Which?, 2 Marylebone Road, London, NW1 4DF
Date: 8 April 2021

Consultation Response

The Payment Systems Regulator's consultation on *Authorised push payment scams – call for views*

Summary

- Four and a half years on from Which?'s super-complaint to the Payment Systems Regulator (PSR) on authorised push payment (APP) scams, progress to address the significant emotional and financial harm experienced by consumers has been far too slow. The time for strong intervention is well overdue.

- The voluntary, industry-led approach that the PSR has taken on consumer protection has not worked. The improvements made to reduce the harm we identified have not been as significant as was expected or is required. For over a year the PSR has stated publicly that outcomes for victims of APP scams have been inconsistent and rates of reimbursement insufficient among customers of signatories to the voluntary Contingent Reimbursement Model (CRM) Code, which is based on the principle that the starting point should be to assume that victims of APP scams should be reimbursed in full.

- The payments industry cannot be left to solve this problem on its own. The overwhelming evidence is clear that neither voluntary initiatives nor competition can be relied upon to provide the minimum, industry-wide levels of protection that are required. We instead need mandatory standards of consumer protection across the industry to provide fairer and more consistent outcomes, and regulatory supervision and effective enforcement to hold firms to these standards.

- Which? therefore welcomes the PSR's proposals to introduce mandatory protection for customers, to require greater transparency on outcomes and to require greater collaboration to share information about suspect transactions. On the specific measures that have been proposed:

    - **We strongly support the proposal to require payment service providers to publish their APP scam, reimbursement and repatriation levels (Measure 1).** We do not agree with parts of industry which argue that this is likely to help fraudsters or that fair comparisons between firms cannot be made. Instead, greater scrutiny will lead to better incentives on firms to prevent fraud and protect their customers.

- **We support the proposal to require payment service providers to adopt a standardised approach to risk-rating transactions and to share the risk scores with other payment service providers involved in the transaction (Measure 2).** A standardised approach to risk-rating transactions has not developed on its own. The PSR therefore needs to intervene to establish such standards, and to ensure that these are adopted across the industry.

- **We strongly support the proposal for the PSR to require Faster Payments to incorporate a reimbursement obligation into its scheme rules (Measure 3a).** This should cover all types of APP scams and values of payments, rather than arbitrarily excluding certain types of payments such as purchase scams. If a simpler standard of care is required for a scheme rule than is currently included in the CRM Code, then this should be based on the same legal basis that is used for unauthorised fraud, with victims reimbursed except for cases of gross negligence or first party fraud.

- **However, we strongly oppose the proposal for the PSR to require Faster Payments to introduce a new scheme rule ensuring protection to a regulator-approved standard (Measure 3b).** This proposal would be a retrograde step that would take us back to the point in time prior to the CRM Code two years ago. It fails to learn the subsequent lessons of the CRM Code, which has been fundamentally undermined by its voluntary nature and lack of regulatory supervision and enforcement.

- The PSR should urgently implement these measures and outline publicly the wider reforms it needs the government to undertake. There is a wealth of evidence on the issues with the current system from industry, consumer groups, the Financial Ombudsman Service and the Lending Standards Board. The PSR should therefore have outlined specific proposals for each of the measures suggested in its Call for Evidence rather than waiting to ask for further views from stakeholders on the issues. It should also take this opportunity to ensure the government removes any barriers the PSR faces in ensuring there is robust, future-proofed oversight of consumer protection for all types of payment fraud.

Progress to address the significant emotional and financial harm experienced by consumers has been far too slow

It is four and a half years since Which? issued its super-complaint to the PSR on APP scams. We highlighted the glaring gap in fraud protection and redress for fraud via authorised push payments compared to other forms of payment such as debit and credit cards. We specifically called on the PSR to investigate:

- the extent to which banks could reduce consumer harm from APP scams; and
- whether changes in legislation or regulation were required to change the incentives on banks and payment systems to mitigate the risks of APP scams and to protect consumers.

Since then we have seen the number of reported cases and the level of losses both more than treble.[1] Better reporting may have contributed to some extent to these increases, but there is no doubt that the threat of fraud is becoming part of our everyday lives. The coronavirus pandemic has further highlighted that fraudsters will harness anything to their advantage, and that they continually adapt their methods and are extremely sophisticated. The impact of fraud is not just financial, it also has a huge emotional impact on its victims. Action Fraud has identified 300-350 fraud reports a week where victims show signs of severe emotional distress – equaling up to 18,000 reports a year. Worryingly, Action Fraud received 241 phone calls between January and November 2020 where a 'threat to life' was flagged.[2]

Which? remains of the view that the PSR needs to get the incentives on payment service providers and payment systems right in order to mitigate the risks of APP scams as well as to provide redress to consumers. The payments industry needs to take greater responsibility for the harm, given that fraudsters exploit accounts with them and the payment systems that they choose to offer their customers.

The wider ecosystem also needs to do more, including telecommunications providers and social media platforms.[3] Which? and many other organisations have been calling for the government to include scams in its proposed Online Safety Bill. But the PSR should not wait for these wider reforms to address the lack of responsibility currently being taken by the payments industry for the harm done to its customers.

[1] Between 2017 and 2021, the number of reported cases and the level of losses both more than trebled. There were 143,259 cases involving customers with personal bank accounts in 2020, up from 38,596 in 2017. Fraudsters stole £388 million in 2021 compared to £108 million in 2017.
[2] See our analysis of 16 research papers and datasets on the emotional impact of fraud from across the world and from UK police: https://www.which.co.uk/news/2021/03/devastating-emotional-impact-of-online-scams-must-force-government-action/
[3] Recent Which? research found that almost one in 10 people (9%) have fallen victim to online scam ads via social media sites or search engines. https://www.which.co.uk/news/2020/11/nearly-one-in-ten-scammed-by-adverts-on-social-media-or-search-engines/

The voluntary, industry-led approach that the PSR has taken on consumer protection has not resulted in the reduction of harm required

For over a year the PSR has concluded that outcomes for victims of APP scams have been inconsistent and rates of reimbursement insufficient among customers of signatories to the voluntary Contingent Reimbursement Model Code, which is based on the principle that the starting point should be to assume that victims of APP scams should be reimbursed in full. Last March, the PSR's managing director concluded that reimbursement were 'well below the levels of reimbursement that I was expecting'.[4] The PSR's latest assessment identifies 'significant issues' with the CRM Code including that 'reimbursement rates are variable, and arguably too low overall'.[5]

The latest figures from the Lending Standards Board show that signatories to the CRM Code are holding victims fully responsible for being scammed 60% of the time.[6] The Lending Standards Board also found that two firms held scam victims fully responsible for their losses on more than nine in 10 occasions.[7] This follows similar findings a year ago by the PSR which showed that between May 2019 and February 2020 half of the signatory firms had fully reimbursed victims in 6% or fewer of cases, with one firm fully reimbursing just 1% of victims.[8] The sheer scale of the differences between the approaches taken by each firm suggests this is highly unlikely to be explained just by differences in the types of cases that firms deal with or their customer bases.

Victims of different types of scams have also been treated extremely differently. Firms have ruled against victims at a particularly high rate for categories of scams which can involve some of the most sophisticated methods used by fraudsters. Around two-thirds (67%) of decisions on investment scams, where someone is conned into investing in schemes or products that are worthless or may not even exist, found the customer to blame. Decisions on purchase and advance fee scams, two forms of fraud which can involve people being tricked into paying for goods and services that aren't real, each held the customer responsible 65% of the time. For romance scams, which can involve months or even years of grooming, the figure stood at six in ten (61%).[9]

Which? has identified a range of issues with how particular provisions in the CRM Code are being interpreted by some firms (see Appendix 1). We are most concerned that the fundamental principle of reimbursing blameless people who have lost money through bank transfer fraud is not being applied fairly or consistently. The Lending Standards Board and the Financial Ombudsman Service have come to similar conclusions:

[4] Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.5
[5] Payment Systems Regulator (2021), *Authorised push payment (APP) scams: Call for views*, p.18
[6] Lending Standards Board (2021), *Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams:Data analysis*, p.17
[7] Lending Standards Board (2021), *Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams:Data analysis*, p.19
[8] Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, pp.23–24
[9] Lending Standards Board (2021), *Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams:Data analysis*, p.18

- The Lending Standards Board found in a series of reviews of the CRM Code that there 'remain inconsistencies in application and outcomes under the Code'[10] and that 'The presumption in the Code that victims should be reimbursed unless there is a clear ground for attributing blame to the consumer was sometimes reversed so that the customer was held liable in many cases where the bank was not.'[11]
- The Financial Ombudsman Service has concluded that its 'overall impression is that firms are applying the reimbursement provisions inconsistently and in some cases incorrectly – failing to reimburse consumers in circumstances anticipated by the Code'.[12] In 2019/20, the Financial Ombudsman Service upheld an average of 75% of complaints involving cases of APP scams, compared to 32% of complaints in general about banks and 58% in relation to complaints about all types of fraud and scams.[13]

This evidence also shows that allowing industry to simply replace the existing Code with a new, industry-written version - as proposed in Measure 3A - will not resolve the issues faced by victims, given the wide range of outcomes that have occurred under a voluntary regime. Such an approach would not address the lack of effective regulatory supervision and enforcement of the standards in the Code, which explains why firms are able to deviate from the expectations set out in the CRM Code.

Neither voluntary initiatives nor competition can be relied upon to provide the minimum, industry-wide levels of protection that are required

In almost two years since the CRM Code launched, just one of the 400-plus firms that are participants in Faster Payments has chosen to sign up to the Code in addition to the eight firms that initially signed up. There is also just one major firm that offers reimbursement protections that provide a greater level of protection than the CRM Code.[14]

This shows the weak incentives on firms to protect their customers. Consumers are unlikely to be aware of the differences in levels of protection between firms. Even where consumers are aware of differing levels of protection, they are much more likely to choose their provider based on other factors. A regulatory approach that relies solely on voluntary initiatives and competition to deliver basic levels of consumer protection therefore places unrealistic and unfair expectations on consumers.

Mandatory, industry-wide minimum standards are better suited to deal with the contentious issue of reimbursement. They would not preclude firms from providing a greater level of

[10] Lending Standards Board (2021), *Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams*, p.4
[11] Lending Standards Board (2020), Contingent Reimbursement Model Code for Authorised Push Payment Scams: Review of approach to reimbursement of customers – provision R2(1) (c): Summary Report, p.2
[12] Financial Ombudsman Service (2020), *Lending Standards Board Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams: Financial Ombudsman Service response*, p.2
[13] https://www.bbc.co.uk/news/business-55286037
[14] TSB's Fraud Protection Guarantee promises to refund all losses unless customers have been wilfully or recklessly negligent. TSB has said that this has led the firm to reimburse 99% of victims, only rejecting customers whose claims were found to be fraudulent with the customer complicit in the case.

protection, and they are consistent with other parts of the payment industry. Other payment schemes have mandatory rules and policies related to consumer protection against fraud or error, including mechanisms for payments to be challenged and reversed. For example, Section 75 of the Consumer Credit Act ensures that a credit card company is jointly and severally liable for any breach of contract or misrepresentation by the retailer or trader. Direct debits, which are operated by Pay.UK, are covered by the Direct Debit Guarantee. The paying firm is responsible for making any refunds immediately if an error is made in the payment of a direct debit.

Attempts have already been made by some parts of industry to address this gap in protection but these have failed. Which? strongly supported the industry-led proposal in 2019 for Faster Payments to introduce a scheme rule requiring users to pay a fee to refund victims of APP scams in 'no blame' scenarios. Which? and UK Finance wrote a joint letter to Pay.UK urging it to approve the proposal (see Appendix 2). Which? also argued that Pay.UK should go further to help communicate this to consumers in the form of a new Faster Payments Guarantee, similar to the guarantee that Pay.UK oversees for direct debits. However neither the no blame proposal nor our recommendation for a Faster Payments Guarantee have been taken forward by Pay.UK. It is clear that we cannot rely on industry to take forward the necessary action any longer. The PSR and HM Treasury now need to intervene.

The history of Confirmation of Payee also provides clear lessons. Despite the huge potential benefits that the PSR has identified,[15] Confirmation of Payee was considered at least as early as 2011 by the then Payments Council but was only implemented for some customers last year. Without the PSR's specific direction to the largest six banking groups, it would have taken even longer.

Most payment firms still fall outside of the PSR's specific direction, and relatively few firms have opted voluntarily to offer Confirmation of Payee. This means that even the customers of the six largest banking groups are not always able to use Confirmation of Payee because the service requires both the sending and receiving firms to participate. Fraudsters are also likely to shift their behaviour and target payment service providers that do not offer Confirmation of Payee, thereby undermining the potential benefits of Confirmation of Payee. We therefore strongly disagree with the PSR's decision to limit its requirement to implement Confirmation of Payee to six banking groups. The PSR should instead mandate all payment service providers to introduce Confirmation of Payee.

[15] In evidence to the TSC inquiry the PSR said that Confirmation of Payee "would have a significant impact on a certain type of authorised push payment fraud". The PSR's impact assessment estimated that 70% of misdirection fraud will be prevented in its first year, and 75% each year afterward. Payment Systems Regulator (2019), *Confirmation of Payee: Consultation on specific direction*, p.29

We strongly support the proposal to require payment service providers to publish their APP scam, reimbursement and repatriation levels (Measure 1)

The aggregate industry data and anonymised firm-level data on the level of APP scams and reimbursements that we cite above have helped to highlight that APP scams is a growing problem and that rates of reimbursement among signatories to the CRM Code are vastly inconsistent and insufficient based on the PSR's expectations of the CRM Code. However, these data do not show how APP scams have impacted customers of particular firms or how these firms have treated their customers who have been victims. Such data would enable much greater scrutiny of firms' approaches to the prevention of APP scams and consumer protection. This would be particularly helpful for organisations that advocate on behalf of consumers to identify issues within the system, and then to work with policymakers and industry to address them. We agree with the PSR that this would therefore provide strong incentives for firms to do more to prevent APP scams from taking place and to protect customers when they do fall victim.

Some parts of industry have previously argued that naming firms could help fraudsters to identify weaknesses in the system. We take such risks very seriously at Which? when we research and investigate fraud. However, we do not think that publishing high-level data by firms poses a significant fraud risk. Instead, we suggest that publishing these data could primarily help to drive improvements in the system, thereby helping to reduce fraud.

We also do not believe that any challenges in comparing firms on a like-for-like basis should prevent the PSR from proceeding with this measure. There are lots of other areas where regulators require transparency where there are challenges to overcome in comparing fairly. For example, the CMA requires the publication of a service quality league table for personal and business current account providers. The FCA also requires banks to publish details of available services and relevant helplines, as well as figures on how long it takes to open current accounts and replace debit cards.

We also believe that it is important to understand how individual firms are handling complaints that are eventually appealed to the Financial Ombudsman Service. The Financial Ombudsman Service currently only routinely publishes firm-level data for all types of fraud and scams. This includes unauthorised fraud, which has higher levels of mandatory protection. Regular data specifically on APP scams would provide better insight on how firms are treating these cases. The PSR should therefore set out its expectation that the Financial Ombudsman Service should publish data for each provider on the APP scams cases that it receives.

We support the proposal to require payment service providers to adopt a standardised approach to risk-rating transactions and to share the risk scores with other payment service providers involved in the transaction (Measure 2)

Better information sharing between sending and receiving firms is hugely important to prevent APP scams and to help catch fraudsters. The sending firm holds vital information and analysis about the potential fraud risk of a payment, which could be extremely valuable to the receiving firm. A standardised approach to risk-rating transactions has not developed on its own. The PSR therefore needs to intervene to establish such standards, and to ensure that these are adopted across the industry.

There also needs to be better information shared in the other direction to help sending firms understand potential fraud risks, as well as greater intervention by receiving firms when there has been suspicious activities. Which?'s super-complaint identified that a key reason why the market had not evolved to address APP scams sufficiently was the presence of significant externalities, largely arising out of the reliance of the sending firm on the actions of the receiving firm, where the fraudster is operating an account to facilitate the fraud. The PSR should look closely at what information is currently shared by the receiving firm, and set out what more it expects of firms when there is suspicious activity regarding one of its payment accounts.

We strongly support the proposal for the PSR to require Faster Payments to incorporate a reimbursement obligation into its scheme rules (Measure 3a)

Given the lack of any rules or policies on consumer protection within Faster Payments, the scheme through which the vast majority of APP scams take place, it is a reasonable expectation for Faster Payments to incorporate a reimbursement obligation into its scheme rules. This will not happen without the PSR's intervention given the competing interests among Faster Payments' 400-plus participants.

The PSR should require the reimbursement obligation to cover all types of APP scams and all values, rather than arbitrarily excluding certain victims from protection. This would also maintain the principles in the CRM Code that all types of APP scams are covered and all values of payments. We do not believe there are any fundamental differences with purchase scams, as suggested in the Call for Evidence. As with other APP scams, purchase scams involve a fraudster operating an account with a receiving PSP and typically exploiting Faster Payments.

The Lending Standards Board reached a similar conclusion on the scope of coverage for the CRM Code. In its review of the CRM Code it rejected calls to carve out certain types and values of payments. On values it said that 'We would not want to see the Code protections withdrawn from customers to whom smaller losses represent huge impacts, such those on lower incomes, nor would we want to create a message for scammers that lower value losses will be disregarded, thus creating the potential for repeated targeting'.[16]

The PSR notes that a simpler standard of care for consumers than is currently included in the CRM Code may be required to enable a scheme rule to be operationalised. However, the

[16] Lending Standards Board (2021), *Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams*, p.5

Financial Ombudsman Service has been clear that the CRM Code provides firms with 'a clear framework for determining when they should reimburse victims of APP scam'.[17] Worryingly though, some firms are interpreting the CRM Code very differently to the Financial Ombudsman Service. If a simpler standard of care is required for a scheme rule than is currently included in the CRM Code, then this should be based on the same legal basis that is used for unauthorised fraud. This would see victims reimbursed except for cases of gross negligence or first party fraud.

We strongly oppose the proposal for the PSR to require Faster Payments to introduce a new scheme rule ensuring protection to a regulator-approved standard (Measure 3b)

This proposal would be a retrograde step, which would take us back to the point in time prior to the CRM Code two years ago. It fails to learn the subsequent lessons of the CRM Code, which has been fundamentally undermined by its voluntary nature and lack of regulatory supervision and enforcement.

Allowing industry the chance to amend the CRM Code with the aim of providing 'more flexibility for PSPs', as the Call for Views argues, is highly unlikely to address the issue of inconsistent outcomes or to strengthen consumer protections, as the PSR suggests. Greater flexibility is instead more likely to lead to an even wider range of outcomes. The proposal also makes no suggestion as to how any new voluntary standards would be enforced, which has been the central weakness of the CRM Code.

Which? does not have confidence in industry to write new standards for itself for reimbursement, even if these would need to be approved by the PSR. The PSR has not suggested that organisations representing consumers would even be involved in the drafting of a revised code as was the case with the CRM Code. Given the industry's interpretation of the CRM Code to date, their disagreements with the Financial Ombudsman Service and consumer groups on implementation, and the changes that they have proposed should be made to the CRM Code, we are therefore concerned that such a process would lead to an eroding of the existing standards in the CRM Code, including the principle that all types and values of APP scams are protected.

The PSR should urgently implement these measures and outline publicly the wider reforms it needs the government to undertake

The PSR has concluded for more than a year that the outcomes from the CRM Code have not met its expectations, and there is a wealth of evidence on the issues with the current system from industry, consumer groups, the Financial Ombudsman Service and the Lending Standards

[17] Financial Ombudsman Service (2020), *Lending Standards Board Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams: Financial Ombudsman Service response*, p.2

Board. The PSR also acknowledged the need to act a year ago when it said: 'If we do not act, these problems are at risk of getting larger, making it more difficult to resolve them.'[18] The PSR should therefore have outlined specific proposals for each of the measures suggested in its Call for Evidence rather than waiting to gather yet more evidence. We do not believe that further evidence of the problems with the implementation of the CRM Code are required.

The PSR has outlined the barriers to it intervening on reimbursement for some time now but it has not proposed a solution. This Call for Evidence was the opportunity to set out clearly what it needs from the government. The PSR should now urgently set out publicly what legislative and regulatory changes it needs to require Faster Payments to incorporate a reimbursement obligation into its scheme rules.

The payments industry is innovating at rapid speed and it is imperative the PSR has sufficient powers to intervene to protect consumers. The PSR therefore needs to take this opportunity to ensure the government removes any barriers the PSR faces in ensuring there is robust, future-proofed oversight of consumer protection for all types of payment fraud.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that influences politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information, contact Alastair Reed, Principal Policy Adviser
alastair.reed@which.co.uk
April 2021

[18] Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.3

Appendix 1 - An overview of the issues with the implementation of the CRM Code

Last year, Which? published a report which shared some experiences drawn from around 150 victims who have contacted Which? since the CRM Code was launched.[19] The report includes some examples where the CRM Code has been used as the basis for much fairer decisions. However, worryingly we found cases where firms have shown:

- **An over-reliance on victims having ignored warnings.** Firms are able to reject reimbursement if the customer 'ignored Effective Warnings'.[20] In many of the cases that we have been involved with, the customer's bank or building society cited the warnings that they had provided. But the victims we spoke to often didn't remember seeing these, or they did but felt the warning wasn't relevant. Other victims were coached by the fraudster to respond in particular ways and ultimately to ignore the guidance offered in any warning. Despite these issues with warnings, Which? has seen that many firms did not sufficiently consider the circumstances of the fraud and how the warning was perceived by their customers. Firms were primarily concerned with establishing that a warning had been provided, and that the customer had still proceeded with the payment. This was in some cases given as sufficient reason to reject a reimbursement claim.

- **Unreasonable expectations of how victims should have verified who they were paying.** Firms can reject reimbursement if 'the customer made the payment without a 'reasonable basis'.[21] The Code does not state that customers are required to have taken active steps when making a payment. This is because steps that may seem rational to bank staff may not align with how people actually behave. APP fraud can be so convincing that a consumer could have a 'reasonable basis' even without taking extra steps, and they may be rushed into making the payment. However, in some of the examples we have seen, firms have assumed that customers should have taken steps in order to be reimbursed. These issues are partly due to firms not sufficiently taking into account the circumstances of the payment and the sophistication of the fraud, as the Code requires. In some of these examples, the fraudster contacted the victim using the same email, phone or SMS details as a legitimate organisation, including their bank. In other examples, the fraudster was able to convince individuals to download software that then enabled them to access the victim's device remotely.

[19] Which? (2020), *Reimbursement for authorised push payment fraud: Consumer experiences of the Contingent Reimbursement Model Code*

[20] Ignoring is defined as 'by failing to take appropriate action when setting up a new payee, amending an existing payee, and/or immediately before making the payment'. 'Effective Warnings' are defined in the CRM Code by requirements under five themes: understandable, clear, impactful, timely and specific. Most significantly, warnings should be impactful in that they 'positively affect customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced'. Lending Standards Board, *Contingent Reimbursement Model Code for Authorised Push Payment Scams*, p.8 & p.12

[21] 'In all the circumstances at the time of the payment, in particular the characteristics of the Customer and the complexity and sophistication of the APP scam, the Customer made the payment without a reasonable basis for believing that: the payee was the person the customer was expecting to pay; the payment was for genuine goods or services; and/or the person or business with whom they transacted was legitimate.' Lending Standards Board, *Contingent Reimbursement Model Code for Authorised Push Payment Scams*, p.12

- **A failure to properly assess vulnerability.** The CRM Code states that firms 'should provide a greater level of protection for customers who are considered vulnerable to APP fraud' and these customers should be reimbursed regardless of their actions.[22] Some victims we have spoken to say that their banks seemed uninterested in the specific details or nature of the scam, even though this could inform their assessment of vulnerability.

- **Poor communications with victims.** Which? has seen many examples where firms have not provided the customer with the reasoning for their decision not to reimburse, have used vague terms to explain the decision or simply say the victim will not be reimbursed because they authorised the payment. Others make no mention that the firm has signed up to the CRM Code or, where they do discuss the Code, they do not say that reimbursement could be possible under the CRM Code or that the firm has assessed their customer's actions and the firm's actions against the requirements of the Code.

We called on the Lending Standards Board to urgently work with firms to ensure they:

- **test warnings to see if they are 'effective';**
- **base their judgements of what is reasonable on evidence of actual customer behaviour;**
- **train all relevant staff in how to identify customers who could be or may have been vulnerable to APP fraud; and**
- **provide victims with specific reasons to explain reimbursement decisions**

[22] Crucially, vulnerability should be assessed on a case-by-case basis, and the definition is much broader than being mentally or physically unwell. The Code states: 'A customer is vulnerable to APP fraud if it would not be reasonable to expect that customer to have protected themselves, at the time of becoming victim of an APP scam, against that particular APP scam, to the extent of the impact they suffered.' Lending Standards Board, Contingent Reimbursement Model Code for Authorised Push Payment Scams, p.13

Appendix 2: Joint letter from Which? and UK Finance to Pay.UK, 08/10/2019

Dear Ms Johnson

This joint letter from Which?, the largest consumer organisation in the UK, and UK Finance, on behalf of HSBC, Santander, Barclays, Lloyds, Metro, Nationwide and RBS follows the Pay.UK Call for Information and is in support of the Faster Payment Scheme (FPS) Change Request. Authorised Push Payment (APP) fraud is a crime which can have a devastating impact on its victims, which is why protecting consumers is a priority for us all.

The launch of the voluntary Contingent Reimbursement Model Code in May set a new standard of consumer protection from this type of fraud, with a commitment from signatory firms to reimburse victims provided the customer has met the standards expected of them under the Code. The Code was produced by the APP Scams Steering Group, which was composed of representatives from consumer groups, the finance industry, government bodies and regulators.

'No blame' fund

The proposal set out in the Change Request for an FPS CRM fee will provide a long-term, sustainable funding system for the reimbursement of victims of APP scams under the voluntary Code in situations where both the customer and payment service provider (PSP) have done everything expected of them, known as a 'no blame' situation. Funds gained from the FPS fee will be held centrally in a 'no blame' fund.

If the Pay.UK board fails to pass the Change Request, many victims of APP scams could once again risk losing their life savings to this devastating crime. Following consultation on seven funding options, with responses received from 34 stakeholders, including many Pay.UK participants, the Steering Group agreed that the FPS model is the best method to ensure that reimbursement for blameless victims continues beyond the end of this year.

As well as providing reimbursement in a 'no blame' situation for customers of PSPs which are signatories to the Code, the proposed model represents the only long-term funding option that also guarantees customers will be covered if their PSP is not a signatory. If a customer is a victim of an APP fraud and their PSP is not signed up to the Code, they will be able to take their case to the Financial Ombudsman Service which will have the power to refer the PSP to the 'no blame' fund to reimburse the customer.

Reducing APP scams

The proposed fee would provide a financial incentive for the firms involved in push payments to individually and collectively reduce APP scams, above and beyond the minimum requirements in the Code. The protection that the fee offers consumers could also benefit payment providers and Pay.UK by strengthening trust among consumers in the Faster Payments Service. The

Faster Payments Service was designed for speed and convenience. Unfortunately, sensible pro-customer and pro-growth measures are being exploited by criminals.

Latest data from UK Finance shows that in the first six months on 2019, 95 per cent of all APP fraud involved a customer making a Faster Payment. Therefore, it is important for Pay.UK to consider the part it can play in the fight against this growing fraud, by recognising that it has the power to take decisive action to protect end users.

The FPS Change Request, submitted to Pay.UK in June, provides a mechanism to achieve this consumer protection. As well as being the decision of the APP Scams Steering Group, the Change Request also demonstrably fits with Pay.UK's strategic objectives. Specifically, these include being "end user focussed" and "acting as a catalyst for change in the payments industry; addressing threats; and supporting industry-wide initiatives.

Protecting consumers

The fight against rising APP fraud has become an issue for society to tackle. Pay.UK is supporting these efforts with its work to introduce the Confirmation of Payee service. Careful consideration of the case for the CRM FPS Fee is now needed, as Pay.UK assesses the responses to its Call for Information.

This well-thought through and widely supported option is proportionate to payment providers of different sizes, consistent with the APP Scams Steering Group proposals, and widely supported by consumer bodies and much of the financial industry. We urge the Pay.UK board to accept this proposal, and put the protection of consumers at the heart of its decision.

Yours sincerely,

Anabel Hoult, CEO of Which?
Stephen Jones, CEO of UK Finance