Which? super-complaint

Consumer safeguards in the market for push payments

23 September 2016

Which?

Contents

About Which?

Which? is the largest consumer organisation in the UK with more than 1.2 million members and supporters. We operate as an independent, apolitical social enterprise working for all consumers and funded solely by our commercial ventures. We receive no government money, public donations, or other fundraising income. Which?'s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people's lives fairer, simpler and safer.

Introduction

UK consumers and businesses rely on using payments services and payment systems every day. Consumers' confidence in payments is important for the economy and consumer welfare.

Yet when consumers are subject to sophisticated scams and are tricked into transferring money to fraudsters via 'push' payments (such as Faster Payments)[1] banks do not provide the levels of protection that they could – and that they typically do provide for other types of payment.

The sums involved are often large and can be life-changing for the victims. The use of push payments is growing and likely to grow further as new push payment services are introduced, increasing the risk of such scams.

In this super-complaint we set out evidence that:

- many consumers lose large sums of money to fraudsters after they are tricked into authorising bank push payments, and never recover this money – and this harm may increase;
- the conduct of banks (with whom the fraudsters must themselves hold – or effectively control – accounts) contributes to this consumer harm – if the banks faced different incentives, protection for consumers would improve.

There are steps that could be taken to protect consumers – similar to those the banks already take to protect against unauthorised payments[2] and card payments authorised as a result of deception. Placing more liability on banks for the losses from such scams would create efficient incentives for banks to develop systems to better manage risks, through identifying and checking high risk payments while maintaining the benefits of Faster Payments (and not reducing liability on consumers who had been grossly negligent or acted fraudulently).

1. A 'push' payment is where the consumer obtains details of the payee's bank account and instructs their own bank to send money to the payee's account from their own bank account. These have commonly been known as 'Bacs transfers' but are typically executed now via Faster Payments.
2. We use 'unauthorised' payment to refer where the scammer has themselves fraudulently accessed the consumer's account to initiate the payment.

The need for an investigation

We are making this super-complaint because we believe an investigation is needed to address the following:

- the extent to which banks' conduct could change so reducing consumer harm from sophisticated scams that trick people into authorising bank push payments to a fraudster;
- changes that are needed in legislation or regulation, to change the incentives on banks and payment systems, and to ensure that more is done to manage the risks from these types of scams and to protect consumers from harm.

This super-complaint outlines the main areas that we consider should fall within the scope of an investigation, and discusses potential remedies that could reduce harm to consumers.

We consider that ultimately new legislative or regulatory requirements on banks may be needed. We appreciate that these requirements may take some time to design, and we also recognise that bringing together the stakeholders that would be involved in implementing the solution may not be straightforward. We expect that the regulator may want to undertake a market study in order to collect evidence, investigate and build the case for appropriate remedies.

Jurisdiction

Legislation requires us to submit this super-complaint as a complaint to the Payment Systems Regulator (PSR) because:

(i) Which? is a designated representative body under section 68(1) of the Financial Services (Banking Reform) Act 2013, allowing us to make a complaint to the PSR that "a feature, or a combination of features, of a market in the UK for services provided by payment systems is, or is likely to be, significantly damaging to the interests of service users."[3]; and

(ii) Section 234C (1A) of the Financial Services and Markets Act 2000 says: "...a complaint may not be made to the FCA under this section if it is a complaint which could be made to the Payment Systems Regulator by a designated representative body."

We are also sending this super-complaint to the Financial Conduct Authority (FCA) because:

- any remedies are likely to address requirements or liabilities on banks in relation to consumers' use of payment services. Existing legislation, which establishes relevant requirements and liabilities on banks for credit card payments and for unauthorised payments (of other kinds), includes the Consumer Credit Act 1974 and the Payment Services Regulations 2009. The FCA is the regulator responsible for implementing these requirements; and
- the PSR acknowledges the need to liaise with other regulators – including the FCA – where those regulators are 'better placed to address the concerns raised', in order to ensure that a super-complaint is considered in the most appropriate way.[4]

We expect the PSR and FCA to investigate the issues raised in this super-complaint and to consider appropriate remedies.

Structure of the super-complaint

The super-complaint is structured as follows:

- Section 1 outlines the relevant market and feature of that market
- Section 2 sets out the evidence for the feature of the market
- Section 3 sets out evidence for the scale of consumer harm
- Section 4 provides initial thoughts on remedies
- Conclusion

3. See the Financial Services (Banking Reform) Act 2013 (Designated Representative Bodies) Order 2016.
4. "Super-complaints Guidance: Guidance for designated representative bodies on making a super-complaint under section 68 FSBRA", Payment Systems Regulator, March 2016, paragraph 4.3.

Section 1: The relevant market and feature of that market

The relevant market in this super-complaint is push payments made by consumers from UK bank accounts.

The relevant feature of this market can be described as:

- the risks that authorised push payments are being made to scammers are not allocated to those best placed to manage them;
- the adequacy of measures banks take to address the risks of consumers being scammed into authorising push payments to fraudsters; and
- banks' conduct in maintaining payment system operating rules that result in inappropriate and inefficient allocation of liability for the costs of such scams.

1.1 The relevant market

A distinction is commonly[5] drawn between:

'Pull' payments: where the consumer provides a merchant with relevant account details and authorises the merchant to pull funds from their account, including:

- credit card payments;
- debit card payments; and
- Direct Debits.

'Push' payments: where the consumer obtains details of the payee's account and instructs their bank to send money to it, including:

- Faster Payments;[6]
- CHAPS payments;[7] and
- Bacs[8]

The relevant product market for this super-complaint is bank push payments (i.e. push payments initiated from a bank account) made by consumers.

While there will be occasions where another electronic payment method could provide a close substitute for a bank push payment,[9] there will be many circumstances in which it would not, and a push payment will be the only feasible option for a consumer,[10] for example where the payment size exceeds card limits or where the payee is not able to receive card payments or Direct Debits. We consider that bank push payments made by consumers should be treated as a separate product market from other types of payment for the purposes of this super-complaint.

We consider the relevant geographic market to be the UK, and specifically the relevant market is push payments made by consumers from UK bank accounts.

We consider that the geographic market should be defined by reference to the initiating bank account. This captures the set of bank push payments through which UK consumers may pay a fraudster.

Even if the product and/or geographic market were considered to be wider, this would not materially change the nature of the market feature or associated consumer harms set out in the super-complaint.

5. See, for example: European Central Bank (2010), The Payment System (https://www.ecb.europa.eu/home/shared/media/publications/paymentsystem201009en.pdf).
6. We mean this to include payments made to another account within the same banking group, the processing of which may not make use of the interbank Faster Payments system.
7. CHAPS is primarily a 'wholesale' payment system, but is also used by consumers to make some large transfers such as for house purchases.
8. Bacs Direct Credit is also a push payment but is generally only used by businesses.
9. From here on we use 'push' payment to mean a push payment initiated by a consumer from a UK bank account, unless otherwise stated.
10. There are other types of 'push' payment, e.g. third party systems like PayPal, where the payer funds their PayPal account (via push or pull from bank or card account) and is then able to 'push' money to a payee's PayPal account. Again, while on some occasions this type of payment could be a close substitute for direct bank push payments, there are many occasions where it would not be.

1.2 The feature of the market

When a consumer is subject to a scam, the 'scammer' needs to fraudulently obtain his funds via use of one or other payment system, including often via push payments. The scammer may achieve payment in one of two ways:

- Unauthorised payment: where the scammer fraudulently accesses the consumer's account using information that has been scammed from (or otherwise gathered about) the consumer;
- Authorised payment: where the scammer deceives the consumer into authorising payment to the scammer's account (although we note that the consumer can't really be understood to have authorised the payment to a scammer).

The consumer harm relevant to this super-complaint concerns authorised push payments. That is, it is concerned with harm arising from scammers deceiving consumers into instructing their bank to make a payment to an account controlled by the scammer. Consumers are currently insufficiently protected against such payments being made. Apart from the, often substantial, individual consumer losses that can result in these cases, such scams can also undermine consumer confidence and participation in what would otherwise be beneficial online activity.

The feature of the market that gives rise to this harm could be described in a number of different related ways, including as follows:

- The risks that authorised push payments are being made to scammers are not allocated to those best placed to manage them. Scammers can use a range of highly sophisticated techniques to identify and deceive consumers into instructing their bank to make a payment. In most other payment contexts (including unauthorised push payments, and authorised and unauthorised pull payments), the bank is liable for losses (typically subject to qualifications such as the consumer not having been grossly negligent).[11] But where consumers have been deceived into authorising push payments, they will almost always bear the resulting costs, even though banks are typically much better placed than consumers to guard against the risks of such payments being made.[12]
- The conduct of banks could change so reducing the extent to which scammers can fraudulently obtain funds through authorised bank push payments.

There are two aspects to banks' conduct:

- The first is the adequacy of measures banks take to address the risks of consumers from being scammed into authorising push payments to the bank accounts of fraudsters. For example, at present, Faster Payments System payments are processed without even checking whether the account name matches the account number.[13] In contrast, banks have demonstrated they can take sophisticated actions to help protect consumers from being tricked into authorising pull payments and from unauthorised access to their accounts.

11. See sub-section 4.1 for an explanation of liabilities for different payment types, and the concept of gross negligence.
12. This because banks (who hold customer relationships with the accounts that scammers are using) are able - acting collectively as a payments system - to develop systemic approaches and to use their data to reduce risks from fraud, in ways that consumers cannot. Such systemic approaches can be far more effective and efficient than individual consumer responses.
13. http://www.fasterpayments.org.uk/consumers/what-happens-if-i-have-sent-payment-wrong-place (accessed 31st August 2016).

- The second is banks' conduct in maintaining payment system operating rules that result in inappropriate allocation of liability for the cost of scams where funds are obtained via authorised push payments. All the liability falls on the consumer, even when they have not behaved negligently and have been tricked by sophisticated scams. No liability falls on the banks involved, including the bank which has a customer relationship with the fraudster's account. Yet banks individually and collectively have considerable scope to develop systematic approaches to reduce the risk from these scams if incentivised to do so. This scope is discussed in sub-section 4.4.

We discuss the evidence for banks' conduct in more detail in Section 2.
A key reason why the market has not evolved to address these features is likely to be the presence of significant externalities, including:

- the majority of the benefit from a bank taking unilateral action to guard against its customers being scammers is likely to go to customers of other banks (who would otherwise have been scammed); and
- a bank's ability to manage the risks of its customers making payments to scammers is likely to be heavily dependent on the actions of other banks, as the scammer is more likely than not to bank with someone else – so there would be significant obstacles to a bank that sought to provide better protection to its customers unilaterally.

Section 2: Evidence for the feature of the market

In summary:

- for unauthorised payments, and for pull payments generally, banks have arrangements for appropriately allocating between themselves the liability for losses due to fraud and scams;
- therefore for unauthorised payments, and for pull payments generally, banks have the incentive to, and do, develop effective systems and approaches for reducing the risk of scams;
- but for authorised push payments banks make consumers bear full liability for the cost of scams and consequently banks do not face the incentives needed to adequately manage risks;
- banks' conduct is not justified by any special characteristics of authorised push payments.

2.1 For unauthorised payments, and pull payments generally, banks have arrangements for appropriately allocating liability

Safeguards against a range of types of payee mis-behaviour have been long-standing features of pull payment systems:

In a pull payment system:

- a payee might obtain a consumer's account (for example, card) details fraudulently and pull unauthorised funds from their account;
- a consumer could authorise a payee to pull funds, but the payee could pull more funds than agreed; or
- a consumer might authorise a payee to pull funds but later discover that the expected product or service did not materialise, including because it was a scam.

In all these cases, the consumer is protected by the rules of the pull payment systems – in particular the inclusion of mechanisms for payments to be challenged and reversed. In the card schemes, the interbank challenge and reversal process is referred to as 'chargeback'.[14] Similarly for Direct Debits, there is the Direct Debit Guarantee.

Banks are also liable to reimburse consumers for unauthorised push payments, provided the consumer did not act with gross negligence or fraudulently.

Chargeback and similar arrangements provide not only a means of reimbursing consumers, but also of shifting costs – through interbank arrangements – onto the misbehaving payee's bank (the merchant acquirer in a card scheme). So, in the case of a scammer, these interbank processes provide for liability to be passed to the bank where the scammer holds his account. Thus liability is allocated to those who are best able to manage the risk of scammers using bank accounts and payment systems to facilitate their scam.

14. Card scheme rules define a number of valid bases upon which a consumer's bank may request that a card payment is reversed. If the supplier's bank does not accept that the payment should be reversed (i.e. does not accept that it meets one of the chargeback criteria) then the card scheme rules provide for an adjudication process. http://chargebacktech.eu/knowledge-base/mastercard-and-visa-chargeback-reason-codes/ (accessed 30th August 2016).

2.2 For unauthorised payments, and pull payments generally, banks have approaches for reducing the risk of scams

Where banks face liability, they are incentivised to develop approaches for managing and reducing the risk of payee misbehavior including the risk from scams. And banks put in considerable effort to monitoring and combatting fraud in relation to these payment types. Financial Fraud Action UK (FFAUK), a payments industry body, publishes annual statistical reports ("Fraud the facts") that focus heavily on detailing and measuring different types of card fraud. And banks have developed a range of approaches for vetting payees and monitoring their conduct, including employing sophisticated fraud detection measures.[15] For example:

- Banks use sophisticated security systems that:
  - protect customers' bank accounts from unauthorised access, such as two-factor authentication; and
  - reduce the likelihood of unauthorised online card use, such as the extra layer of protection provided via American Express SafeKey, MasterCard SecureCode and Verified by Visa.
- Organisations using the Direct Debit scheme go through a careful vetting process before they are authorised, and are closely monitored by the banking industry.
- FFAUK highlights banks' use of intelligent fraud detection systems in relation to card payments, including sophisticated customer-profiling neural networks that can identify unusual spending patterns and potentially fraudulent transactions (following which the card company will contact the cardholder to check whether the suspect transaction is genuine).
- Card system merchant acquirers typically levy additional fees on suppliers that have significant chargeback requests made against them, in order to encourage better conduct.

2.3 For authorised push payments banks make consumers bear full liability for scams and consequently banks are not incentivised to do more to manage risks of scams

Unlike other types of payment, if a consumer authorises a push payment to another bank account that turns out to be fraudulent the consumer is very unlikely to secure reimbursement. The Financial Ombudsman Service (FOS) says: "...where the consumer has been tricked by fraudsters into making a payment or transfer of funds themselves, they are unlikely to be able to get their money back".[16] This is the case even if the consumer has acted sensibly to protect themselves and is simply subject to a sophisticated scam.

The allocation of liabilities therefore places little incentive on banks to manage the risks of relevant scams. Not surprisingly therefore there is much less evidence – compared to other payment types – for the banks developing systematic approaches to adequately manage the risks from scammers using bank accounts and payment systems to receive push payments.

A bank's role in push payments is often characterised as simply following the consumer's payment instructions. The Faster Payments process currently involves checking that the submitted account number and sort code are valid – i.e. only checking that the account exists. When a payment is instructed there is currently no check of whether the submitted account name matches the account number, let alone whether the payee account is held by a legitimate user. A consumer can submit the name of who they intend the money to go to, but – regardless – it will go to whoever actually holds the account with the submitted account number.[17]

15 "Fraud the facts 2015 – The definitive overview of payment industry fraud and measures to prevent it", Financial Fraud Action UK.

16 In its 2015 review of vishing scam cases, "Calling time on telephone fraud a review of complaints about "vishing" scams", the Financial Ombudsman Service, concludes that: "...where the consumer has been tricked by fraudsters into making a payment or transfer of funds themselves, they are unlikely to be able to get their money back. "The bank is not liable to reimburse who has authorised a payment.

17 Payments UK have a 'confirmation of payee' initiative underway looking at ways of providing a check on who money is being sent to. While this indicates that some action is being taken, it will not be sufficient. This is discussed sub-section 4.2.

We recognize that individually banks may take steps to try to stop or trace funds where a customer reports that they may have been scammed into authorizing a push payment. But we have not found evidence of routinely or systematically applied approaches to managing the risk that a push payment payee is a scammer. For example:

- Faster Payments compares use of its system to using cash,[18] and tells consumers: 'protect yourselves from fraud'.[19]
- As discussed earlier, the industry body FFAUK's "Fraud the facts"[20] report focuses on measures to combat unauthorised access and card fraud. In relation to authorised push payments, its focus is on advising consumers to watch out for themselves (which is unlikely to be a sufficient approach – discussed further in sub-section 4.2).
- Banks can be slow to act when consumers alert them to a push payment scam. The FOS found in its review of vishing[21] cases that 34% of payers' banks took more than 12 hours to contact the receiving bank, and 12% took more than 3 days or may not even have contacted the receiving bank at all.[22] Since fraudsters typically access the funds quickly, these delays do not appear indicative of careful and coordinated procedures for minimising risks.

Instead systematic bank fraud prevention efforts in relation to push payments appear to be focused on guarding against unauthorised access to accounts – where, of course, banks do face liability. Of course, efforts to identify account-holders who are scammers would be a way to guard against both unauthorised and authorised push payment fraud. However, a bank that invested in identifying those of its account-holders who were scammers would reap only a fraction of the benefits of such investment (the externalities point discussed in section 1.2). Additional co-ordination arrangements would be required to overcome the externality, similar to chargeback in cards. Banks appear instead to find it easier to focus on security of account access, requiring little interbank co-ordination but failing to address authorised payment scams.

2.4 Banks' conduct is not justified by any special characteristics of authorised push payments

We do not consider there is justification for banks' conduct in relation to authorised push payments, such that consumers bear full liability for scams and banks do little to manage risks of scams. This subsection refutes number of possible justifications.

Potential conduct justification 1: Banks have a duty to act on their customer's instructions

Banks are required to execute a valid, authorised push payment instruction. But this should not prevent them developing arrangements for how instructions are executed that make it harder for consumers to pay scammers – without failing to execute an instruction if (notwithstanding the bank's efforts to protect the consumer) the consumer wanted to proceed, fully aware of an accurate view of the risk. This is discussed further in Section 4.

There seems scant justification for lower levels of protection when the consumer's instructions are direct (to the bank) as opposed to indirect (as when using a card).

18. We disagree the Faster Payments is similar to cash, and explain why in sub-section 2.4.
19. The Faster Payments website justifies this advice by saying: 'Once sent, a Faster Payment cannot be reversed'. But this statement confuses the technical characteristics of how Faster Payments works with the contractual arrangements that apply between banks, and implications for consumers. The fact that a specific payment instruction – once sent – cannot be reversed does not mean that the payment cannot be reversed from the perspective of the consumer as payer, with an offsetting payment. The Faster Payments comment, therefore, simply amounts to a statement that the liability sits with the consumer.
20. "Fraud the facts 2015 – The definitive overview of payment industry fraud and measures to prevent it", Financial Fraud Action UK.
21. 'Vishing' (voice phishing) is the criminal practice of using the phone to defraud, dupe or mislead someone.
22. "Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015.

Potential conduct justification 2:
Banks cannot do much – "Paying using a Faster Payment is similar to paying using cash"

Faster Payments says "paying using a Faster Payment is similar to paying using cash", and "as soon as the money reaches the recipient's account they can be sure it's theirs".[23]

But electronic payments are not similar to cash payments. Cash can be spent anonymously, and it is this feature that means that the transfer (and loss) of cash can be final. Faster Payments is not anonymous. Like most other electronic payment systems it involves a transfer to an identifiable party who has opened and is using another bank account. Both the consumer's and the scammer's bank (if different) must be part of a payment system – collectively provided as a service by the banks – for the transfer to be possible.

Therefore – unlike cash – banks both provide the systems that enable the scam and have the ability to vet and monitor where payments are going and to whom. Banks could develop proportionate ways of authenticating the legitimacy and associated risk of payees, for example, through credit reference type arrangements, and adjusting anti-fraud measures accordingly. Key risk factors could be identified and used, for example, if scammers typically open and use accounts for only a short period, or 'mule' accounts[24] have certain patterns of usage, then payments to accounts with such characteristics could trigger additional layers of protection. Possible approaches are discussed further in Section 4.

Potential conduct justification 3:
It is appropriate for consumers to bear full liability

Some[25] have argued that consumers should carry full liability for protecting themselves from fraud – even in areas where they are currently protected. While it is right that consumers should have incentives not to be grossly negligent, or act fraudulently, consumers are often not best placed to address the risks from scams.

It is clear that many consumers do not protect themselves well even where they are fully liable (see Section 3), in a context where scammers can use increasingly sophisticated techniques to target and trick consumers. As the Director of Enforcement at the FCA has said (in the context of investment fraud): "You don't need to be gullible to lose money to a scam or fraud. Fraudsters target financially sophisticated people too, who often don't like to ask what might sound like silly or basic questions."[26]

Many consumers who fall victim to scams have sought to guard against fraud and have not been negligent. The FOS[27] has noted that vishing scams can be very convincing. Consumers are tricked into believing they were protecting their money when in fact it was being stolen.

At the same time, banks (who hold customer relationships with the accounts that scammers are using – and who ought to 'know their customer') are – unlike consumers – able to develop systemic approaches and to use their data to reduce risks from fraud (and, where incentivised, have demonstrated an ability to do so). Such systemic approaches can be far more effective and efficient than individual consumer responses.

23. http://www.fasterpayments.org.uk/protect-fraud (accessed 24 June 2016).
24. Money 'mules' are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules receive scammed funds into their account, they are then asked to withdraw it or wire the money to a different account.
25. http://www.bbc.co.uk/news/business-35890028 (accessed 24 June 2016).
26. "Over 55s at heightened risk of fraud, says FCA", FCA press release, 25th May 2016.
27. "Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015.

The Payments Strategy Forum's Draft Strategy[28] says: "...Consumers and PSPs [Payment Service Providers] both want a system where criminals can be more easily identified, legitimate users are not excluded wrongly, and the costs of financial crime are kept as low as possible." In order that the costs of financial crime are kept as low as possible the risks need to be allocated to those best placed to manage them. Banks are better placed to manage many of the risks related to scammers, in part because of the potential they have to apply the sort of big data analytic techniques also discussed in the Draft Strategy: "The UK payment industry creates a very large, high quality dataset through the processing of payments. The emergence of more sophisticated ways to handle and query large amounts of data has opened up the potential for the industry to better exploit this 'big data' set to determine trends or actual financial crime being committed."

In any case, the current difference in the treatment of victims scammed via authorised push payments and the treatment of other scam victims leads to perverse outcomes. In otherwise equivalent scam situations, consumer exposure to losses is dependent on the payment method that the scammer chooses to extract funds. For example, banks reimburse the costs of 'no hang up' scams where a consumer[29] has been tricked into providing their banking security details to the scammer (or where the consumer has been tricked into making a card payment), but not the costs of 'no hang up' scams where the consumer has been tricked into making the transfer themselves.[30]

Box 1 summarises FOS case studies that illustrate the different outcomes for the consumer depending on scam payment method.

FOS vishing case studies

CASE STUDY SCAM 1

Unauthorised card withdrawals[31]

No hang up scam with cards collected by courier.

- Mr H took a call from someone saying they were from the police saying that his debit cards had been compromised
- Mr H then called his bank's number to check this was true, but didn't realise that the scammer was still on the line
- He was asked to key his PIN into the phone for verification and while on the phone a courier he thought was from the bank arrived to take his cards away
- Mr H contacted his bank the following day after feeling that something was not right
- His bank confirmed that a significant amount had been removed from his savings account and more had been withdrawn at cash machines
- The bank said he had been negligent in giving away confidential information
- The FOS disagreed: 'there was no opportunity for Mr H to reflect on what was happening. He was following directions from people he thought were acting to protect his accounts'

The FOS decided Mr H should be refunded in full.

Box 1 continues on page 12.

28. Being responsive to user needs - A draft strategy for consultation, Payments Strategy Forum, July 2016.
29. A consumer who has not acted fraudulently or with gross negligence.
30. 'No hang up' scams are where the scammer stayed on the line after the consumer put the receiver down and pretended to be the consumer's bank or the police answering the consumer's call to check the scammer's story. These have recently been addressed by BT and other telecoms providers. Since November 2015, all BT exchanges end a call two seconds after the receiver is put down. https://letstalk.globalservices.bt.com/en/security/2015/11/better-security-in-two-seconds/ (accessed 30 August 2016).
31. "Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015.

Box 1 continued.

CASE STUDY SCAM 2

Unauthorised push payment[32]

No hang up scam with security information collected.

- Mrs E was called by someone pretending to be her bank
- She called her bank's number but didn't realise that the scammer was still on the line
- She gave enough security information for the scammer to access her account using internet banking
- Mrs E called her bank later that day but £5,600 had been transferred
- Her bank said they couldn't refund Mrs E because she herself allowed the fraudster access to her account, and that it didn't delay in trying to get her money back once she'd told it what happened
- The FOS took the view that Mrs E could not have been expected to know the technical elements of a no hang-up scam. She had not been grossly negligent

The FOS decided Mrs E should be refunded in full.

CASE STUDY SCAM 3

Authorised push payment[33]

No hang up scam with consumer transferring funds to a scammer's account.

- Ms L was called by someone pretending to be her bank saying there had been suspicious activity and asking if she had made certain purchases
- When she said she hadn't, they said she should call a different department straight away to sort the problem
- She called the number on the back of her debit card but didn't realise that the scammer was still on the line
- They gave her details of a different account she should transfer her money, and she did that straight away
- Ms L called her bank later that day but it was too late to recover the money
- The FOS said it could understand why Ms L thought the bank ought to refund the money, but that she had logged in herself using her usual details and asked the bank to transfer the money. The bank had fulfilled her request

The FOS decided that no refund was due.

32. http://www.ombudsman-decisions.org.uk/viewPDF.aspx?FileID=87077 (accessed 9th August 2016).
33. http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/issue116.pdf (accessed 9th August 2016).

Section 3: Evidence for scale of consumer harm

In summary, consumer harms include:

- more scams being perpetrated (than if banks' conduct improved);
- consumers being left out of pocket, with individual losses causing substantial distress; and as a result;
- potential for diminished overall consumer confidence in the use of electronic payment systems.

The scale of harm, while hard to estimate, is likely to be substantial, and the size of losses to individuals are typically large. The potential for harm is also likely to be increasing as a result of (otherwise beneficial) developments in push payments.

3.1 Types of consumer harm

We identify three sources of consumer harm resulting from the conduct of banks set out in this super-complaint.

First the misallocation of liability for the costs of scams means that victims, who have not acted with gross negligence, are left liable for their costs, with harm from the permanent financial loss and associated stress. The sums involved are typically large and can be life-changing for the victims (see for example Box 3 page 16).

Second, banks could do more to systematically manage and reduce the risk of authorised push payment scams so it is easier than it could be for scammers perpetrate such scams. More individual consumers are therefore likely to be directly harmed by scams.

Third, there may also be indirect harm. Awareness and public reporting of examples where consumers have lost significant sums through scams may result in diminished overall consumer confidence in the use of electronic payment systems, with potential impacts on consumers' welfare and on the economy.

3.2 Estimating consumer harm

We have attempted to identify how much money is currently lost to scammers via authorised push payments, but of course this is something the regulator is much better placed to do, with its information gathering powers.

We did not identify reporting of this type of fraud by banks (consistent with our argument that banks lack incentives to properly address this type of fraud). Nor did we identify other data sources that could help us develop a reliable estimate of harm.

While it has not been possible to estimate a figure, we have identified evidence that suggests the sums are likely to be substantial.

Certain types of scam are likely to involve significant use of authorised push payments, including phone (for example, vishing) scams, online dating fraud and holiday booking fraud. These types of scams often involve large individual sums. Such higher value scams can be expected typically to involve push payments, both because this is necessary for payment of large sums and because (given banks' conduct already discussed) it is unlikely to trigger bank anti-fraud safeguards. And there is evidence from the FOS on vishing scams that a high proportion involve authorised push payments.

Many of the instances of vishing considered by the FOS were 'no hang up' scams. The FOS reviewed 185 vishing-related complaints involving gross consumer losses totalling £4.3m (in 20% of cases, between £20k and £50k was lost; 11% of cases involved losses of £50k or more; 2 consumers lost £100k or more). The FOS upheld only 37% of the complaints it reviewed in this sample, and in most of the not-upheld examples given in the report, the reason was that the scam involved an authorised push payment.[34]

Reported financial losses from each of these types of scam, and the sizes of individual losses are given in Box 2. But recent ONS research suggests figures for reported fraud (such as those in Box 2) very significantly understate the prevalence of fraud.[35]

Box 2

Figures for reported losses due to scams

- In 2014, £24m of identified total losses from phone scams The average gross individual financial loss in "no hang-up" complaints 2012-14 reviewed by the FOS was c.£25k/person[36]
- In 2015, £27m of identified total losses from online dating scams[37]
  Over 2,700 reported cases, with average individual financial loss of c.£10k/person[38]
- In 2015, £11.5m of identified total losses from holiday booking fraud
  4,910 reported cases, with average individual financial loss of c.£3k/person[39]

Fraud may not be reported because scams involve deception and may not be discovered, and because those harmed may be reluctant to report, for example, from embarrassment or shame at being duped. The National Fraud Authority's Annual Fraud Indicator in 2013 (the final year in which it was produced) estimated over 5 million total frauds costing consumers £9bn each year – an estimate built up from data that included survey evidence.[40] The order of magnitude difference between these figures and figures[41] for reported fraud, though not directly comparable, suggest the extent to which the reported fraud figures are likely to underestimate actual fraud losses.[42]

3.3 The potential for consumer harm is increasing

Developments in payment services are likely to continue to drive up the potential for consumer harm.

In recent years, the introduction of Faster Payments, while delivering potentially large consumer benefits, is likely also to have increased the risks of consumer harm from scams. Before Faster Payments, push payments would have would have taken c.3 days to be fully processed, giving more opportunity for consumers to raise concerns that they may have been scammed and for transfers to be blocked. But the near immediate nature of Faster Payments transfers means consumers have very little time in which to realise they may have been scammed and to report it. In its vishing report, the FOS found that 20% of consumers had raised the alarm with their bank within 2 hours of the scam, and over 75% within 24 hours.[43] Of course, the speed of Faster Payments is in general highly beneficial. It is not that Faster Payments needs to slow down, but the systems for protecting consumers from the risk of scams need to be effective in the Faster Payments context.

34. "Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015.
35. "CSEW Fraud and Cyber-crime Development: Field Trial"; TNS BRMB for the ONS, October 2015.
36. Action Fraud, "New figures show steep rise in telephone scams", Press Release, 2 December 2014.
37. "Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015. The 173 individual consumers who brought complaints reviewed by the FOS represented a collective gross consumer loss of £4.3m.
38. Action Fraud, "Online dating fraud cost victims £27 million last year", Press Release, 11 February 2016.
39. Action Fraud, "Travellers conned out of £11.5 million last year", Press Release, 4 April 2016.
40. Annual Fraud Indicator; Technical report; National Fraud Authority, 2013.
41. For example, Action Fraud reports £268m of identified losses from the top 10 internet enabled scams. http://www.actionfraud.police.uk/news/get-safe-online-week-one-in-five-victims-of-cybercrime-think-they-were-specifically-targeted-by-cybercriminals-oct15 (accessed 8th August 2016).
42. It is clear that much of the £9 billion estimate of losses would not relate to authorised push payments.
43. "Calling time on telephone fraud a review of complaints about "vishing" scams", Financial Ombudsman Service, July 2015

Increases in maximum limits for Faster Payments transfers (for example, up to £100k)[44] (while, again, delivering substantial benefits) have further increased the potential scale of consumer harm from scams. Again, higher maximum limits provide highly beneficial flexibility for users, but consumer protection systems need to develop in line with the greater risks.

The number of consumer push payment transactions in the UK, has increased dramatically in the last decade, and continues to increase. Faster Payments now processes Single Immediate Payments at a rate of over 850 million a year,[45] compared to Bacs' processing of only just over 100 million remote banking direct credits in 2006).[46]

Looking forward, there is considerable potential benefit to consumers from more use – and new types – of push payments, enabling increased consumer control over payments and requiring less data sharing.[47] Payments UK has a work stream on 'Request to Pay' – a secure electronic message to facilitate wider use of push payments.[48]

But, given the conduct of banks already discussed, a shift from pull to push payments could result in an overall loss of fraud protection for consumers. Scam purchases paid for by pull methods are protected while those paid for by authorised push methods are not.

There is also a risk that new forms of push payment may generate opportunities for new types of scam that would further expose consumers to harm.

For example, scammers could send fraudulent requests to pay to consumers, or tamper with legitimate ones so as to try to get funds sent to a different account. This has been a significant source of fraud in Brazil.[49] Forms of this type of scam have already been reported in the UK, consumers having received false payment details as a result of fake emails.[50] In July 2016, Action Fraud warned that they were "continuing to receive reports where parties' involved in house purchases are targeted to transfer money to bank accounts under the control of fraudsters, resulting in large losses for house buyers or solicitors."[51]

Box 3 describes one case study, based on a report in the Guardian in March 2016,[52] which illustrates:

- how simple but convincing scams may deceive sophisticated consumers;
- the very large, life-changing losses that can be involved; and
- the potential for such scams to diminish consumer confidence in the use of online payments

44. We understand caps on individual online transfers are now between £10k and £50k, and some banks allow phone transfers of up to £100k.
45. "Faster Payments monthly volumes and values 1990-2016", based on March 2016 monthly figure, http://www.paymentsuk.org.uk/industry-information/free-industry-statistics (accessed 8th August 2016).
46. "Bacs processing statistics", https://www.bacs.co.uk/documentlibrary/bacs_processing_stats.pdf (accessed 8th August 2016).
47. With push payments the consumer can then decide whether, when and how much to transfer to a payee.
48. http://www.paymentsuk.org.uk/sites/default/files/REPORT%20World%20Class%20Payments%20-%20A%20focus%20on%20Request%20to%20Pay.pdf.
49. http://www.bbc.co.uk/news/technology-28145401 (accessed 27th June 2016).
50. https://www.theguardian.com/money/2016/feb/13/banks-current-account-fraud (accessed 9th August 2016).
51. http://www.actionfraud.police.uk/news-fraudsters-hacking-into-emails-to-divert-house-purchase-payments-jul16 (accessed 9th August 2016).
52. https://www.theguardian.com/money/2016/mar/04/fraud-scam-email-barclays-lloyds (accessed 27th June 2016).

Box 3

CASE STUDY

Authorised push payment scam using false payment details

A record label general manager and her husband were scammed out of £25,000.

The couple were having an extension built, so had been in regular communication with their building company. On 30th October 2015 the company's accounts executive emailed an invoice for the work, in the form of a PDF attachment carrying the company's logo. It was an invoice the couple were expecting and was 100% genuine. It gave the total due – £27,829 – plus an account name (the name of the building company), bank account number, sort code and reference number.

Then on 2nd November they received what appeared to be a follow-up email from the same employee, written in the same style ("Dear Sarah & David" ...), and featuring all the same logos and formatting, and the same email signature. This stated: "We have changed who we bank with. I forgot to amend the changes on the invoice I sent 30/10. The attached invoice has our new banking details ... I'm sorry for any inconvenience these changes may have caused ..." This second invoice was identical in almost every way to the first – only the account number and sort code were different.

The couple paid £25,000 (their account's daily payment limit) so were surprised when, a few days later, they received an email from the company chasing payment. They told the accounts executive they had paid the bulk of the bill, but she emailed back to say that the second invoice had not come from her.

It was then the couple realised they had been scammed, with the most likely explanation being that either the building company, or the couple, unwittingly downloaded malicious software, which enabled the fraudster to intercept their emails. When the couple looked back at the emails, they noticed that the one received on 2nd November was sent from an email address just one letter different to the genuine one ("development" instead of "developments" in the company name).

The couple have not been able to recover the £25,000, and are quoted as saying: "This is a life-changing amount... It happened in a split-second, yet it has changed what the next few years look like for us." "The reason the police are citing for not pursuing an investigation is that this type of crime is so rife they haven't got the resources – they say that compared to some of the cases they are dealing with, it's small scale."

The Guardian reported that the couple's bank declined to accept any responsibility on the grounds that the transfer was authorised by the couple and the bank was merely following their instructions. Their bank is reported to have told them it had been unable to obtain a return of the funds from the fraudster's bank. By the time the latter bank had been alerted, the couple's £25,000 had been "utilised" by the account holder, so it was unable to return any of their cash. The Guardian reported that the fraudster's bank would not disclose the documentation they held on their account holder "for confidentiality reasons"; and that it also said: "We do not report scam claims to the police because the bank is not the victim."

The Guardian went on to offer advice to consumers on how to protect themselves, including the following: "There's a simple way to reduce your risk of being fleeced: don't bank online. In November 2015, we featured Ross Anderson, Professor of Security Engineering at the University of Cambridge's Computer Laboratory, who has never banked online because of the risks of fraud."

Section 4: Initial thinking on remedies

In summary, we consider that ultimately new legislative or regulatory requirements on banks are needed to incentivise banks, and payments systems, to do more to protect consumers when authorising push payments. We appreciate that these requirements may take some time to design, and we also recognise that bringing together the stakeholders that would be involved in implementing the solution may not be straightforward. We expect that the regulator may want to undertake a market study in order to collect evidence, investigate and build the case for appropriate remedies.

Current legislation gives consumers much better protection when scammers seek to secure funds through other payment routes. In particular, if the consumer:

- authorises a payment to a scammer using a credit card they are likely to be able to recover lost funds from their bank under Section 75 of the Consumer Credit Act;
- has been tricked into providing their banking security details, and the scammer has used those details to make an unauthorised transfer of funds, then the consumer is likely to retrieve the lost funds from their bank under the Payment Services Regulations 2009 (PSRs).

The liability placed on banks under these pieces of legislation generates strong incentives for banks to manage the risks of fraud losses arising in relation to the relevant payment types. As discussed in Section 2, banks have developed a range of mechanisms for doing so.

It is not perhaps surprising that legislation does not yet adequately cover push payments. The Payment Services Regulations 2009 implement the Payment Services Directive, which was finalised in 2007 when push payments were used at a much lower rate than today. But Faster Payments now processes Single Immediate Payments[53] at a rate of over 850 million a year[54].

We consider that a legal change is necessary to bring the allocation of liability for authorised push payment fraud broadly into line with other payment types.

We consider options for achieving this, in particular making banks liable for reimbursing consumers[55] who have been deceived into authorising a push payment to a scammer.

Placing more liability on banks for the losses from such scams would create efficient incentives for banks to develop systems to better manage risks, through identifying and checking high risk payments while maintaining the benefits of Faster Payments (and not reducing liability on consumers who had been grossly negligent or acted fraudulently).

4.1 Current legal and other arrangements for consumer protection

Our understanding of the sources of consumer protection in relation to payments to fraudsters or scammers, for different payment types, is set out below (and summarised in Diagram 1).

Credit card payments (authorised or unauthorised): Covered by the Consumer Credit Act (CCA). Under Section 75 of the CCA, the consumer's bank is liable where there is supplier (payee) breach of contract or misrepresentation, for transactions over £100 and not more than £30,000. Under Section 83 of the CCA, the consumer's bank is liable where the credit card has been used by someone other than the cardholder without their permission.

Other unauthorised payments (including debit card, Direct Debit and bank push payments): Covered by the Payment Services Regulations 2009 (PSRs). The consumer's bank is liable for losses unless the consumer has acted fraudulently or with gross negligence (see Box 4 on page 18).[56]

53. According to Faster Payments, Single Immediate Payments (SIPs) "are usually used when making internet or mobile banking payments. With the rapid growth of e-commerce and the digitalisation of the economy, SIPs are expected to see steady growth in the coming years."
54. "Faster Payments monthly volumes and values 1990-2016", based on March 2016 monthly figure, http://www.paymentsuk.org.uk/industry-information/free-industry-statistics (accessed 8th August 2016).
55. A consumer who has not acted fraudulently or with gross negligence.
56. The consumer will also be liable for the first £50 of any losses incurred in certain circumstances, for example losses arising from unauthorised use of a lost or stolen payment card where the bank is not promptly notified (regulation 62(1) and (3) of the PSRs).

Box 4

Relevant provisions of the Payment Services Regulations 2009

61. Subject to regulations 59 and 60, where an executed payment transaction was not authorised in accordance with regulation 55, the payment service provider must immediately—
    (a) refund the amount of the unauthorised payment transaction to the payer; and
    (b) where applicable, restore the debited payment account to the state it would have been in had the unauthorised payment transaction not taken place.

62. (2) The payer is liable for all losses incurred in respect of an unauthorised payment transaction where the payer—
    (a) has acted fraudulently; or
    (b) has with intent or gross negligence failed to comply with regulation 57.

The gross negligence test means consumers have clear incentives to guard against scams. The application of the test is contextual, and depends on the actions of both the consumer and their bank. Failure of a consumer to take adequate steps to protect themselves is unlikely to be grossly negligent if they are unaware of the risks. For example, in Box 1 (second case study), the FOS took the view that Mrs E could not have been expected to know the technical elements of a no hang-up scam, so had not been grossly negligent.
But if a consumer has had their attention drawn to the risks – for example via security measures or targeted awareness-raising efforts by their bank – they might be considered grossly negligent. For example, carrying an undisguised PIN number with a card in a public place is likely to be treated as gross negligence by the FOS under existing protections against unauthorised payments[57].

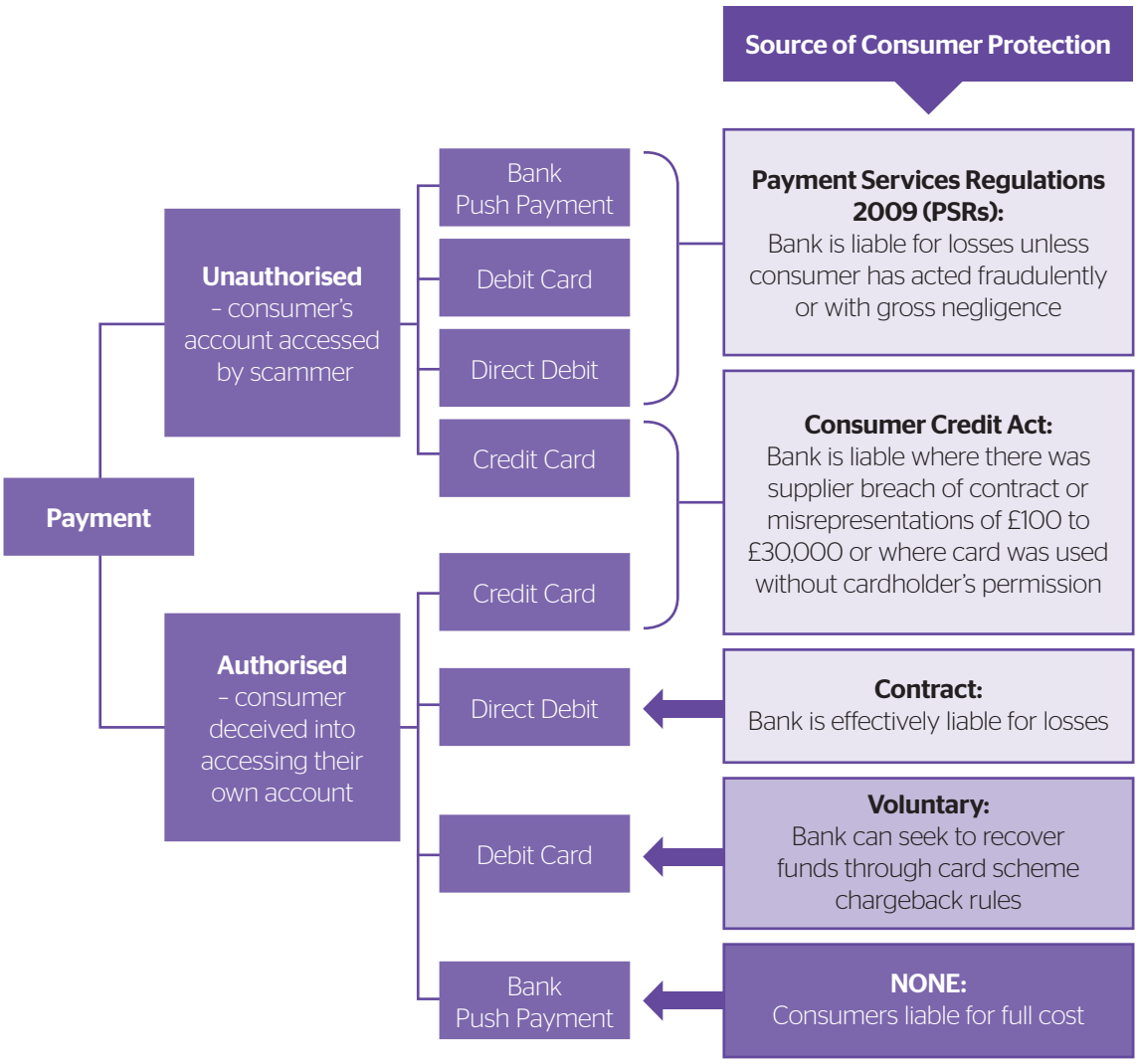
Authorised Direct Debit payments: In Bacs' explanation of consumers' rights under the Direct Debit Guarantee, which provides a contractual basis for consumers' protection, consumers are told: "All organisations using the Direct Debit system are sponsored into the Scheme by their bank or building society. They are checked for integrity, sound financial standing and administrative capability before being permitted to offer Direct Debit to their customers."[58] The banks therefore commit to taking steps to prevent use of the Direct Debit system by scammers. It would therefore be unlikely that a bank could or would argue that (having undertaken to vet users of Direct Debit) a consumer was liable for being tricked into authorising a Direct Debit to a scammer who the bank had failed to identify.

Authorised debit card payments: Here protection of the consumer relies on banks' voluntary – not legal or contractual – application of arrangements where they can seek to recover funds through card scheme chargeback rules.

Authorised bank push payments: No protections – the consumer is liable for the full cost of scams.[59]

57. "...we might have decided that keeping the card with its PIN amounted to "gross negligence" ...[f]or example, if the card and PIN had been kept together in a wallet and carried about in a public place." http://www.financial-ombudsman.org.uk/publications/ombudsman-news/116/issue116.pdf (accessed 5th September 2016).
58. https://www.directdebit.co.uk/DirectDebitExplained/FAQs/Pages/YourRightsAndSafeguards.aspx (accessed 8th August 2016).
59. PayPal (and other such overlay payment service providers) may also provide means for 'push' payments. The protections provided by PayPal appear to match or exceed (depending on the circumstances) the protections for bank push payments.

Diagram 1: Sources of consumer payments protection for different payment types



So for most categories of payment it is clear – in legislation or contract – that liability for scam losses is allocated to the consumer's bank, subject to varying qualifications, for example that consumers have not been grossly negligent.

For authorised debit card payments, arrangements are voluntary. It is not clear the extent to which these voluntary arrangements are as effective as those backed by statute or contract. There is clearly the potential for practices to vary between banks, with limited consequences for them, and therefore for some consumers to be less well protected. We also note the voluntary nature of the arrangements could affect the willingness of the FOS to intervene to ensure outcomes that adequately protect consumers.

We have not been able to identify, from the sources available to us, significant evidence for detriment associated with the authorised debit card chargeback arrangements. But given potential for questions over the effectiveness and consistency of such voluntary arrangements, we think that these arrangements should be considered for inclusion within the scope of the investigation of the issues raised in this super-complaint.

What is clear is that, while voluntary, the principle of authorised debit card consumer protections is well established, and ought to be treated as an effective requirement that should be formalised in law if necessary.

For authorised push payments, there are no relevant consumer protections, whether statutory, contractual or voluntary.

It is not perhaps surprising that relevant legislation does not yet adequately cover the risks to consumers in relation to push payments. The Payment Services Regulations 2009 implement the Payment Services Directive, which was finalised in 2007. While there were around 6 billion debit and credit card purchases in 2006 in the UK,[60] Bacs was processing under 2% of this number in remote banking payments (just over 100 million remote banking direct credits in 2006).[61] Since 2006 however, numbers of consumer push payments have increased, and continue to increase, rapidly. Faster Payments (as successor in this function to Bacs) now processes Single Immediate Payments at a rate of over 850 million a year.[62]

As set out in Section 3, there is likely to be significant consumer harm now arising from this gap in the legal arrangements for consumer protection.

4.2 Actions already under consideration or in train

Payments UK have a 'confirmation of payee' initiative underway looking at ways of providing a check on the name of the account that a transfer is being addressed to. This is also one of the proposed measures that the Payments Strategy Forum has recently consulted on.[63] If implemented, this measure would be a welcome step, and is relevant in particular to some vishing scams where consumers believe (wrongly) they are transferring money to a new account in their own name. But 'confirmation of payee' will not fully address the issues raised in this super-complaint. Many authorised push payment scams do not use that approach. For example, some scammers have opened accounts with a very similar name to the intended recipient account, and in such cases knowledge of the payee account name may do little to alert the consumer to the risk of the account being fraudulent. Scammers will be able to adjust their approaches if one particular avenue is closed off.

The Home Office has launched a new Joint Fraud Taskforce, which is looking at, among other things, using better data sharing and matching to speed up the identification of victims and address the barriers preventing the refund of scam victims.[64] While welcome, we do not expect the work of the Taskforce to fully address the issues in this super-complaint. We think there will remain many, potentially most, occasions where it will be impossible to retrieve the funds once they have been transferred to a scammer, for example if they have gone abroad. We are not aware that the Taskforce is looking to require banks to refund consumers if funds have not been successfully traced, nor put in place the safeguards needed to reduce the risk of transfers to scammers in the first place.

Ofcom has been working with the telecoms industry to close off the 'no hang up' scam. Since November 2015, all BT exchanges end a call two seconds after a receiver is put down. Other telecoms companies have made similar changes.[65] But 'no hang up' is just one example of a scam that involves authorised push payments. 'No hang up' scammers can be expected to move to alternative strategies.

60. "UK card payments 2015", http://www.theukcardsassociation.org.uk/wm_documents/UK%20Card%20Payments%202015%20taster%20for%20website.pdf (accessed 8th August 2016)
61. "Bacs processing statistics", https://www.bacs.co.uk/documentlibrary/bacs_processing_stats.pdf (accessed 8th August 2016)
62. "Faster Payments monthly volumes and values 1990-2016", based on March 2016 monthly figure, http://www.paymentsuk.org.uk/industry-information/free-industry-statistics (accessed 8th August 2016)
63. Being responsive to user needs - A draft strategy for consultation, Payments Strategy Forum, July 2016
64. Home Secretary speech on new joint fraud taskforce, 10 February 2016
65. https://letstalk.globalservices.bt.com/en/security/2015/11/better-security-in-two-seconds/ (accessed 30th August 2016)

We understand that the banking industry is taking forward a publicity campaign aimed at educating consumers to protect themselves from scammers' pressure to make payments. This initiative is welcome. At the time of finalizing this super-complaint, we do not know the full strategy or extent of this campaign. But we would urge realism about the likely effectiveness of any information-focused campaigns and remedies.

Research[66] suggests that for many victims, the problem is not their lack of awareness of fraud and scams but rather that they are not able to overcome the emotional and intuitive urge to comply, which is triggered by the psychological methods used by fraudsters; and that many victims of fraud are overconfident about their ability to distinguish fraudulent schemes from non-fraudulent ones.[67] This underlines the advantages of the sorts of systemic approaches to managing scam risks that banks could put in place, over reliance on individuals correctly identifying the risks.

4.3 Potential remedies

We have identified two broad options for remedies that could more fully address the gap in consumer protections. These remedies may require primary legislation or be implementable through regulation.

We recognize that solving the issue we have raised in the super-complaint is not straightforward, and expect that the regulator may want to undertake a market study in order to consider and develop appropriate remedies.

Option A

Under Option A, banks would be made liable for reimbursing consumers when an authorised push payment has been made to a scammer, other than where the consumer has acted fraudulently or with gross negligence.

This would effectively extend the kind of protection that consumers have under the PSRs – in relation to unauthorised payments (see Box 4) – to authorised push payments.

Option B

Under Option B, standards for risk management would be established which banks would be required to meet when executing authorised push payments. Banks would then be liable to reimburse a consumer if an authorised push payment had been made and the bank was not in compliance with these risk management standards (and a consumer had not acted fraudulently or with gross negligence).[68]

Variants of this option could be envisaged. Risk management requirements could be defined in terms of high level principles, with banks having to show how their processes satisfied those principles. For example, banks could be required to have adequate processes in place for authenticating or risk rating the legitimacy of payees when payments are made, such that customers are made aware of any significant risks associated with making a payment, and appropriate hurdles are applied when instructions to pay 'high risk' payees are received. Alternatively, more specific requirements could be set out, for example, specific ways in which payee risks should be assessed, categorised and responded to.

66 "The psychology of scams: Provoking and committing errors of judgement", Stephen Lea, Peter Fischer and K Evans, 2009. In: Report for the Office of Fair Trading. www.oft.gov.uk/shared_oft/reports/consumer_protection/oft1070. Pdf

67 "Which? Policy Research: An experiment on the relationship between confidence, online behaviours and the ability to spot scams", Tech rep, 2016

68 This would complement the banks' existing responsibilities under the FCA's 'Treating Customers Fairly' principle and over-arching consumer protection rules, such as (i) the contractual obligation to deliver services with reasonable care and skill pursuant to section 49 of the Consumer Rights Act 2015 and (ii) the obligation not to act in a way that is contrary to the requirements of professional diligence pursuant to Regulation 3(3) of the Consumer Protection from Unfair Trading Regulations 2008. Given that banks have developed and implemented mechanisms to prevent fraud for other payment types, it is arguable that a failure to extend those protections to push payments falls short of the standard that consumer protection laws do – or will soon – expect banks to meet.

Discussion of options

Options A and B differ in terms of where liability falls in the absence of specific identified failings on the part of the consumer or the bank. In particular:

- under Option A, providing the consumer has not acted in a grossly negligent manner (or fraudulently), then they will be protected – they would be reimbursed by the bank even where no fault is attributed to the bank;
- under Option B, the consumer is only protected in circumstances where the bank's actions are identified as having fallen short in some way – so if neither the consumer nor the bank is found to have been at fault, then the consumer would face the losses associated with a scam.

We consider there to be good efficiency reasons for providing the more comprehensive protection of consumers afforded by Option A. In particular, this focuses bank attention on consumer outcomes. It creates dynamic incentives to develop approaches that tackle sources of harm over time. Thus, even where a bank might be regarded as not having exhibited specific failings in the short term, having it face liability can be justified in terms of incentives to improve protections in the medium and longer term. The fast moving and innovative nature of payment systems, and of big data analytic techniques of the kind that might be used to improve protections, makes this issue of dynamic incentives particularly important.[69]

At the same time, it would be important, under Option A, to properly balance the exposure of banks with appropriate incentives on consumers. The gross negligence qualification would mean consumers would still have clear incentives to guard against scams. They could face substantial losses if they did not take adequate care. And banks' efforts to protect consumers could affect where liability fell. What was considered grossly negligent would depend in part on banks' use of security measures used and awareness raising efforts.

4.4 Likely impact of the potential remedies

Under Options A or B, banks would have better incentives to put in place proportionate arrangements for managing the risk that payees are scammers.

We would expect banks to develop interbank rules for appropriately allocating the liabilities between banks. Each bank could be made liable for the losses resulting from scams perpetrated by its account-holders, as it is best placed to assess and respond to the risks arising from its own customer bank accounts. Alternatively, all push payment service providers could be made collectively liable for all relevant fraud losses, for example funding a 'collective liability pot'.[70] Both approaches would incentivise action to reduce the scale of such losses, but the former approach would better ensure that each bank's liability reflected the strength or weakness of its risk management arrangements.

We would expect banks to respond to their new liability by developing systematic risk-based approaches to authenticating those opening accounts and authenticating payees in a push payment transaction (that is, better 'knowing their customer'), and adjusting payment processes and fraud checks accordingly. We would expect additional checks to be focused on those payments identified as carrying significant risk. We would not expect that additional safeguards would lead to a general slowing of Faster Payments.

69. This also implies that - if Option B were to be adopted instead - it would be preferable to apply it through the use of broad principles.
70. Such an approach would have some similarities to Ofgem's approach to losses from theft of electricity, where it proposed a collective industry-funded scheme to incentivise individual suppliers to take action to detect theft. (Tackling Electricity Theft - The way forward, Ofgem, March 2014) Energy suppliers were disincentivised from detecting theft because the benefits were mainly shared across the industry, while the costs fell on the individual supplier - analogous to the disincentives on payment service providers detecting their account-holders who may be scammers, as discussed in Section 2.

For example, banks could develop processes for authenticating the legitimacy and associated risk of payees through credit referencing type arrangements. We note the Payment Strategy Forum's Draft Strategy[71] "proposes that the industry builds a single view of confirmed, suspected and attempted fraud data and other financial crime data, subject to a robust legal framework. In due course the combined view of confirmed, suspicious, attempted and at-risk fraud data events can be fed into the shared analytical capability to prevent payments before the money leaves the system." This could be developed in a way that aided development of such credit reference type arrangements for payees. But without banks facing liability for authorised push payment fraud we are concerned that the Payment Strategy Forum work would be focused only on those areas in which banks do face liability, i.e. unauthorised payments and pull payments. Online banking apps already include pre-loaded details for a number of large frequently used payees such as other banks and credit card firms, utility firms, HMRC, etc. These payees have effectively already been authenticated by the bank, and this prior payee authentication approach could be extended. Alongside such an approach, consumers might be able to self-authenticate payees in some ways, for example, a form of 'friends and family' list, and protections / warnings associated with additions to this list could affect interpretations of gross negligence. In addition, a number of payee key risk factors might be identified. For example, if scammers typically open and use accounts for only a short period, or 'mule' accounts[72] have certain patterns of usage, then payments to accounts with such characteristics might be classed as higher risk and trigger additional layers of security.

The options for risk management could differ depending on whether payments were made to other UK accounts or to overseas accounts. We recognize that fraudulently-obtained funds may often be moved quickly overseas. But we expect that in most scams where a consumer is deceived into authorising a transfer, this would be to a UK bank account (in order that the need for IBAN and SWIFT codes did not arouse suspicion). Even where this was not the case, the issue would remain one of the processes for managing the additional risk of transfers instructed to overseas accounts.

The types of risk management arrangements discussed could better safeguard consumers, while limiting the extent to which they hindered flexible usage of push payments. Indeed banks have been able to do much to manage risks in relation to other types of payment without serious detriment to the usage of those payment types.

In terms of practical implementation of new arrangements, we have already noted the work by Payments UK on 'confirmation of payee'. If a major systems change to Faster Payments is required to implement confirmation of payee, that may provide a good opportunity for systems change also to include authentication of payees' legitimacy.

We also note that legal barriers to data sharing could be an obstacle to implementation of new arrangements. We think the regulator should consider whether there are any data-sharing, or other, barriers to implementing desired remedies that cannot be overcome within the existing data protection framework (i.e. by identifying a lawful ground for such processing), and recommend whether specific provision needs to be made to allow sharing of appropriate data to detect and prevent fraud.

71. Being responsive to user needs - A draft strategy for consultation, Payments Strategy Forum, July 2016
72. Money 'mules' are recruited, sometimes unwittingly, by criminals to transfer illegally obtained money between different bank accounts. Money mules receive scammed funds into their account, they are then asked to withdraw it or wire the money to a different account.

4.5 Compatibility of remedy options with the Payment Services Directives I and II (PSDs)[73]

We consider that remedy Options A and B are compatible with the PSDs. But even if the PSDs were found to constrain implementation of desired remedies, following Brexit the UK may have greater flexibility in relation to relevant EU law.

Scope of the PSDs

We consider that liability for authorised push payments that are made to a scammer is not a matter that is covered by the PSDs, and so the introduction of new provisions related to this would be compatible with the PSDs, notwithstanding their maximum harmonisation status.

The PSDs address the question of liability in respect of unauthorised payments, payee initiated payments and wrongly executed payments. Given that the PSDs are silent on the question of liability for authorised payments, Member States retain the power to legislate in that field, as long as that legislation does not conflict with the express provisions of the PSDs.

Option A, in particular, provides a rational policy position in a 'no fault' scenario. The payer has fallen victim to a fraud (and was not grossly negligent or fraudulent themselves). The payment service provider is not at fault for executing a properly authorised payment. Accordingly, it is a question of policy where liability should lie. Liability should be imposed on the bank because of the two parties they may have access to more information about the payee that might give rise to concerns about their legitimacy and more ability to manage the risk of scams; and shifting the liability would resolve the anomaly that the liability of the parties depends on whether a card or bank push payment was used.

Authorisation processes

Under the PSDs, banks are required to execute a valid, authorised push payment instruction. We consider neither Options A or B to be in conflict with this requirement.

Changing the requirements and/or liabilities that banks face would not affect the need for banks to execute valid, authorised push payment instructions. Rather, it would be expected to affect the arrangements and processes that banks applied when doing so (as discussed in sub-section 4.4).

These arrangements would formally form part of the authorisation process. They would ensure that the consent given by the payer was informed, and provide an additional layer of consumer protection by bolstering the authorisation procedures for high-risk payments. Banks would be expected to make it harder for consumers to pay scammers but they would still, under Option A or any variant of Option B, need to execute an instruction to pay a scammer if – notwithstanding the banks' efforts to protect the consumer – the consumer wanted to proceed. That may involve the consumer acting in a way that is grossly negligent (as a bank's efforts to alert and otherwise protect the consumer would affect what would be deemed grossly negligent) in which case the consumer would remain liable.

The statutory framework imposes no constraints over the manner in which consent may be given in order to authorise a payment. That is a question of the agreement between the parties (see Article 64(4) PSDII). The FCA, in its capacity as statutory regulator, is empowered to specify some aspects of that agreement and to require that additional protocols are engaged when a 'high risk' payment is in view.

73. We expect that (any) transposition of the Payment Services Directive II into UK law would not materially alter the relevant provisions of Payment Services Directive I which have already been transposed into UK law via the PSRs (2009)

Conclusion

It seems clear that banks are not doing as much as they could be doing to protect consumers from sophisticated scams that trick consumers into transferring money to a fraudster.

Unlike with other payment types, all the liability for such scams is on the consumer, and none on the banks who are typically better placed to address the risks arising from their bank account holders being scammers. Banks therefore lack incentives to put in pace adequate risk management arrangements to protect consumers.

This super-complaint sets out evidence for how banks lack incentives to better protect consumers, and for the potentially increasing consumer harm this is leading to. It suggests ways in which banks could be incentivised to better address these types of scam.

The regulator now has an opportunity to reduce the consumer harm from scams. We want them to launch an investigation which addresses the following:

- The extent to which banks' conduct could change so reducing consumer harm from sophisticated scams that trick people into authorising bank push payments to a fraudster.
- Changes that are needed in legislation or regulation to change the incentives on banks and payment systems, and to ensure that more is done to manage the risks from these types of scams and to protect consumers from harm.

We look forward to working with the payments sector, regulators and other relevant bodies to address the significant issues we have highlighted in this super-complaint.

SEPTEMBER 2016

Which? 2 Marylebone Road, London, NW1 4DF
which.co.uk | 020 7770 7000