Written evidence submitted by Which?

Introduction

1) Which? is the UK's consumer champion. As an organisation we're not for profit - a powerful force for good, here to make life simpler, fairer and safer for everyone. We're the independent consumer voice that provides impartial advice, investigates, holds businesses to account and works with policymakers to make change happen. We fund our work mainly through member subscriptions. We're not influenced by third parties – we never take advertising and we buy all the products that we test.

2) Which? welcomes the opportunity to submit written evidence to this important inquiry. We were pleased to be able to feed into the previous Committee's inquiry into Economic Crime through written and oral evidence, and we hope this submission enables the Committee to see clearly how consumers continue to be impacted by various types of economic crime in the UK.

3) Since we last gave evidence to the Committee, the urgent need to implement strong measures to tackle various types of economic crime has increased as a result of the wide-scale impact of the coronavirus pandemic. It is clear that criminals are exploiting and adapting to the pandemic, and this is shown by a distinct rise in online data harvesting and a fall in cheque and contactless card fraud as a result of criminals' lack of ability to commit traditional types of fraud. For example, in September 2020, UK Finance found that losses to investment scams rose by 27% to £55.2 million in the first half of 2020, the largest increase of any scam type.

Summary

4) This submission focuses on two key areas of economic crime where people are being failed by the existing regulatory system. The first is the growing prevalence of online scams - particularly in light of the ongoing coronavirus pandemic - and the lack of protection afforded to users of online platforms, including social media sites and search engines. The second is the inadequacy of the preexisting voluntary Contingent Reimbursement Model Code for reimbursing victims of authorised push payment (APP) scams to provide effective redress for victims.

5) Scammers have been quick to adapt to the new reality of people working, shopping, and socialising from home, and coronavirus has been an effective 'hook' that has led to a surge in online scams this year.[1] However, online platforms - sites that host user-generated, third party content, including search engines and social media companies - which have become part of people's everyday lives have no legal obligation to protect users from scams on their sites and their voluntary measures have been ineffective in preventing scammers from operating to target victims on their sites. As scammers use increasingly sophisticated and convincing scam tactics, this lack of protection leaves online users extremely vulnerable.

6) Victims of online scams, as well as those who are not properly protected by the current APP reimbursement model, often suffer huge financial and emotional distress. Investment and

[1] UK Finance (2020), 'Criminals exploit coronavirus as fraud moves increasingly online' https://www.ukfinance.org.uk/press/press-releases/criminals-exploit-covid-19-fraud-moves-increasingly-online#summary

insurance scams in particular can cost people tens or hundreds of thousands of pounds, with figures showing that the number of investment scams has quadrupled since the first lockdown in March.[2] Smaller scale purchase scams for individual items may have a lower monetary value, but the relative impact can be huge, particularly for financially vulnerable people. Which? research indicates that as many as 3.8 million people might have fallen victim to a scam from an advert that appeared on their social media feed.[3]

7) Victims of APP scams - i.e. those who have authorised a bank transfer payment to someone who turns out to be a scammer - currently face a lottery of protection when it comes to whether or not they will be reimbursed by their bank, even if they they are found not to be to blame under the principles of the Code, due to banks interpreting and implementing the Code in a variety of ways. The voluntary Contingent Reimbursement Model (CRM) Code has improved customer protections to some extent; however, there are significant issues in the current operation of the Code which we believe can only be resolved by replacing it with a mandatory scheme.

8) Which? believes that much stronger regulatory frameworks are required to both prevent people from becoming victims of scams through online platforms, and to provide certainty and protection to those who do fall victim to APP scams. The Government has the perfect opportunity to improve prevention of online scams through the current Online Harms Bill. With the greater role they play in our everyday lives, online platforms must be given legal responsibility for preventing scam content from appearing on their sites, as well as more responsibility for taking effective action to remove harmful content when it is reported.

9) Similarly, the current voluntary Contingent Reimbursement Model Code for victims of APP scams should be replaced with a mandatory scheme providing regulatory oversight and giving all victims full protections regardless of who their account is with. The PSR has stated that it cannot act to mandate the Code due to restrictions under an EU Directive. Therefore we would recommend that following the end of the Brexit transition period, the Government should use its regained legal powers to bring forward legislation to enable the creation of a statutory code overseen by a regulator. This would replace the existing voluntary CRM Code to provide victims with stronger protections and enable oversight of the implementation of the Code which is currently lacking.

Emerging trends in consumer-facing economic crime as a result of the coronavirus crisis

10) Scams and fraud are now the most prevalent types of crime in the UK, resulting in growing numbers of people losing life-changing sums of money, as well as taking a significant emotional toll on victims and in many cases causing serious harm to people's mental and physical health. Based on regular reports received from scam victims, and through our research and investigations, we have identified two key trends in this type of economic crime as a result of coronavirus.

11) Firstly, scammers have been quick to adapt to the crisis. While scammers have continued to use sophisticated techniques and tricks to draw in victims, an increasing number have used coronavirus as the "hook" for these crimes.[4] This is of particular concern at a time when

[2] BBC (2020), 'Coronavirus: Investment scams quadruple since virus lockdown' https://www.bbc.co.uk/news/business-55126228

[3] Which? (2020), 'Nearly one in ten scammed by adverts on social media or search engines' https://www.which.co.uk/news/2020/11/nearly-one-in-ten-scammed-by-adverts-on-social-media-or-search-engines/

changes to people's lifestyles may increase their exposure to scams and make it more difficult for individuals to recognise them. For example, higher levels of stress due to lockdown or financial hardship may lead to people being less vigilant when it comes to spotting a scam.

12) Secondly, social media and other online platforms are playing a growing role in enabling scammers to reach internet users and defraud them. The coronavirus pandemic has accelerated this trend with more people now reliant on online activity and spending more time online. It is therefore evident that the pandemic increases individuals' vulnerability to scams due to profound changes to people's lifestyles. Yet online platforms currently have no legal obligation to protect users against scams on their sites, placing an unreasonable burden on people to protect themselves.

Online platforms are not doing enough to protect users from online scams

13) Online platforms bring huge benefits for consumers in the form of greater choice, convenience and lower costs. The services provided by online platforms - sites that host user-generated, third party content - are now an essential part of daily life, allowing people to shop, socialise, and work with greater ease than ever. This reliance on digital services has increased significantly as a result of the coronavirus pandemic. However, there is significant evidence that the lack of clear legal responsibilities on platforms to ensure the safety of their users has left consumers increasingly exposed to fraud, safety risks, and misleading information from the content hosted on these sites.

The scale and range of online scams

14) Online platforms, including social media sites and search engines, are playing a growing role in enabling criminals to reach and defraud internet users. Action Fraud estimates that in the year to June 2020, 85% of all fraud was cyber-enabled and that the use of social media is increasing in all aspects of fraud.[5] Consumers face a growing variety of online scams when navigating the digital world, with scammers using an increasingly sophisticated range of tactics and guises as the "hook" to dupe people. They also utilise a range of different channels, including paid-for adverts on online platforms and organic, user-generated content on the sites to reach victims. Given that people are spending a higher proportion of their time online, we are concerned that more people than ever before are exposed to social engineering and grooming techniques used by scammers. For example, by April 2020, at the height of the first lockdown, UK adults were spending on average over four hours a day online - up from just under three and a half hours in September 2019.[6]

15) Our investigations have found that prominent types of online scams target those who are looking for investments, insurance, pension advice, online shopping, and even those seeking debt help. Recent Which? investigations have uncovered impersonator ads appearing in Google search results for insurance and investment firm Aviva,[7] financial technology company Revolut,[8] and debt charity StepChange. Action Fraud figures show the total number of fraud

---

[4] Financial Times (2020), 'Facebook allowed thousands of illegal ads in UK until they were reported' https://www.ft.com/content/1aba8d75-823e-488f-88fe-15ee51f3f0ab

[5] Action Fraud (2020), 'Fraud Crime Trends 2019–20' https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf

[6] Ofcom (2020), 'Online Nation'

[7] Which? (2020), 'How scammers use Google to lure victims' https://www.which.co.uk/news/2020/09/browser-beware-how-scam-advertisers-use-google-to-lure-their-victims/

[8] Which? (2020), 'Google fails to stop scam ad targeting Revolut users for a third time' https://www.which.co.uk/news/2020/09/google-fails-to-stop-scam-ad-targeting-revolut-users-for-a-third-time/

reports they received in the year to June 2020 was 822,276 and the value of losses from reported incidents was £2.3 billion.[9]

Inadequate action from online platforms to protect users from online scams

16) Yet we continue to find that online platforms do not currently have adequate systems and processes in place to prevent fraudulent content from appearing on their sites. Our investigations have exposed a lack of effective controls on Facebook and Google that could allow fraudsters to create and post fake adverts to target victims within a matter of hours.[10] This can result in people losing devastating amounts of money as well as accessing other harmful content - one victim lost almost £100,000 after clicking on an online investment advert featuring fake celebrity endorsements from Martin Lewis and Deborah Meaden, while another lost £160,000 after clicking on an ad for an 'Aviva' investment scheme.

17) We have received hundreds of reports in the last 3 months of people falling victim to social media purchase scams and have uncovered a number of ways in which scammers are exploiting the lack of checks and the ability to target and reach victims online, including:

- ☐ **Scams perpetrated through paid-for adverts on social media sites and search engines taking place on a widespread scale.** Our research found that almost one in 10 people (9%) in the UK have fallen victim to a purchase scam - when a consumer is misled into paying in advance for goods that are never received or are not at all as described - via an advert on a social media site. The same proportion of people (9%) had fallen victim to a scam advert via a search engine.[11]
- ☐ **Organic, user-generated scam content which is extremely easy to find on social media platforms.** Our investigations have uncovered scammers openly selling personal information that has been captured illegally on Facebook, Instagram and Twitter. Which? was able to find 50 scam profiles, pages and groups on the sites promoting the sale of a mixture of stolen identities, credit card details and compromised accounts.[12]

18) Voluntary initiatives introduced by platforms to date have been insufficient to tackle online scams. While platforms have implemented some measures to deal with scam adverts, many of these rely on users having to report ads, creating an overreliance on consumers to protect themselves. Our survey of Facebook users showed only three in 10 users were aware of the social media site's scam advert reporting tool while only one in 10 users had used the tool.[13]

19) In addition to users' lack of awareness of the tool, there are several challenges that limit the effectiveness of this initiative, including people's inability to spot scams and behavioural barriers that deter people from engaging with the tool. Additionally, Google's advertiser verification scheme will allow ads to run before advertisers have been verified, creating a window that scammers may look to exploit.

Which?'s recommendations for tackling online consumer scams

[9] Action Fraud (2020), 'Fraud Crime Trends 2019–20' https://data.actionfraud.police.uk/cms/wp-content/uploads/2020/07/Fraud-crime-trends.pdf

[10] Which? (2020), 'Fake ads; real problems: how easy is it to post scam adverts on Facebook and Google?' https://www.which.co.uk/news/2020/07/fake-ads-real-problems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/

[11] Which? (2020), 'Nearly one in ten scammed by adverts on social media or search engines' https://www.which.co.uk/news/2020/11/nearly-one-in-ten-scammed-by-adverts-on-social-media-or-search-engines/

[12] BBC (2020), 'Facebook and Twitter allow scammers 'free rein'' https://www.bbc.co.uk/news/technology-52471837

[13] Which? (2020), 'Connecting the world to fraudsters?' https://www.which.co.uk/policy/digital/6514/connectingfraudsters

20) The ineffectiveness and lack of consistent voluntary measures introduced by platforms demonstrate the need for a strong regulatory framework, with the responsibilities of online platforms brought more in line with consumers' expectations and the role the sites play in our everyday lives.

21) Online platforms should be given a legal responsibility for preventing scam content from appearing on their sites, as well as more responsibility for taking quick action to remove harmful content when it is reported. To prevent scams, online platforms should:

    - ☐ Have clear site conduct policies that block bad actors from accessing services.
    - ☐ Have easily accessible and easy to use systems that allow users to report ads that may expose consumers to illegal activities, including fraud, safety issues, and disinformation.
    - ☐ Take down reported ads that enable illegal activities, including fraud, safety issues, and disinformation, within a defined time period.
    - ☐ Where content or ads have been identified as fraudulent and been removed, alert those users who have engaged with the content about why it has been removed and notify them of their options for redress.
    - ☐ Prevent ads from being relisted where they have been taken down.
    - ☐ Report illegal activities including fraud, safety issues, and disinformation to the appropriate regulatory and law enforcement bodies.

22) We believe these measures that would require platforms to take reasonable steps to identify and prevent illegal user-generated content from appearing on their sites are consistent with the expectations and Duty of Care approach within the forthcoming Online Harms Bill. We therefore strongly recommend for scams to be included within the scope of the legislation.

23) There is widespread support for this with Which?, UK Finance, Carnegie UK Trust, the Government's Joint Fraud Taskforce, and the Financial Conduct Authority (FCA) all calling for the scope of the new regulatory framework to include online scams, requiring online platforms to play a greater role in protecting people from fraud. This will help ensure online platforms better support regulators and enforcement authorities in the fight against scams online and avoid the need for regulators such as the FCA to resort to paying for adverts on Google warning people about the risk of online scams. Therefore if online scams are not addressed through Online Harms legislation, it is imperative the Government sets out plans to effectively protect people from scams.

Opportunities are being missed to tackle online scams

24) While there are several initiatives being progressed by the Government and regulators that may tackle aspects of online scams, such as DCMS' work on digital advertising, the Treasury's work on financial promotions, and the FCA's Consumer investments call for input, there is a growing risk that current plans for future regulatory frameworks are not taking a comprehensive approach to the threats faced by consumers and loopholes such as a lack of regulation of organic, user-generated content will be exploited by scammers.

25) It is critical that relevant government departments and regulators are working together to deliver a joined-up approach to tackling online scams. Unless online platforms are required to actively tackle this problem, the harm from scams will continue to grow with devastating consequences for people, in particular those in vulnerable circumstances.

26) We would welcome the Committee exploring the following as part of its inquiry:

- ☐ The effectiveness of online platforms' current systems and processes for protecting their users and preventing fake and fraudulent adverts from appearing on their sites.
- ☐ The adequacy of the current incentives for, and legal responsibilities of, online platforms to take appropriate action to deal with fraudulent content on their sites.
- ☐ The effectiveness of the Government and regulators' approach to regulatory reform to dealing with rising online scams.

The operation of the Contingent Reimbursement Model for Authorised Push Payment Fraud

27) When the voluntary CRM Code was introduced in May 2019, Which? welcomed it as a positive step forward for victims of APP scams. Our 2016 super-complaint highlighted the glaring gap in APP scams protection and redress compared to other forms of payment such as debit and credit cards. The voluntary Code has made some progress to address these issues by committing bank signatories to work to prevent APP scams and reduce the impact on those who fall victim to them.

28) However, the voluntary agreement with no formal regulatory oversight is limited in success as the operation of the CRM Code has yet to provide comprehensive protection for all victims. There is still not universal sign-up to the Code and reimbursement rates remain far below what was expected. Our review of over 150 cases has highlighted that the Code is not being understood and implemented in a common, coherent way by signatories, and a lack of official regulatory oversight has led to the Financial Ombudsman Service becoming the de facto decision maker on how the Code should be interpreted. Due to these issues with the operation of the Code, Which? agrees with this Committee's 2019 report recommendation that the Code should be made mandatory. We believe that the Treasury should take the opportunity of the post-Brexit transition legal landscape to introduce legislation in 2021 to enable the creation of a mandatory scheme instead.

29) Given the huge losses to APP scams that are being reported - over £200m in the first six months of 2020 alone - we welcome the Committee revisiting the operation of the current Code and future reform. Alongside the recent consultations by the Lending Standards Board and the Treasury on this issue, we hope that this renewed focus on APP scams and the CRM Code across industry, the Government, and Parliament will result in positive changes for consumers and victims.

Reimbursement rates by signatories of the Code remain too low

30) In the past year, there has been an increase in the share of victims being reimbursed under the Code. In the full year before the Code launched, only 19% of the amount lost by individuals was returned. In comparison, in the first six months after the Code's launch industry figures show that signatory firms reimbursed 41%,[14] and in the second six months, 38% was reimbursed.[15] Yet, while this increase is to be welcomed, we agree with the Payment Systems Regulator (PSR) which has made clear that it believes that rates of reimbursement remain "well below the levels" that it expected.[16] The situation is even more

[14] UK Finance (2020), 'Fraud – The facts 2020: The definitive overview of payment industry fraud', p.46

[15] UK Finance (2020), '2020 Half year fraud update', p.23

concerning when broken down at an individual firm level. Anonymised data published by the PSR earlier this year shows that between May 2019 and February 2020:

- ☐ Four of the eight signatory firms had fully reimbursed victims in 6% or fewer of cases, with one firm fully reimbursing just 1% of victims; in contrast one firm had fully reimbursed 59% of victims.
- ☐ Some firms had chosen to partially reimburse a significant share of cases, including one firm that partially reimbursed 93% of cases; whereas another firm partially reimbursed just 1% of cases and another firm just 3% of cases.
- ☐ The value reimbursed also varies significantly, with one firm reimbursing just 6% of the value of cases compared to another firm that reimbursed 63% of the value of cases.[17]

31) The scale of the differences in approach taken by each firm indicates that it is highly unlikely to be simply due to differences in the types of cases that firms deal with or the makeup of their customer bases. The findings clearly show that some firms are taking advantage of their decision-making position in their approach to the reimbursement of their customers, and that a lack of regulatory oversight of the Code is allowing it to be interpreted and implemented in vastly different ways by individual signatories. This demonstrates that the CRM Code is not operating in a way where every victim can be confident that their complaint will be handled in a standardised way.

Firms are not meeting the Code's standards

32) Which?, the Payment Systems Regulator,[18] the Financial Ombudsman Service,[19] and the Lending Standards Board's interim review[20] have all found significant issues with reimbursement decisions taken by signatories. Which? has seen and helped intervene in cases where there have been issues with the following:

An over-reliance on Effective Warnings

33) Under the terms of the CRM Code, firms are able to reject reimbursement if the customer is determined to have *"ignored Effective Warnings"*. There are several relevant definitions and guidelines included in the Code. Most significantly, the Code stipulates that 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"*.

34) In many of the cases that Which? has been involved with, the customer's bank or building society cited the warnings that they had provided. However, the victims we spoke to often didn't remember seeing these, or they did but felt the warning wasn't relevant. Even more concerningly, some victims were coached by the scammer to respond in particular ways and ultimately to ignore the guidance offered in any warning.

35) Which? has seen clear examples where many firms did not sufficiently consider the circumstances of the scam and how the warning was perceived in context by the victim, as

[16] Payment Systems Regulator (2020), 'Authorised Push Payment (APP) scams conference call – 30 March 2020', p.5

[17] Payment Systems Regulator (2020), 'Authorised Push Payment (APP) scams conference call – 30 March 2020', pp.23–24

[18] Payment Systems Regulator (2020), 'Authorised Push Payment (APP) scams conference call – 30 March 2020'

[19] Financial Ombudsman Service (2020), 'Response to Lending Standards Board Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams' https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/07/LSB-CRM-Code-Consultation-document.pdf

[20] 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'

required by the CRM Code. Firms appeared primarily concerned with establishing that a warning had been provided and that the customer had still made the payment. This was in some cases given as sufficient reason to reject a reimbursement claim. The Financial Ombudsman Service reported similar concerns in their response to the LSB's review of the CRM Code in October 2020.[21]

36) Through our engagement with industry we have seen many different types of warning presented as examples of an 'effective warning'. However, there is no coherent agreement across industry on what such warnings should look like or how they could be measured. Some firms have acknowledged that more needs to be done in order to understand just how effective these online or mobile app-based warnings are in preventing people from making payments to scammers. We are concerned that firms are relying on 'effective warnings' to reject claims without providing evidence that they are actually effective. Separately, the Financial Ombudsman Service has also proposed that firms should "do more to evidence the effectiveness of their warnings and to differentiate in their case handling between warnings that may meet the definition of an effective warning and those that don't".[22]

37) Which? recently found an example of a bank's mobile app that did not show Confirmation of Payee warnings to some Android and iPhone users for 31 days.[23] Though the bank rectified the issue as soon as we brought it to their attention, the fact that it had not been noticed prior to our investigation is extremely worrying given the reliance firms have on the existence of these warnings to deny reimbursement.

38) We would therefore welcome the Committee exploring how firms define 'effective warnings' and what evidence they have that they work in actively preventing people from making payments to scammers.

Unreasonable expectations of how victims should have verified who they were paying

39) Under the terms of the CRM Code, firms can reject reimbursement if *"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."* In making these judgements, firms are required to consider *"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."*

40) This 'reasonable basis' test 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 consumers actually behave. APP scams can be so convincing that a consumer could have a *"reasonable basis for believing"* even without taking extra steps, and they may be rushed into making the payment.

41) However, in some of the decisions seen by Which?, firms have asserted that customers *should* have taken certain steps, and because they did not they have had their reimbursement claims denied. 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

[21] Financial Ombudsman Service (2020), 'Response to Lending Standards Board Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams' https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/07/LSB-CRM-Code-Consultation-document.pdf

[22] Payment Systems Regulator (2020), 'Authorised Push Payment (APP) scams conference call – 30 March 2020', p.16

[23] Which? (2020), 'Starling Bank fraud warning system failed Android users for 31 days' https://www.which.co.uk/news/2020/11/starling-bank-fraud-warning-system-failed-android-users-for-31-days/

requires. The FOS has reported similar observations.[24] In some of these examples, the fraudster contacted the victim using the same email, phone or SMS details as a legitimate organisation, such as their bank or solicitor. In other examples, the fraudster was able to convince individuals to download software that then enabled them to access the victim's device remotely.

42) We are concerned that these varied interpretations by signatory firms are undermining the efficacy of the operation of the Code, and that the lack of regulatory oversight is resulting in a failure to properly intercept and address such issues.

A failure to properly assess vulnerability

43) The CRM Code states that firms *"should provide a greater level of protection for customers who are considered vulnerable to APP fraud"* and that these customers should be reimbursed regardless of their actions. 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."* Despite this, it remains unclear to us how firms are defining vulnerability and whether they are taking into account the context of the scam and its subsequent impact on the victim's behaviour.

44) Which? has seen examples where banks have considered vulnerability carefully, including the impact of the fraud on the victim. Yet some victims we've 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. One victim was initially rejected for reimbursement and it was only when Which? intervened that her bank considered fully that she had been undergoing extensive medical treatment when she became a victim.

Poor communications with victims

45) Which? has seen many examples where firms have not provided the customer with written reasoning for their decision not to reimburse. We have seen other examples where vague terms have been used to explain the decision. Some letters say that the victim *"could have taken more responsibility and conducted checks prior to making the payment"*. This is very concerning as judgment on "responsibility" is not derived from the CRM Code. These letters also do not provide any specific suggestions as to the types of checks that the victims could have conducted, which limits victims' ability to ensure this does not occur again. Similar observations have been recorded by other organisations, including the FOS.[25]

46) The worst examples we have seen, however, state that the victim will not be reimbursed simply because they authorised the payment, which is in direct contravention of the Code. One letter explains that the customer had authorised the payment and *"therefore, the bank cannot accept liability and offer you a refund or any redress."* Another letter states that:

> *"...as you have willingly made the payment out of your account...the bank cannot treat this as a fraudulent act. As a bank we have acted on your genuine instruction to*

[24] Financial Ombudsman Service (2020), 'Response to Lending Standards Board Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams' https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/07/LSB-CRM-Code-Consultation-document.pdf

[25] Financial Ombudsman Service (2020), 'Response to Lending Standards Board Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams' https://www.lendingstandardsboard.org.uk/wp-content/uploads/2020/07/LSB-CRM-Code-Consultation-document.pdf

process the transfer you have made. Therefore we cannot be held responsible for the loss you have incurred, nor can we look to refund the outstanding amount."

47) Which? has also seen numerous examples of firms sending letters to their customers regarding a decision not to fully reimburse that make no mention of the CRM Code. Many other letters mention the Code but provide no indication that reimbursement could be possible under the Code or that the firm has assessed their customer's actions and the firm's actions against the requirements of the Code.

Long-term funding for cases which are determined to have "no blame"

48) The CRM Code created a 'no blame fund' to provide a pool of money for signatories to draw on in the event of a determination that neither the firm nor the victim should take responsibility for the scam. There was no explicit guidance on how this fund should be financed, however, and signatories have therefore agreed temporary agreements which have had to be re-agreed around every six months. Without a long-term funding arrangement, the voluntary Code risks being undermined as 'no-blame' victims will risk losing money that should have been reimbursed under the principles of the Code, and industry will have limited confidence in the long-term viability of the scheme.

49) We believe that a permanent industry fund would provide stronger incentives for industry to work together to reduce APP fraud, including at a systemic level. It is a failing of the Code that such a mechanism has not been able to be secured as the fund was only ever referenced in the language of the Code, but responsibility and guidance for creating the fund was not provided. A mandatory scheme would provide a solution to this, as the Government and / or overseeing regulator could provide clear direction on a long term funding solution.

Which?'s suggested remedies

50) In our 2016 super-complaint to the PSR we called on them to investigate:

- ☐ The extent to which banks could reduce consumer harm from authorised push payment (APP) fraud.
- ☐ Whether changes in legislation or regulation were required to change the incentives on banks and payment systems to mitigate the risks of APP fraud and to protect consumers.

51) The CRM Code is the most significant change to have come off the back of the PSR's investigation and we welcome the positive work that has been done since its introduction in May 2019. We are clear, however, that the Code in its current form is not capable of considerably reducing consumer harm from APP scams. The evidence we have laid out demonstrates this: reimbursement rates remain relatively low and a wide variety of interpretations of the Code has created a lottery of protection; signatory banks are not fully respecting or implementing key aspects of the Code around effective warnings, vulnerability of victims, and contextualisation of customer behaviour, all of which are designed to reduce harm; and the ongoing issue with securing long-term funding of the 'no blame fund' demonstrates the need for legislative change in order to have the regulator provide clear direction on the future of the fund.

52) Which? believes that the current voluntary CRM Code should be replaced with a mandatory scheme to establish a set of minimum industry standards. This is a view shared by UK Finance[26] and echoes the call made by the previous Committee in their Economic Crime

inquiry report in 2019.[27] As well as ensuring that all payment providers offer the same protections, it would also enable the requirements to be enforced effectively and consistently. A mandatory scheme would provide more certainty on issues like funding for 'no blame' cases which are currently decided by time-limited industry agreements.

53) Mandatory standards would not preclude firms from providing a greater level of protection. TSB's Fraud Protection Guarantee, for example, already 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.[28]

54) The PSR has made clear that, in its view, it currently lacks the powers to take action on reimbursement. This is based on the PSR's interpretation of the EU Second Payment Services Directive - notably that it expressly prohibits EU member states (and the UK during the transition period) from forcing payment service providers to go beyond the terms set out in the Directive.[29] This will no longer be the case after 31st December 2020. Which? therefore believes that the Government should take the opportunity following the end of the Brexit transition period to use the powers it has regained and bring forward legislation to enable the creation of a mandatory scheme overseen by a regulator. This would provide victims with stronger protections and enable oversight of the implementation of the Code which is currently lacking.

55) Therefore we would welcome the Committee exploring the following as part of its inquiry:

- ☐ The inconsistencies in the interpretation and application of the Code by signatory banks and the relatively low reimbursement rates comparative to the expectations of the Code.
- ☐ The evidence base for specific elements of the Code which are regularly used by banks to deny full or any reimbursement, particularly effective warnings and the consideration of vulnerability in the context of a scam.
- ☐ The role of the PSR in providing regulatory oversight and direction for the current Code.
- ☐ The options open to creating a mandatory scheme to replace the existing Code, with particular focus on legislation which could be brought forward by the Government.

December 2020

[26] The Guardian (2020), 'Which? calls for all banks to adopt anti-fraud measures' https://www.theguardian.com/money/2020/mar/17/which-calls-for-all-banks-to-adopt-anti-fraud-measures

[27] House of Commons Treasury Committee (2019), 'Economic Crime: Consumer View', p.29

[28] TSB (2020), 'TSB reveals 100 percent reimbursement rate for innocent victims through the TSB Fraud Refund Guarantee' https://www.tsb.co.uk/news-releases/fraud-refund-guarantee-100-reimbursement-rate/

[29] Payment Systems Regulator (2020), 'Authorised Push Payment (APP) scams conference call – 30 March 2020', pp.9–10