FINANCIAL CONDUCT AUTHORITY
PAYMENT SYSTEMS REGULATOR

CP17/2 Annexes

Authorised push payment scams

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

Annexes

November 2017

Contents

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

Annex 1
List of consultation questions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annex 2
Practices in other UK payment systems

2.1 As part of our work programme on authorised push payment (APP) scams, we have considered whether the role of payment system operators could be expanded to minimise the harm of APP scams. To inform our thinking on this, we have considered what practices for fraud and other disputed payments are used in UK payment systems.

2.2 In this annex we specifically consider the practices of:

- Mastercard and Visa, the largest four-party card payment systems
- Bacs
- the new cheque Image Clearing System (ICS)
- Faster Payments Scheme (FPS) and CHAPS
- other proprietary payments systems and overlay services, such as PayPal and Paym

2.3 We then discuss how these practices could inform the approach to reducing harm from APP scams.

Card systems (Mastercard and Visa)

2.4 The Mastercard and Visa card systems enable consumers to make pull payments using credit, debit and prepaid cards. These systems operate a four-party model, involving:

- the consumer (the cardholder)
- the card issuer (the consumer's payment service provider (PSP))
- the acquirer (the merchant's PSP)
- the merchant offering goods and services

To make a purchase, the consumer gives the merchant their card details and permission to draw funds from their account.

2.5 This four-party model for cards creates a more limited network of payees than FPS and CHAPS, because only merchants can receive pull payments.[1] In FPS and CHAPS, push payments can also be made from consumer-to-consumer.

2.6 Mastercard and Visa have rules and processes in place to help prevent fraud and that allow cardholders that are victims of fraud to seek redress (known as the chargeback process). In the UK, there are legal requirements to provide redress in certain circumstances (for example, under section 75 of the Consumer Credit Act 1974).[2] However, we find that Mastercard and Visa's fraud prevention and redress practices typically go beyond this minimum legislative protection. This may reflect the pressure on these operators to compete for customers – which gives them an incentive to maintain the integrity of their brand so that cardholders feel secure using them.

1 Mastercard and Visa have developed the ability to make consumer-to-consumer and business-to-consumer push payments across their systems. These products are referred to as 'MasterCard Send' (which is not yet available in the UK, but is planned for implementation in 2018), and Visa Direct (which has just been launched in Europe).

2 Payment Systems Regulator (December 2016) *Which? authorised push payment super-complaint:* our response, page 31: www.psr.org.uk/psr-publications/news-announcements/which-super-complaint-our-response-Dec-2016

2.7 The majority of fraud against cardholders is unauthorised fraud and many of the card systems' fraud prevention practices are focused on detecting and preventing this type of fraud. The operators have rules requiring issuers and acquirers to use fraud prevention practices. In our view the chargeback rules and processes also give parties an incentive to meet certain responsibilities related to these fraud prevention practices.

2.8 We note the requirements and processes set out in the schemes' and systems' rules focus on the issuers and acquirers. They are the members of the card system and are directly subject to these rules, including the chargeback process. Issuers and acquirers can, and do, incorporate elements of the requirements and responsibilities into their contracts with their cardholders and merchants, respectively, so that all parties bear some responsibility for preventing fraud.

2.9 In the remainder of this section, we set out an overview of certain fraud prevention practices that card issuers and acquirers are required to follow. We then outline the chargeback process used in the four-party card payment model. We note that this is not an exhaustive list of practices used.

Fraud prevention practices – card issuers

2.10 When a consumer makes a card payment, the acquirer typically sends the card issuer a request to authorise the payment. The issuer is required to have tools in place to detect fraudulent payments in these circumstances. It is also required to have processes in place to make a decision whether to authorise the payment. This decision can incorporate information gathered by fraud detection tools.

Fraud detection tools (transaction scoring)

2.11 Card issuers typically use 'transaction scoring' tools to help detect fraud. They can buy these tools from specialist third-party suppliers, or from Visa and Mastercard themselves. The tools may use information about the payment transaction (generated in the authorisation message from the merchant), and can also use other data specific to that tool, to generate a score indicating how likely the payment is to be genuine. Scores are often within a range – for example, 0 to 999 – with higher scores showing a greater likelihood of fraud. Issuers decide the score and other criteria at which they will accept transactions.

2.12 Scoring tools may focus on measuring how likely the person making the transaction is to be genuine or how likely the transaction is to be genuine. Some use machine learning on large datasets of transactions to detect new and existing fraudulent behaviours. Different tools have access to different scopes and sizes of datasets of transactions. In some cases, the tools will be hosted on a card issuer's own systems and use additional information that the issuer has about the customer's previous history and known activities to augment the authorisation message. Scoring tools and models are confidential, to prevent criminals finding ways to commit fraud without generating a high fraud score.

2.13 The tools offered by the operators analyse network-level transaction data processed by Visa or Mastercard for centralised scoring that the issuers can use. PSPs that are direct participants in the systems report fraudulent transactions to the operator. In Mastercard, this information is incorporated into the operator's tools to help identify new patterns of fraud.

2.14 The tools offered by the operators may be beneficial to some issuers, especially those that are relatively small and do not have a significant level of transactions on their own. Tools that draw on network-level transaction data can give these issuers a more meaningful scoring model than they might be able to establish using their own transactions.

2.15 Other issuers may choose to procure a detection tool to be implemented directly on their own systems. This may be beneficial if they issue cards for more than one card system and gain value from looking at their combined set of transactions. In addition, issuers' own tools can incorporate the information that issuers have about their customers, which may provide additional benefit.

2.16 Some issuers may have an in-house detection tool and also use a centralised scoring tool. This could make them more resilient against small differences between algorithms, or potential internal system failings.

Decision-making systems

2.17 Issuers use automated decision-making systems to decide whether they will authorise a transaction or reject it. These decision systems may incorporate the transaction scores from the fraud detection systems. Issuers will also take other factors into account, such as whether the customer has sufficient funds or credit available in their account.

2.18 [✂]

2.19 Mastercard has developed a product, Mastercard Safety Net, to sit behind card issuers' own decision-making systems and add an extra layer of protection from significant levels of unauthorised payment fraud. The product could help if card issuers' internal systems for monitoring, alerting, and limiting unusual or extreme account activity should fail. The Mastercard system would flag and stop this activity. [✂]. This service has been mandatory for all issuers since April 2017.

Fraud prevention practices – acquirers

2.20 Acquirers have a role to play in ensuring that a card payment has been appropriately authenticated. Acquirers are also responsible for monitoring their merchants to help identify where they may be acting fraudulently. We discuss authentication and monitoring in the following sections.

Authentication tools and processes

2.21 In the card systems, there are certain tools and processes for authenticating cardholders. These include:

- **Chip and PIN:** Each debit and credit card has a microchip on it and a personal identification number (PIN) associated with it. When you put the card into a chip reading terminal, you have to enter the correct PIN for the transaction to be authorised. Because of the nature of the hardware required, this is only used for physical point-of-sale transactions.
- **3D Secure for internet purchases:** These are products such as Verified by Visa and Mastercard Identity Check (previously called SecureCode) and require a customer authentication step for card-not-present purchases over the internet. This is typically a password or a one-time code sent by text or email, to be entered on screen to authenticate.
- **CVC (also known as card verification value, CVV or CVV2):** The card verification code (CVC) is the number printed on the signature strip on the back of a card. For CNP transactions, this code is a way to verify that the customer making the purchase has physical ownership of the card. [✂].
- **Address Verification Services (AVS):** For CNP transactions the address of the account holder can also be checked as part of the authorisation, but it is typically up to the merchant whether or not to proceed.

2.22 The chargeback rules incentivise the use of certain secure authentication tools by influencing where liability sits in a disputed transaction (see below). [✂]. Where liability is allocated to acquirers, they may pass this on to the merchants through the commercial contract in place between them.

2.23 [✂].

Monitoring merchants' activity

2.24 To protect against harmful merchant activity, Mastercard and Visa require acquirers to carry out due diligence checks on merchants before entering into an acquiring relationship with them. [✂]. The acquirer has an incentive to perform these checks as it may be ultimately liable for the merchant's actions.

2.25 Mastercard and Visa also require acquirers to have processes for monitoring merchants' performance; operators can review merchants' activity as a secondary step in certain circumstances. Among other reasons, this may be done to detect fraudulent activity. Where an operator finds problems with a merchant, it may require the acquirer to take specified actions. [✂].

2.26 High ratios of chargebacks can indicate potentially fraudulent activity at a merchant. If a merchant consistently has a high ratio of chargebacks, then the operator may levy additional fees on the merchant's acquirer. [✂]. In our view, the use of additional fees gives the acquirer an incentive to ensure its merchants are acting appropriately and are using sufficient fraud prevention practices to help reduce the number of chargebacks at that merchant, and in the system.

Chargeback process (cardholder redress)

2.27 Mastercard and Visa have rules and processes in place that allow cardholders to seek redress if they believe that they have suffered a financial loss when making a purchase due to, for example, fraud. This is known as the chargeback process. A cardholder can dispute a transaction for a number of reasons. These include fraudulent transactions – where the cardholder never authorised the payment, or they authorised the payment but the merchant never delivered the goods or services (a fraudulent merchant). It also includes other disputed payments – for example, where the goods and services received were not as expected. [✂].

2.28 If a cardholder wants to dispute a payment, they report it to their card issuer. The issuer investigates the complaint and decides whether to refund the cardholder. If the cardholder reports suspected fraud on their card, the issuer generally has to refund the cardholder the whole transaction amount immediately, according to the rules, before the issuer has completed their investigation. The cardholder may not be refunded if they had been negligent or had acted fraudulently. For any disputed transaction, if the issuer believes that the cardholder has a case, the issuer can initiate a chargeback to recover funds from the acquirer.

2.29 When a chargeback is initiated, the chargeback rules ultimately determine which party – the issuer or the acquirer – is liable for the redress. The acquirer may be able to pass this liability on to the merchant in line with its commercial agreement with the merchant. The liability generally depends on whether the parties meet certain responsibilities set out in the rules, such as whether the acquirer's merchant used certain secure authentication measures.

2.30 The rules include guidance to determine how the issuer and acquirer can come to an agreement as to the liability of the dispute. If an issuer and acquirer cannot agree, they can send their dispute to the operator for arbitration. The operator will consider the case and then has the final ruling on which party is liable. We therefore find the chargeback processes have a dispute resolution mechanism in place where the operators act as the arbitrator.

Bacs system

2.31 The Bacs system supports both Bacs Direct Debit and Bacs Direct Credit payments.

2.32 A Bacs Direct Debit is a pull payment. It is an instruction from a payer to their PSP authorising a third party organisation (for example, a utility company) to collect varying amounts from their account as long as the payer is given advance notice of the collection amount and collection date. For these payments, there is a Direct Debit Guarantee (DDG) in place. Under the DDG, the payer is entitled to a refund if there has been an error in the payment of a Direct Debit, for example:

- if the payer did not authorise the Direct Debit in question
- the collecting organisation did not comply with the Direct Debit scheme rules – for example, it took more than the billing amount advised in the pre-notification to the payer

The DDG only covers the payment process and cannot be used to address contractual disputes over the delivery of goods or services.

2.33 Under the DDG, the payer's PSP will refund the payer if it is satisfied that they have a valid refund claim. The payer's PSP will then recover the money from the collecting organisation, typically by submitting a claim through Bacs' infrastructure. The collecting organisation may, in some circumstances, be able to 'challenge' the payer's PSP regarding the legitimacy of the refund request, by providing additional information to the payer's PSP to support its challenge. However, there is no dispute resolution mechanism, so if the payer's PSP does not accept the challenge then the collecting organisation must settle the refund claim.

2.34 The collecting organisation's PSP underwrites the liability of the organisation (its customer), so if the organisation becomes unable to meet its obligations in respect of reimbursing the payer's PSP, then the organisation's PSP would have to do so.

2.35 Their potential to be liable gives collecting organisations' PSPs an incentive to carefully vet organisations that want to offer Direct Debit as a payment option. Likewise, organisations have an incentive to check that their customers (payers) are who they say they are and have the appropriate authority to set up Direct Debits.

2.36 Similar to the chargeback process used in cards, the DDG allows consumers to feel secure in using Direct Debit as a payment method, by offering reimbursement where they have acted appropriately but there has been an error made by their PSP or by the collecting organisation. It also provides some incentives for the parties (specifically the PSPs and the collecting organisations) to adhere to scheme rules and standards when setting up payers who want to pay using Direct Debit, which can help prevent fraud. Over the last two years, Bacs has implemented new rules and guidance aimed at improving the refund claim process of the DDG and the validation of refund requests. We have been liaising with the operator of Bacs with regard to monitoring the effectiveness of these measures and making further improvements, if necessary.

2.37 The other Bacs payment service – Bacs Direct Credit – is a type of push payment. These days these payments are almost exclusively initiated by business and governments, rather than by consumers. There is a practice in place for handling accidentally misdirected Bacs Direct Credit payments: the Credit Payment Recovery Operating Guide, which is also used for misdirected FPS payments. See paragraph 2.45 below for more details.

Cheque Image Clearing System

2.38 Despite its relative low occurrence, cheque fraud has always been a concern in the Cheque and Credit Clearing system. Cheques can be counterfeited (all of the cheque is fake including the paper), forged (not completed or authorised by the payer), or the value or the payee details on the cheque can be altered by a fraudster. Some scams that are similar to APP scams can be perpetrated via cheques. For example, maliciously redirected scams can occur where a fraudster has changed the payment details on an invoice for a legitimate business, unknowingly to the payer when they give consent for the payment. The other example is scams where the payer is tricked into buying goods or services from a fraudster, such as paying a deposit on a holiday property that does not exist.

2.39 Scams may currently be more difficult to perpetrate with cheques because it takes a longer time for the funds to be transferred (currently 2 days after being paid in but only available after 4 days) than for real-time FPS and CHAPS payments. With cheques there is a risk that the payer or their PSP becomes aware of the scam in time to prevent payment.

2.40 However, the introduction of the new cheque Image Clearing System (ICS) in the UK will significantly reduce the time to clear cheques. The ICS allows payees to take an electronic image of the cheque in order to deposit it. The image is sent to the payer and payee's PSPs almost immediately, with the funds settling the following working day. The operator and participants recognise that this could lead to a rise in fraud and scams perpetrated using cheques. However, there are aspects of the new functionality of the ICS system that allow for greater fraud protection capabilities:

- Imaging cheques allows a cheque to be analysed against previous cheques drawn on any account. [✂].
- [✂].
- Information on cheques can be passed to both the sending and receiving PSP almost immediately; this would allow, for example, the receiving PSP to spot fraudulent patterns on accounts prior to any money being settled.
- Any cheques in the system being sent to known scammer accounts (or those that become known) can be stopped prior to settlement so the funds are not passed to the scammer.

2.41 The majority of the PSPs that are participants of the ICS have contracted with third party suppliers in order to undertake some aspects of fraud checking. This has not been centrally mandated in the ICS rules, but participants considered it to be beneficial. Other participants have implemented their own fraud identification techniques appropriate to their own fraud and risk profiles.

2.42 At the current time, it is the paying PSP that generally reimburses the payer in the event of fraud. This model is relatively unique internationally where cheque imaging has been implemented. Internationally it is generally the payee's PSP that is held liable for frauds. On 3 November, HMT published a consultation[3] on proposals for secondary legislation that would require payee's PSP to be held liable for losses in the new ICS system. HMT set out the view that this change is needed to ensure users of cheques (i.e. payers) have a safety-net to ensure they do not suffer any un-remedied losses. However, it also states the view that ICS system rules should remain the primary indicator of which party compensates the payer. HMT's consultation is open until 1 December, and it currently plans to lay the revised legislation before Parliament in February 2018.

2.43 There is also a dispute resolution mechanism between the PSPs where, if the PSPs cannot agree on liability, an independent third party acts as an arbitrator.

Faster Payments and CHAPS

2.44 As we set out in our response to the super-complaint, the operators of Faster Payments and CHAPS currently do not have any rules, policies or procedures in place related specifically to consumer protection against fraud or scams. This issue is generally seen as being between the customer and the PSPs because the operator – as a distinct entity in the centre of the payment chain – is not party to, and does not control, the establishment and ongoing operation of commercial relationships between PSPs and their customers.

2.45 However, there are procedures to help when payers (or PSPs) accidentally make payments to the wrong payee. The operators have each put in place best practice principles that participants follow to recover credit payments 'sent in error'. The operator of FPS manages and facilitates the principles [✂] for FPS and Bacs credit payments, which have been in place since early 2015. The process forms part of the FPS system's procedures, so all FPS participants must follow it. [✂]. In CHAPS, there is credit payment recovery guidance that has been in place since late 2015 – the operator does not have an operational role in this guidance.

3 HMT (2017) *Legislation to support cheque imaging: consultation.* www.gov.uk/government/consultations/legislation-to-support-cheque-imaging/legislation-to-support-cheque-imaging-consultation

2.46 The principles set out the process and timeframes that the sending and receiving PSPs should follow when interacting and [✂] with each other, and with the payer and payee, when attempting to recover a payment. This includes telling the payer the outcome.

2.47 [✂].

2.48 The principles do not guarantee that funds are recovered. However, the principles mean that in cases where the payee does not dispute the return of the funds, the money can be returned within 20 working days.[✂].

249 Clearly setting out the principles can help make the process for recovering the funds from a misdirected payment more transparent and efficient.

2.50 In our view, the principles appear to be similar in some ways to the process that could be used if an APP scam was discovered. However, the principles specifically note that the recovery of fraud-related payments, such as APP scams, is out of scope. For these payments, PSPs are told to use their own fraud procedures to attempt to recover the money.

2.51 The operators noted that there are drawbacks to the principles. The current process is based on manual communication, via emails and telephone, and can take some time to reach an outcome (up to 20 days). By this time, the funds are likely to have been moved to another account. This timeframe is less of a concern for genuinely misdirected payments, where the beneficiary is not expecting the funds and is unlikely to have criminal intent.

2.52 [✂].

2.53 We also note that the best practice standards developed by UK Finance set out the standards PSPs should follow when responding to APP scams claims (see Chapter 3).

Proprietary three-party systems and overlay services

2.54 In our terms of reference, we said we would consider the incentives and actions of proprietary payment systems (such as PayPal) and payment system overlay services (such as Paym) in relation to disputed payments.

Proprietary systems

2.55 Proprietary systems, such as PayPal and American Express – also known as three-party systems – are fundamentally different to the other push and pull payment systems considered in this annex. In proprietary systems, the system operator acts as a single PSP that serves all the system's payers and payees.[4]

2.56 This contrasts to other payment systems, including CHAPS and FPS, in which there are numerous PSPs, with payers and payees for a given payment generally being serviced by different PSPs (which are separate commercial entities) operating across that system.

2.57 This limits the usefulness of considering proprietary systems for our purposes:

- The PSP/operator of a proprietary system has a direct commercial relationship with both the payer and payee – so there are different incentives to the situation where payer and payee are typically serviced by different PSPs.
- In proprietary systems the PSP/operator has full visibility over parties on both sides of a payment. This puts them in a stronger position on fraud than PSPs operating across other systems, who will typically only have a relationship with a party on one side of a payment.

4 These systems work in a similar way to an 'on us' push payment across a PSP for some payments where both the payer and payee hold accounts at the same PSP.

2.58 Given these factors, we do not consider it helpful to consider the specific fraud-related practices in proprietary systems at this time.

Paym

2.59 Paym is an overlay service that allows the majority of UK current account holders to:

- use their mobile phone number as an identifier for payment
- make push payments via mobile banking applications to other registered users, using a mobile phone number (rather than sort code and account number) as the payee identifier

2.60 Underlying Paym is a database that links mobile phone numbers to bank account sort codes, account numbers and account holder names. Using a mobile banking application, payments are initiated using the mobile number of a registered payee, which is mapped to an account sort code and number and other relevant details. In particular, the name of the payee is presented back to the payer, who confirms if they want to continue with the payment or not. The underlying payment itself is executed across Faster Payments or LINK.

2.61 As the payee name is presented to the payer before payments are initiated, payers using Paym are given the opportunity to avoid some types of APP scam – specifically, malicious misdirection scams where the scammer poses as someone else (for example, a safe account scam where a scammer is impersonating a bank). We note that industry initiatives are currently underway to bring similar capabilities to Faster Payments initiated using channels beyond Paym, such as internet and telephone banking (see discussion of Confirmation of Payee in Chapter 4).

Considerations for APP scams

2.62 There are liability models in place for disputed payments in payment systems that provide pull payments – card systems (Mastercard and Visa), Bacs and ICS. These are used for disputes over fraudulent payments, and in card payment systems for other commercial disputes. In the card systems, liability (and therefore the party which bears the loss) is contingent on whether the parties involved have met certain responsibilities or acted appropriately, as set out in the model. The responsibilities are linked to practices to help prevent the fraud from happening. Liability can apply to all parties involved: PSPs, the merchant and the consumer. They are all expected to have taken a certain amount of care. Where the victim has shown the appropriate level of care, they are reimbursed.

2.63 There are also examples of dispute resolution mechanisms in UK payment systems. It may be the operator (cards) that acts as an arbitrator or an independent third party (ICS).

2.64 Where these liability models are used, we recognise there are some distinct differences to APP scams:

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

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

2.66 The use of penalties is another measure that is used to incentivise participants, specifically PSPs, to use practices for preventing fraud. This concept is used in the card systems. Penalties include additional fees or audits. A comparable practice for APP scams could be to penalise PSPs for having a high proportion of APP scams. These PSPs could be required to undertake changes to enhance their monitoring and detection capabilities and/or face a financial penalty. To implement this process, the standards would need to be determined and a body established to monitor adherence and impose penalties where required.

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

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

Annex 3
Practices in comparable network industries

3.1 In this annex, we explore other network industries that face challenges comparable to APP scams. In the case of APP scams, one PSP's actions can affect the volume of APP scams at other PSPs. For example, by providing a current account to a scammer a PSP will increase the volume of scams in the system. We have therefore looked at cases in other industries where the actions of one network participant can impose costs on other participants in the industry.

3.2 For each of the industries we have considered, we provide a brief overview of the network, set out the relevant challenges facing the industry and discuss the approach the industry has taken to address these challenges. We then discuss potential considerations for payment systems and APP scams.

3.3 The industries, and challenges, we have chosen for this are:

- **Telecommunications:** Misuse of premium rate services, and caller line identification spoofing
- **Rail:** Delays and cancellation affecting other train operating companies and passengers
- **Electricity:** Theft of electricity

3.4 We conclude with a summary of the considerations for addressing APP scams in the payments industry.

Telecommunications

3.5 When a customer (the originator) makes a phone call, it is routed to the recipient through communication providers (CPs), such as BT. If both the originator and the recipient are customers of the same CP then only that CP needs to be involved in making the call. If the originator and the recipient are customers of different CPs, then the two CPs must communicate with each other to route the call, via direct network 'interconnection' or indirectly via one or more third party networks.

3.6 Since not all CPs are connected a single call could be routed through more than two CPs. Some CPs, known as virtual CPs, do not own their own routing systems, and instead use the capacity on the systems of other CPs. Calls are routed between CPs, or varying direct or indirect router, rather than through centralised infrastructure. This is in contrast to interbank payments, where payments are routed through payment systems with a centralised infrastructure, such as Faster Payments.

Industry challenge: Misuse of premium rate services

3.7 Premium rate services are services that consumers can purchase by charging the cost to their phone-bill or mobile pre-pay account. Some current and popular examples include voting in TV competitions, directory enquiries and donations to charity via text messages.[5]

3.8 Premium rate services started out as higher-rate fixed line numbers, (for example, numbers starting with 09 or 118), that could be used to access a range of services. Premium rate services subsequently evolved into mobile text short-codes (for example, to enter competitions or download mobile content). The latest evolution of the premium rate services market is into the apps arena, with consumers downloading digital content and services from app stores (such as those provided by Apple and Google) onto their smartphones and charging it to their phone bills. The recipient receives a share of the cost of a call.

3.9 Premium rate services create serious risks of consumer harm due to a number of features intrinsic to this service – there is a long history of serious consumer harm where regulation has not been effective. This includes internet dialler fraud, the mis-selling of mobile ringtones and games and problems with broadcast premium rate services, all of which have required strong regulatory action to deal with.

3.10 Consumers can call premium rate numbers to access premium rate services, such as using directory enquiries or calling business information lines. Premium rate numbers cost more to call than a normal number. For most premium rate services the recipient of the call receives a share of the cost of the call.[6] These numbers can be based either in the UK or internationally.

3.11 It is possible for a fraudster to obtain a premium rate number, or otherwise make arrangements to benefit from a number, and fraudulently cause calls to be made to it, without incurring the proper cost of such calls. Fraudsters can trick customers into making calls to these numbers – for example, through 'missed call' scams where consumers are deceived into dialling premium rate numbers without being made aware of the cost of the call.

3.12 A CP which provides termination network facilities for a fraudulent premium rate service is not required to reimburse the victim and, similarly to APP scams, the victim may not be able to recover the money from the fraudster, typically where the fraudster is based abroad. However, the victim's CP may choose to reimburse the victim to some degree, as is done with APP scams.

3.13 As the cost of the misuse of premium rate services is largely not borne by the fraudster's CP, without rules there are limited incentives for some CPs to stop fraudsters getting access to the network.

Industry approach

3.14 We discuss two of the approaches taken to tackle the misuse of premium rate services in the UK. This includes strict regulation of premium rate services through a dedicated enforcement authority, and delaying and withholding payments.

5 Ofcom page on *Premium Rate Services:* www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/policy/premium-rate-services

6 This is not true for all number ranges. For example, for 070 numbers the end user does not receive a share of the revenue.

Regulating premium rate services

3.15 Most premium rate numbers in the UK are regulated by the Phone-paid Services Authority (PSA). Businesses offering controlled premium rate services are required to register with the PSA and comply with its Code of Practice. The PSA can use its powers to take enforcement action against businesses and traders that do not comply with its Code of Practice.[7] In the most serious cases, the PSA's Code Adjudication Tribunal can order businesses to pay substantial fines, refund all consumers or prohibit them from operating in the market for significant periods.

3.16 APP scammers can use personal payment accounts to facilitate APP scams, whereas the owners of premium rate services are businesses. Regulating individual payment accounts like premium rate services would require the owners of individual payment accounts to register with a regulatory body. It would also require the regulatory body to be able to take action against the scammer following an APP scam, which is challenging because the scammers are difficult to trace. These factors mean it may not be possible to adopt this approach for payments. PSPs, as providers of payment accounts, are already required to undertake Know Your Customer (KYC) checks.

3.17 The PSA can also add a variety of Special Conditions for what it identifies to be high-risk services in addition to the normal requirements of its Code of Practice. One Special Condition available is a requirement to lodge a bond which could then be used to pay refunds and fines in the event that a Code Adjudication Tribunal orders these sanctions following a breach of the PSA's Code of Practice. Requiring PSPs, or other parties, to provide guarantees for payment accounts could have a negative impact on PSPs' ability to offer the accounts, and may significantly increase costs.

Delayed and withheld payments

3.18 CPs can, and generally do, choose to route calls through BT's infrastructure instead of having a direct connection to each terminating CP in the UK. BT has a Standard Interconnect Agreement for CPs that route calls through its infrastructure, which includes rules governing how CPs address the artificial inflation of traffic (AIT).[8]

3.19 If a CP has reasonable suspicion of AIT with respect to calls it has originated, it can withhold payment to the CP hosting the premium rate number. The two CPs, and BT if relevant, can then exchange information to review whether AIT did take place, and follow a dispute resolution process if necessary. If investigation reveals that the calls were not AIT, the payments would be released.

3.20 The equivalent in payments would be a PSP delaying the execution of a payment, or the settling of funds, to at-risk accounts. As PSPs face legal requirements to execute payments by the next day, they would only be able to delay for a short time. While it would be difficult to identify at-risk receiving accounts (beyond those known on the Cifas blacklist), it could be possible to apply delays to payments from high-risk senders or large-value payments.

3.21 South Korea's withdrawal delay system operates with a similar principle, and prevents the cash withdrawal of a transfer of funds for up to 30 minutes if the transfer value exceeds 3 million Korean won (~£2000). We discuss international comparators in more detail in Chapter 5, where we consider the role of operators in APP scams.

3.22 Exchanging information could help respond to APP scams outside the context of delaying payments. If PSPs adopt standardised practices for exchanging information with each other, following an APP scam, they may be able to respond to APP scams more effectively. We discuss the industry's work on information sharing in Chapters 3 and 4.

7 *Code of Practice:* psauthority.org.uk/-/media/Files/PSA/For-Businesses/Your-phone-paid-service/Code-of-Practice/PSA_Code_of_Practice_14th_Digital

8 *Standard Interconnect Agreement (Annex E):* www.btwholesale.com/assets/documents/Billing/Annex_E_Document.doc

Industry challenge: Calling Line Identification spoofing

3.23 Recipients of phone calls can see a phone number associated with the originator of the call using Calling Line Identification (CLI). Originators are able to modify the number shown by CLI. There are good reasons why an originator may wish to do this – for example, so the recipient sees an 0800 number also owned by the originator so they can call back on a free call number. This service is provided to originators by CPs.

3.24 It is also possible for fraudsters to modify the number shown to the recipient in order to spoof an identity when contacting a potential victim. This can form part of an APP scam – for example a scammer can pretend to be calling from a PSP.[9]

Industry approach

3.25 Ofcom sets guidelines for CPs regarding the provision of CLI facilities. These include guidelines that the CPs should ensure that the CLI data is authentic.[10]

3.26 While the real originating number is hidden from the recipient, it is always known to the originator's CP. CPs are required to give the originator's identity to parties with a 'legitimate interest' – this is undefined but likely to include the police, regulatory bodies, and the customer receiving the calls.[11] However, calls may be routed via international carriers who may not choose to recognise the jurisdiction of such law enforcement and regulatory agencies so as to obscure the identity of the originator.

3.27 CLI authentication is a new capability being developed for the newest technology systems used to convey voice calls. It can be used to verify that the numbers used in CLI are owned by the caller. Ofcom is working with the industry to implement this in the UK.[12] As calls can be routed internationally, Ofcom is also working with the Internet Engineering Task Force (IETF) to standardise CLI authentication.

3.28 Authentication of CLI is comparable to Confirmation of Payee in payments, which will help prevent customers from sending money to a different person than intended. We discuss Confirmation of Payee in Chapter 4, where we provide an update on wider industry and regulatory developments.

Rail

3.29 In the rail industry, train operating companies (train companies) are the companies that carry passengers across the rail network infrastructure, which is operated by Network Rail. Examples of train companies include Great Western Railway and South West Trains. Freight operating companies also use the rail network to transport goods. In this case study we focus on train companies.

3.30 The Office of Rail and Rail (ORR) is the regulator for Great Britain's rail industry.

Industry challenge: Unplanned delays and cancellations affecting other train companies and passengers

3.31 Network Rail works with the wider rail industry to develop a national timetable for passenger services that sets out the timing of each train at each station. Trains can be delayed or cancelled.

3.32 Passengers are harmed by delayed or cancelled trains. Delays and cancellations may[13] also affect the reputation and finances of the train companies operating the delayed train.

9 NatWest page on *Caller ID scams*: www.business.natwest.com/business/natwest-business-bankingsupportcentre/fraud-and-security-advice/common-scams/caller-ID-scam.html

10 Ofcom page on *Guidelines for the provision of Calling Line Identification Facilities and other related services over Electronic Communications Networks (Version 2)*, section 7: www.ofcom.org.uk/phones-telecoms-and-internet/information-for-industry/telecoms-industry-guidance/calling-line-identification

11 ICO page on *Line identification*: ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/line-identification-cli/12

12 *Tackling nuisance calls and messages*: update on the ICO and Ofcom Joint Action Plan www.ofcom.org.uk/__data/assets/pdf_file/0026/44909/jap_update_dec2015.pdf

13 This is subject to the franchise arrangements with the government.

3.33 As delays can be caused by other train companies (or freight operating companies) or Network Rail, in the absence of any other arrangements network participants may not fully consider the impact of their actions on other participants when making decisions. This is comparable to APP scams, where the actions of PSPs can affect the volume of APP scams at other PSPs.

Industry approach

3.34 The impact of unplanned delays on train companies and on passengers is addressed through:

- data collection and analytics undertaken by Network Rail
- Schedule 8, which sets rules for when train companies must compensate, or be compensated by, each other, and when Network rail must compensate train companies; this uses Network Rail's data collection and analysis
- passenger compensation arrangements for when train companies must reimburse their passengers for delays to their journey

Network Rail analytics

3.35 Network Rail collects data from train companies in order to calculate delays, and to allocate the causes of delays to organisations.

3.36 Train companies can use the data from network analytics to understand the impact of their actions on other train companies, and the impact other train companies have on them. Centralised analytics are also used in calculating Schedule 8 payments, which we discuss below.

3.37 The payments industry is developing solutions that will analyse network-level payment transaction data. Transaction data analytics can be used to identify money mule accounts and trace fraudulent payments. We discuss transaction data analytics and APP scams in Chapter 4, where we provide an update on wider industry and regulatory developments.

Schedule 8

3.38 In the track access contract between Network Rail and train companies there are provisions to cover planned delays or cancellations (Schedule 4) and unplanned delays or cancellations (Schedule 8). ORR sets the policy for both Schedules 4 and 8.

3.39 Schedule 8 has three main functions:

- to help limit the financial impact on train companies of poor performance at other train companies and Network Rail
- to incentivise Network Rail to improve performance
- to incentivise train companies to limit the delay they cause to other operators

3.40 Schedule 8 payments are made when train companies or Network Rail's level of performance diverges from a pre-determined benchmark. When train companies or Network Rail perform worse than their benchmark they make penalty payments. Conversely, if they perform better than their benchmark they receive bonus payments.

3.41 Network Rail's system records delays and cancellations on the network and attributes them to the party responsible. If there is a disagreement the Delay Attribution Board (DAB), of which Network Rail and the train companies are members, will arbitrate.[14] If the decision by the DAB is not accepted it can then be put in front of the Access Disputes Committee (ADC), an independent body.

3.42 As a result of this system, train companies and Network Rail are penalised for causing delays and cancellations. This can help reduce delays and cancellations on the rail network by incentivising these parties to do their best not to cause delays or risk incurring a penalty.

3.43 We consider how PSPs can be appropriately incentivised to address harm from APP scams in Chapter 6 of our report, as part of a contingent reimbursement model.

Passenger compensation

3.44 Nearly all train companies now operate the 'Delay Repay' passenger compensation scheme as part of their franchise agreement with the government.

3.45 Under the scheme, passengers may claim compensation of 50% of the price of their ticket at 30-59 minutes' delay to their journey and 100% at 60 minutes' delay, regardless of the cause of the delay. In 2015 the government announced its intention to roll out an extension to this scheme so that passengers may claim (25%) compensation at 15 minutes' delay.[15]

3.46 We consider consumer reimbursement for APP scams in Chapter 6 of our report, as part of a contingent reimbursement model.

Electricity

3.47 Great Britain's high voltage transmission line network, the National Grid, transmit electricity across the country. Distribution network operators (DNOs) operate the connections between the National Grid and customers.

3.48 DNOs do not sell electricity to customers; instead electricity suppliers form contracts with both DNOs and customers to sell electricity.

3.49 Electricity suppliers must purchase the electricity used by their customers from electricity generators. This is done through contracts agreed between the parties. Many suppliers are also generators, which limits the need to buy and sell electricity with other parties.

3.50 DNOs are comparable to central operators, as they operate infrastructure used by the energy suppliers. Energy suppliers are comparable to PSPs, as they use the infrastructure to sell services to customers.

Industry challenge: Electricity theft

3.51 As electricity is transmitted across distribution networks some energy is lost as heat. As a result, the amount of electricity taken off the National Grid is more than the electricity used by customers. Where losses do occur, the costs of this are shared between energy suppliers in the local area, weighted by market size. However, electricity can also be lost due to theft. This can occur in two ways:

- **Manipulating the accuracy of electricity meters:** Criminals can get free electricity by bypassing the meter, or by tampering with the meter. Here the criminal has a contract with an energy supplier.
- **Tapping the line:** The criminal takes electricity directly from the DNO's infrastructure. Here the criminal does not have a contract with an energy supplier.

14 *The Delay Attribution Board, An Introduction*: www.delayattributionboard.co.uk/forms/Introduction%20to%20the%20DAB%20Booklet.pdf

15 *Government announces improved compensation scheme for rail passengers:* www.gov.uk/government/news/government-announces-improved-compensation-scheme-for-rail-passengers

3.52 In the first case, the criminal's energy supplier can observe usage patterns and may be able to prevent theft. Physically inspecting the meter may also detect tampered meters, or bypassed meters. However, more generally, electricity loss from theft is difficult to differentiate from transmission loss. If the theft is undetected, the costs are shared across energy suppliers.

3.53 This can cause problems comparable to APP scams. An energy supplier which does not take sufficient steps to prevent theft will cause losses which will affect other energy suppliers, and ultimately consumers.

3.54 The theft of electricity has a material impact on customers in terms of both cost and safety. Ofgem has had long-standing concerns that suppliers did not have adequate incentives to proactively detect, investigate and prevent electricity theft. These are explored in their *Tackling electricity theft*[16] consultation and *Tackling Electricity Theft – The way forward* decision.[17] Ofgem introduced new requirements for electricity suppliers to tackle electricity theft in May 2014.[18]

Industry approach

3.55 There have been a number of initiatives to address electricity theft. We outline here:

- the role of energy suppliers in monitoring the usage patterns of their customers
- Ofgem's role in setting standards for energy suppliers
- the role of trade bodies

Usage monitoring

3.56 Meters at the properties of electricity customers can allow for limited monitoring of electricity usage, such as comparing the total amount of electricity taken off the grid to the total amount sold by suppliers over a given period.

3.57 Smart meters enable the remote reading of electricity usage on a near real-time basis. Data from smart meters goes to a centralised hub, currently run by the Data Communications Company. This data can be accessed by those with permission via gateways, including energy suppliers. This could make it easier for them to detect unusual usage activity which would indicate theft.

3.58 Ofgem introduced a requirement for electricity suppliers to set up a cross-industry Theft Risk Assessment Service (TRAS).[19,20] TRAS enables energy suppliers to assess the risk of theft by analysing usage data and third party data, including credit history. Ofgem has also supported the industry's development of a new code of practice to establish minimum standards for theft investigations.

3.59 In payments, PSPs are already able to monitor transactions made by their own customers. The payments industry is also working to introduce centralised transaction monitoring called transaction data analytics. We discuss transaction data analytics in Chapter 4, where we provide an update on wider industry and regulatory developments.

Requirements for energy suppliers

3.60 Ofgem issues, and monitors compliance with, supply licences. These list the requirements that all energy suppliers must comply with in order to supply energy to consumers. The electricity licence includes conditions that electricity suppliers must take 'all reasonable steps' to detect, investigate and prevent electricity theft.

16 *Tackling electricity theft – Consultation:* www.ofgem.gov.uk/publications-and-updates/tackling-electricity-theft-consultation

17 *Tackling Electricity Theft - The way forward:* www.ofgem.gov.uk/sites/default/files/docs/2014/03/electricitytheft-decisionfinalv1.pdf

18 *Tackling electricity theft – new requirements for electricity suppliers:* www.ofgem.gov.uk/publications-and-updates/tackling-electricity-theft-%E2%80%93-new-requirements-electricity-suppliers

19 *Direction under paragraph 7 of condition 12A of the Standard Conditions of the Electricity Supply Licence to introduce the Theft Risk Assessment Service: www.ofgem.gov.uk/publications-and-updates/direction-under-paragraph-7-condition-12a-standard-conditions-electricity-supply-licence-introduce-theft-risk-assessment-service* 20

20 ElectraLink page on *TRAS*: www.electralink.co.uk/services/governance-management/theft-risk-assessment-service/

3.61 In payments, a central body could set additional rules for continuous account monitoring in order to adopt this approach for payments. PSPs are already required to undertake KYC checks.

Trade body

3.62 The United Kingdom Revenue Protection Association (UKRPA) is a voluntary body set up to address electricity theft, and theft from other utilities. Its members include DNOs and electricity suppliers, who can use the UKRPA as a forum for coordination and sharing best practice. The UKRPA's Strategic Plan 2017-18[21] sets out the UKRPA's most recent thinking.

3.63 In payments, PSPs already have an industry body which they can use as a forum for APP scams – UK Finance.

Considerations for APP scams

3.64 We have identified several challenges that other network industries face that are comparable to APP scams, and approaches that are used to address these challenges.

3.65 Some of the approaches used in these industries are similar in principle to measures that are already in use in the payments industry. These are:

- PSPs having the ability to analyse data for monitoring and possibly detecting transactions for their own customers which are part of fraud
- a trade body which focuses on addressing the issue, through UK Finance
- regulating access to the payments network. PSPs are required to undertake KYC checks for customers

3.66 Other approaches used in these industries are similar in principle to measures that are now being implemented in the payments industry. These are:

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

3.67 However, there are some notable processes used in the rail industry that are not used currently in push payment systems. The rail industry has formal arrangements in place for compensation between train companies, and for compensation of passengers, if trains are delayed or cancelled. These schemes are designed to give the train companies an incentive to act in the best interest of the passengers, and to compensate passengers for the harm they may have caused.

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

21 *UKRPA Strategic Plan 2017-18: www.ukrpa.co.uk/images/UKRPA_FORUM_17_02_04_Strategic_Plan_2017-18.pdf*

Annex 4
Economic incentives for APP scam prevention and response

4.1 In this annex we discuss the economic incentives and ability of different parties to prevent and respond to APP scams.

Different incentives and abilities to reduce harm from APP scams

4.2 There are five parties that are directly involved in the execution of an individual APP scam:

1. The **victim/payer** who is duped by the scammer into making payment(s)
2. The **victim's PSP**, which, having received legitimate authorisation from its customer (i.e. the victim), sends the payment(s)
3. The **payment system operator** whose system is used to process and settle the payment(s)
4. The **receiving PSP**, which receives and credits the payments to a payment account used by the scammer
5. The **scammer/payee** who perpetrates the scam and is the sole party with criminal responsibility for the scam; they are also (directly or indirectly) the payee

4.3 For each party we consider their:

- **incentives** to prevent consumer harm from APP scams
- **ability** to prevent consumer harm from APP scams

4.4 It is important to note that in some APP scams both the victim's PSP and the receiving PSP may be the same entity – in these instances, the scam may not involve a payment that crosses a central payment system.

4.5 The distinction between victims' and receiving PSPs is relevant when discussing individual APP scams. However, when considering APP scams as a whole, we consider it likely that many PSPs (especially larger PSPs) will be in the position of having been the PSP for both victims and scammers. We explore the implications of this point further in our discussion below.

4.6 For the purposes of this discussion we exclude consideration of the scammers themselves, who clearly have no incentive in reducing consumer harm from APP scams. We further assume that scammers are not going to participate in scam resolution or restitution (although in some cases they may be, if apprehended by law enforcement and convicted, and in possession of assets that are available to assist with restitution).

4.7 We acknowledge that the presentation of the parties above is a simplification:

- In practice, once the initial payment made by a victim is received into a payment account controlled by a scammer, the scammer will typically transfer the funds onwards to multiple further payment accounts. This helps obfuscate the source of funds and complicates recovery efforts. These further payment accounts may be operated by PSPs other than the initial receiving PSP, which widens the group of PSPs involved in the receipt and onward transfer of funds associated with an APP scam.
- From January 2018, following the implementation of the second EU Payment Services Directive (PSD2), there are likely to be additional actors directly involved in this chain, such as payment initiation service providers.
- There are other parties that may, indirectly, be involved in the execution of an APP scam. For example, scammers may leverage social networks to build trust with a potential victim, or use personal information obtained from a data breach at a company which a potential victim has given sensitive personal data to.

APP scam victims/payers

4.8 Currently there are very strong incentives for payers to act in a manner that reduces the risk of becoming a victim of an APP scam, and to react swiftly when they realise they have become a victim. The legal position is that payers are liable for all losses incurred by APP scams. In some cases PSPs provide goodwill compensation to victims, although they are under no formal obligation to do so.

4.9 Potential APP scam victims have the most information available on the reason and context of a potential payment and how it relates to their wider payment activity. They are also likely to have been in touch with the payee, giving them the chance to look for signs of a scam. This puts them in a strong position to prevent APP scams.

4.10 Victims have a vitally important role in reporting APP scams as soon as they are recognised. However, their ability to influence or participate in the further response to a scam is very limited, and they must rely on other parties to investigate and take action on their behalf.

Victims' PSPs

4.11 As we set out in our initial response to the super-complaint, there are commercial incentives for victims' PSPs to act in a manner that reduces harm from APP scams. Victims of APP scams are customers of the PSPs, and may choose to take their custom elsewhere if they think that their PSP has not protected them enough or responded well when they reported an APP scam. Victims' PSPs may also suffer negative media coverage resulting in wider commercial losses.

4.12 Victims' PSPs are in a good position to contribute to the prevention of APP scams. They may be able to identify payments associated with APP scams, as they may have unusual characteristics for a given payer. For example, the payments may be for unusually large amounts, or to payees that the payer has not made payments to before. Victims' PSPs may also be able to identify when payments are made to accounts that have previously been controlled by scammers (for example, as a result of PSPs sharing information). These factors give victims' PSPs the opportunity to intervene and query payments before and as they are made.

4.13 Victims' PSPs can influence the effectiveness of the response to reported APP scams. They are typically the first point of contact for victims (this role will be formalised under the new best practice standards for responding to APP scams – see Chapter 3). They are then key in identifying and contacting the relevant receiving PSP to initiate recovery efforts. If funds can be successfully repatriated, they also have an important role in ensuring they are credited back to the victim as quickly as possible.

Payment system operators

4.14 The direct commercial incentives of payment system operators to prevent and respond to APP scams are limited – they have no direct relationship with victims and potential victims. We do consider, however, that there are some indirect reputational and commercial incentives for operators to minimise the level of APP scams made across their systems. For example, if consumers lose confidence in the overall security of push payments, they may migrate to alternative payment methods. Furthermore, the operators of the push payment systems in scope are currently run by companies in which PSPs have a significant governance role, and whose customers are the direct victims of APP scams. This provides some incentive for the PSPs to influence the operators to make changes to help reduce the harm caused by APP scams.

4.15 Operators have an important role to play in APP scam prevention, through the aggregate data that passes through central payment infrastructures. This data identifies the accounts involved in a specific APP scam, at both victim's and receiving PSPs. Importantly, the data can also identify the aggregate payment activity associated with all payments made and received to and from all other accounts operated by PSPs participating in the system. Thus, while not having direct knowledge or relationship with the payer and payee in a given payment, analysis of the aggregate data that flows through the central infrastructure could identify patterns that may identify scams and potential mule accounts.

4.16 The operators could communicate this information to PSPs, who could then take action when their customers attempt to make payments to these accounts. An example may be an account that has not received any payments for a long time that starts to receive large multiple payments from accounts that have not paid into it before. The Payments Strategy Forum (the Forum) is currently working on establishing the industry collaborative standards that would enable transaction data analytics solutions (see Chapter 4 for details).

4.17 There is also an important role for operators in the response to APP scams. Again using the data that flows through the central infrastructure, both the initial transfer and onward transmission to other accounts of the fraudulently obtained funds can be traced and identified. This information can then be used to assist with the suspension and recovery of these funds. Work in this area is currently being taken forward by both the Forum's transaction data analytics workstream and the Joint Fraud Taskforce funds repatriation workstream (see Chapter 4 for details).

Receiving PSPs

4.18 As we set out in our initial response to the super-complaint, the incentives for receiving PSPs to prevent and respond to individual APP scams are weaker than for victims' PSPs. The receiving PSP will generally have no commercial relationship with the victim. There are, however, other incentives for receiving PSPs to play a larger role than is suggested by direct commercial motives. The first is that receiving PSPs may act to avoid negative media coverage (for example, being labelled as the 'scammer's bank') and to preserve their wider corporate reputation (which is at least in part an indirect commercial consideration). Second, PSPs are under a range of legal and regulatory obligations aimed at preventing crime, including financial crime such as APP scams. Amongst these are Anti-Money Laundering (AML) and Countering the Financing of Terrorism (CFT) requirements, and Know Your Customer (KYC) checks.[22]

4.19 As a scammer must have access to a payment account to execute APP scams, minimising their access to accounts is key in preventing APP scams. Given this, PSPs' KYC procedures play a vital role in keeping scammers out of the system. Receiving PSPs are also in a good position to monitor incoming payment transactions for potential signs of activity that may indicate APP scams. We believe these are areas where receiving PSPs (and potential receiving PSPs) are in a strong position to assist with APP scam prevention.

22 *For detail of these obligations, see Annex 4 of PSR (2016) Which? authorised push payments super-complaint: PSR response, www.psr.org.uk/psr-publications/news-announcements/which-super-complaint-our-response-Dec-2016*

4.20 Receiving PSPs have a key role in responding effectively to reports of APP scams. This includes responding and investigating promptly, and if necessary taking appropriate actions to prevent the further disbursement of funds and to assist with their repatriation to the original payer.

Summary of incentives and ability to reduce harm from APP scams

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

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

4.23 Equally, no one party is able to exert influence, or co-ordinate activity, over the whole chain. Moreover, each party's influence on scam prevention and response would, in general, complement (rather than substitute) that of other the parties in the chain.

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

PUB REF: CP17/2 Annexes

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