133]
- disclosure was to a specified anti-fraud organisation (SAFO), such as Cifas, and is necessary or the purpose of preventing fraud[134]

[127] DPA 1998, Schedule 2, Sections 2, 3, 5(a), 5(d) and 6.
[128] See ICO meeting notes from second meeting.
[129] ICO Data Sharing code of practice (page 16).
[130] DPA 1998, Section 2(g).
[131] DPA 1998, Schedule 3, Section 1.
[132] The Data Protection (Processing of Sensitive Personal Data) Order 2000, Section 1.
[133] Ibid, Section 2.
[134] DPA 1998, Schedule 3, Section 7A.

12.5 Once those conditions are satisfied, the PSP is required to share information only in accordance with the **data protection principles**[135], which:

- Require them to obtain personal data for **lawful and specified purposes** only[136]; to process personal data **fairly**[137]; to ensure personal data processed is relevant and **not excessive**[138], is **accurate** and up to date[139], and is **not kept longer than necessary**[140]; and to maintain **appropriate technical and organisational measures** to protect data.[141] The ICO recommends the use of privacy notices to indicate what information is going to be collected and how it will be shared.[142]

- Give **customers the right to access their data**.[143]

12.6 However, the legislation also includes a number of exemptions. For example, there is an exemption from some of the obligations under the DPA if it is **necessary**[144] for '***the prevention or detection of crime'***, where applying the DPA would otherwise '*be likely to prejudice'* that aim.*[145]* Where the crime exemption applies, an organisation will be exempt from complying with the first data protection principle (though it must still be able to establish a condition for processing under Schedule 2 and, where it applies, Schedule 3). It will also be exempt from complying with a subject access request by an individual who is seeking access his or her data.[146]

12.7 However, in its guidance on using the crime and tax exemptions, the ICO has stated that organisations may not be able to rely on the exemption in the absence of '*specific evidence of potential criminal activity'* or as part of *'a blanket policy*', as prejudice must be established on a '*case by case basis*'.[147] A PSP would therefore have to consider each case on its merits.

[135] DPA 1998, s.4(4); Schedule 1, Part 1 and Part II.
[136] DPA 1998, Schedule 1, Section 2.
[137] DPA 1998, Schedule 1, Section 1.
[138] DPA 1998, Schedule 1, Section 3.
[139] DPA 1998, Schedule 1, Section 4.
[140] DPA 1998, Schedule 1, Section 5. See also C-131/12 *Google Spain SL and Google Inc v Agencia Espanola de Proteccion de Datos and Gonzalez* [2014] QB 1022.
[141] DPA 1998, Schedule 1, Section 7.
[142] See further: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/
[143] Personal Data must be 'processed in accordance with the rights of the data subject': DPA 1998, Schedule 1, Section 6. An individual is normally entitled: (a) to make a 'subject access request', for disclosure of his or her personal information which the PSP holds (DPA 1998, Section 7); (b) to issue a 'data subject notice' prohibiting the PSP from processing his or her personal data (DPA 1998, Section 10); and (c) to apply for a court order to require the PSP to rectify or delete his or her personal information (DPA 1998, Section 14).
[144] The word 'necessary' does not appear in DPA 1998, Section 29 itself. However, the courts have recently confirmed that the provision must be read in light of Article 13 of the parent Directive, for which the exemption must be a 'necessary measure': *Guriev v Community Safety Development (UK) Ltd* [2016] EWHC 643 (QB) (6 April 2016, unreported).
[145] DPA 1998, Section 29. See also *R (Lord) v Secretary of State of the Home Department* [2003] EWHC 2073 (Admin); [2004] Prison L.R. 65.
[146] ICO guidance on exemptions: https://ico.org.uk/for-organisations/guide-to-data-protection/exemptions/
[147] ICO guidance on using the crime and taxation exemptions (page 4, paragraph 10 and page 11, paragraph 35), respectively.

12.8 Where PSPs wish to share data on an ongoing basis, the ICO suggests that, instead of relying on an exemption, they should consider entering a **data sharing agreement** to regulate their cooperation.[148] Such an agreement is not itself an exemption or indemnity against claims against the PSPs under the DPA 1998, but is likely to encourage good practices.[149] The ICO's guidance also suggests that it would be advisable for PSPs to conduct a **privacy impact statement** if they intend to share information systematically.[150]

12.9 Turning to the duty of confidentiality, bankers owe a duty of secrecy to their customers. The duty covers a range of information that is beyond the scope of the DPA 1998. The DPA 1998 only limits the processing of 'personal data', which is data which relates to an individual and enables the PSP to identify him or her. In contrast, the duty of confidence covers:

- corporations and LLPs
- all information acquired at a time when the customer-banker relationship was in existence[151]

12.10 There are, however, recognised exceptions to the duty. These include where the duty of confidence comes into conflict with a duty owed to the public. There is limited case law in this field, though the courts have held that the public interest in aiding foreign fraud proceedings could override the duty of confidence owed to a customer.[152] In the leading case on banking confidentiality, *Tournier v National Provincial and Union Bank of England*, the Court indicated that a bank could disclose a customer's confidential information '*to prevent frauds or crimes'*.[153]

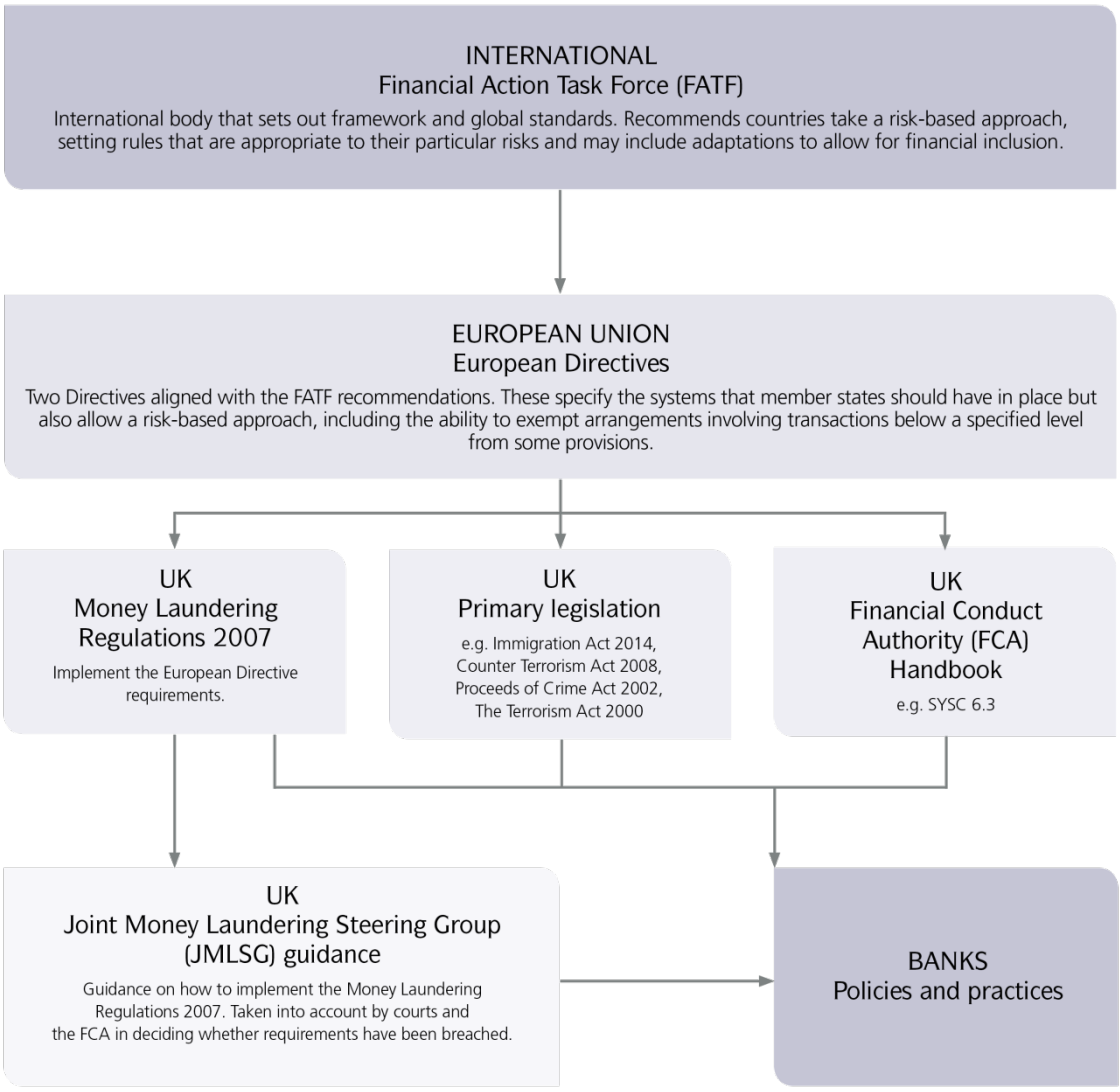
Preventing fraud: obligations of the PSPs

AML, KYC checks and POCA reporting

12.11 PSPs are under a range of obligations the aim of which is the prevention of crime. Amongst these are the PSPs' **Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) requirements and Know Your Customer (KYC) checks**. The Proceeds of Crime Act 2002 (POCA 2002) introduced a number of money laundering offences, for example, for transferring, concealing or acquiring criminal property or assisting in the retention of the proceeds of crime.[154] Obligations not to facilitate money laundering stem from a variety of sources[155], shown in Figure 5 below.

[148] The ICO Data sharing code of practice (page 26).
[149] The ICO Data sharing code of practice (page 41).
[150] See further the ICO's Conducting privacy impact assessments code of practice, available: https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf. See also the ICO Code on Privacy notices, transparency and control, available: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/
[151] Ibid, per Scrutton LJ at [481].
[152] *Pharaon v Bank of Credit and Commerce International SA (in liquidation)* [1998] 4 All ER 455.
[153] *Tournier v National Provincial and Union Bank of England* [1924] 1 KB 461, at [474].
[154] POCA 2002, Sections 327, 328 and 329.
[155] Most recently, see the Immigration Act 2014 (Current Accounts) (Compliance etc.) Regulations 2016. Under the Immigration Act 2014, PSPs are not allowed to open a current account where the prospective customer is known to be an illegal migrant and are required to shut such an account even in the absence of a court order. Under the Regulations, the Secretary of State will provide PSPs with information to facilitate this and, from 2018, the PSPs will be required to conduct quarterly immigration checks.

Figure 5: Anti-money laundering requirements in the UK



Source: FCA (2016) *Occasional Paper 17 – Access to Financial Services in the UK*, https://www.fca.org.uk/publication/occasional-papers/occasional-paper-17.pdf
Note: Not all of the above requirements apply to all types of PSP (e.g. SYSC6 does not apply to all PSPs).

12.12 **The Money Laundering Regulations** 2007 (MLRs) implement the Directive on the Prevention of the Use of the Financial System for the Purpose of Money Laundering and Terrorist Financing (3rd Money Laundering Directive).[156] They set out the procedures PSPs are required to put in place and follow to avoid the facilitation of money laundering. If a PSP does not comply with the MLRs, it (and its officers) may have committed a criminal offence.[157]

[156] Directive 2005/60/EC. See also the FCA Handbook, SYSC 6.3.4.
[157] MLRs, Regulation 45(1).

12.13 The MLRs contain the following requirements:

- **Customer due diligence**[158]**:** PSPs must conduct due diligence checks both when they establish a business relationship[159] and for 'occasional transactions' worth £15,000[160] or more.[161] They must also conduct due diligence when they suspect money laundering or terrorist financing, when they have doubts as to a customer's previously ascertained identity, or when necessary for existing customers (for example, a change of circumstances).[162] If they cannot do so, they are not allowed to enter into a business relationship with customers, must terminate any such existing relationship and must not carry out transactions for them.[163] In practice, a PSP must:
    - **Identify the customer and verify identity from a reliable source**[164]**:** It is preferable that the PSPs verify identity before the account is opened, though this stage can take place afterwards so long as safeguards are put in place to ensure that the account is not closed and no transactions take place in the interim.[165]
    - **Identify any beneficial owner**[166]**:** In some circumstances, the equitable rights in property will lie with someone other than the customer, and that person or company may exercise a degree of control over the customer.[167] A PSP is required to take 'adequate measures' in verifying the identity of any such person and is expected to take a 'risk-based approach'. However, it is not currently[168] obligated to check this against information from a reliable and independent source.
    - **Find out information on the purpose and nature of the customer's intended relationship with the PSP.**[169]
    - **Monitor the business relationship on an ongoing basis**: The PSP must check, for example, that the customer's transactions are consistent with what the PSP knows about him or her and reporting suspicious transactions.[170]
    - **Adapt its due diligence:** The PSP must do this in certain circumstances where appropriate.[171]
- **Record keeping:** A PSP is required to maintain records of a customer's identification documents and any other documents used for due diligence purposes for at least five years from the customer's last transaction or the end of the business relationship.[172]

[158] MLRs, Regulation 5.
[159] A business relationship exists if both the PSP and customer expect it to be ongoing. Information that the PSPs will seek includes employment details, the source of funds used and recent financial statements.
[160] MLRs, Regulation 2(1). However, this sum may arise from 'linked transactions', where a large sum has deliberately been broken down into smaller sums for the purpose of avoiding due diligence checks.
[161] MLRs, Regulation 7.
[162] MLRs, Regulation 7.
[163] MLRs, Regulation 11.
[164] MLRs, Regulation 5(a).
[165] MLRs, Regulation 9.
[166] MLRs, Regulation 5(b).
[167] See MLRs, Regulation 6 for a definition of 'beneficial owner'.
[168] Stricter verification requirements for discretionary trustees and public access requirements for beneficial owners will be implemented with the 4th Anti-Money Laundering Directive, discussed in Chapter 6.
[169] MLRs, Regulation 5(c).
[170] MLRs, Regulation 8. See also the Joint Money Laundering Steering Group (2014) Guidance, 2014, Part 1, paragraph 5.1.9).
[171] MLRs, Regulations 13 and 14, and Schedule 2.
[172] MLRs, Regulation 19.

- **Policies, procedures and training:** A PSP is required to adopt risk sensitive policies and procedures related to customer due diligence[173] and to train staff on a regular basis on the law in this field and how to spot money laundering.[174]

12.14 The FCA's Handbook also reflects many of these requirements.[175] For example, certain PSPs[176] (banks) are required to have adequate policies and procedures to counter the risk that they might be used for financial crime (including fraud).[177] Those PSPs are also required to ensure money laundering is taken into account in their day to day operations, including in its decisions as to whether to develop new products and take on new customers.[178] Senior management will have operational responsibility for making sure the PSP has systems in place to manage and combat financial crime, and should allocate a director or senior manager who has overall responsibility for this.[179] An individual must also be appointed as the PSP's money laundering reporting officer (MLRO).[180] The Handbook also indicates that, in determining compliance, the FCA will have regard to whether the PSPs in question followed the **Joint Money Laundering Steering Group Guidance**.[181] Further detail of the PSPs' financial crime obligations can be found there.

12.15 In addition to their AML and KYC obligations, PSPs are also under a duty to report financial crime. Under POCA 2002, a person commits an offence if he or she:[182]

- **knows or suspects** (or has reasonable grounds for knowing and suspecting) that another person is engaged in money laundering
- came by the information upon which that knowledge or suspicion (or the reasonable ground for such knowledge or suspicion) is based in **the course of business**
- **can identify the person suspected of money laundering or the criminal property** in question (or that he or she believes, or it is reasonable to believe, that the information will assist in such identification)
- **fails to disclose** the identity of the person or the location of the criminal property (or the information upon which his or her suspicion is based) **either internally to the nominated person or externally to the NCA as soon as is practicable**

12.16 PSPs and their employees can avoid criminal liability if:

- they have a reasonable excuse for not making a disclosure[183]
- as an employee, they did not receive suitable training and did not in fact have any knowledge of suspicion of money laundering[184]

[173] MLRs, Regulation 20. See also FCA Handbook, SYSC 6.3.1. and SYSC 6.3.3.
[174] MLRs, Regulation 21. See also FCA Handbook, SYSC 6.3.7(1).
[175] FCA Handbook, SYSC 6.3. See also the FCA's guidance entitled 'Financial Crime: A Guide for Firms', which offers practical assistance and information on money laundering prevention for PSPs.
[176] The SYSC provisions of the FCA Handbook do not apply to all PSPs, but instead only applies to firms with Part 4A permissions (e.g. deposit takers).
[177] FCA Handbook, SYSC .1.1R.
[178] FCA Handbook, SYSC 6.3.7(4).
[179] FCA Handbook, SYSC 6.1.1 and 6.3.8.
[180] FCA Handbook, SYSC 6.3.9.
[181] FCA Handbook, SYSC 6.3.5.
[182] POCA 2002, Section 330. See also related offences for 'nominated officers' within a PSP.
[183] POCA 2002, Section 330(6)(a).
[184] POCA 2002, Section 330(7).

12.17 Where an employee made an internal report to the PSP's MLRO, it is an offence for the MLRO not to make a Suspicious Activity Report (SAR) to the National Crime Authority as soon as is practicable where, as a result of the internal report, he or she knows of or suspects money laundering.[185] The government's guidance[186] on this suggests that a delay may be acceptable where '*it is not practical – or not safe – to suspend the transaction',* in which case the SAR should be made '*as soon as possible after the transaction is completed'.* Again, the MLRO may be able to rely on the reasonable excuse defence.[187]

Obligations under the common law and PSRs 2009

12.18 As noted above, a PSP is obliged not to exercise a payment instruction where it is on notice that an agent of the customer is misappropriating funds.[188] In addition, the PSRs 2009 introduce a number of obligations on PSPs that, from a practical perspective, reduce the scope for potential fraud. Notably, PSPs are required:[189]

- to ensure that the safety features of a payment instrument cannot be accessed by someone other than the customer
- not to send unsolicited payment instructions, except in cases of replacement
- to establish and maintain appropriate means for the customer to notify it of loss, theft, misappropriation or unauthorised use of a payment instrument; those means must be available at all times
- to ensure a payment instrument cannot be used after a customer has notified it of any fraudulent activity

Preventing fraud: the customer's obligations

12.19 Finally, customers owe PSPs a limited duty of care not to facilitate fraud. In practice, this means the customer must:

- Refrain from making a payment order or drawing a cheque in a way that will facilitate fraud or forgery.[190] What that means in practice will depend on the circumstances of the case.[191]
- Inform the PSP of any fraud on the account as soon as he or she becomes aware of it.[192]

12.20 Beyond this, at common law, the courts have rejected any extension of the customers' obligations. For example, there does not appear to be any general obligation on a customer to manage a business in a way that will prevent fraud, or to check his or her accounts at certain intervals.[193]

[185] POCA 2002, Section 331.
[186] HM Revenue and Customs. *Money Laundering Regulations: report suspicious activities.* https://www.gov.uk/guidance/money-laundering-regulations-report-suspicious-activities
[187] POCA 2002, Section 331(6).
[188] *Barclays Bank plc v Quincecare Ltd* [1992] 4 All ER 363, per Steyn J at 3783B-J; *Lipkin Gorman v Karpnale Ltd* [1992] 4 All ER 409.
[189] PSRs 2009, Regulation 58(1).
[190] *London Joint Stock Bank Ltd v Macmillan* [1918] AC 777.
[191] See, for example, *Slingsby v District Bank Ltd* [1932] 1 KB 544.
[192] *Greenwood v Martins Bank Ltd* [1933] AC 51. This is replicated in the PSRs 2009, Regulation 59.
[193] *Tai Hing Cotton Mill v Liu Chong Hing Bank Ltd (No.1)* [1986] AC 80.

12.21 The customer's obligations at common law are now largely replicated in the PSRs 2009.[194] In addition, the customer has a number of obligations, related to any use of a 'payment instrument', which are designed to prevent fraud. A payment instrument is any personalised device or personalised set of procedures agreed between the PSP and its customer to initiate payments. They include (but are not limited to) cards, credit transfers and direct debits. As noted above, a customer will be liable under the PSRs 2009 for losses arising from the unauthorised use of a payment instrument if he or she has, intentionally or with gross negligence,[195] failed to comply with statutory obligations. The customer is required to:

- act in accordance with the terms and conditions of any payment instrument[196]
- inform the PSP '*without undue delay*' if he or she realises the instrument has been lost, stolen, misappropriated or used without authorisation[197]
- take '*all reasonable steps*' to keep the security features of the payment instrument secure[198]

[194] See PSRs 2009, Regulation 59.
[195] If a customer's conduct amounts to 'gross negligence', but there is no element of culpability on his or her part, he or she will only be liable for the first £50 lost: PSRs 2009, Regulation 62.
[196] PSRs 2009, Regulation 57(1)(a).
[197] PSRs 2009, Regulation 57(1)(b).
[198] PSRs 2009, Regulation 57(2).

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