Which?

POLICY RESEARCH REPORT AUGUST 2020

# Reimbursement for authorised push payment fraud

## Consumer experiences of the Contingent Reimbursement Model Code

# Foreword

It's just over a year since eight of the UK's major banks and building societies signed up to the UK's first set of standards detailing how to treat victims of authorised push payment (APP) – or bank transfer – fraud. Which? welcomed the Contingent Reimbursement Model (CRM) Code as a significant step forward. Our 2016 super-complaint 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. The voluntary code introduced in May 2019 is designed to give victims the chance of fairer and more consistent redress.

The scale of APP fraud has grown rapidly over recent years. Between 2017 and 2019, the number of reported cases and the level of losses both roughly trebled. 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.

The overwhelming priority must be to prevent fraud. Signatories to the CRM Code have committed to protect their customers with procedures to detect, prevent and respond to APP fraud. While much of this fight against fraudsters is out of sight, we believe the Code has helped to provide renewed impetus. In particular, we've seen firms introduce warnings for customers that are tailored to the purpose of the payment. But banks and building societies are just part of the solution. We need a holistic approach to tackling fraud that also targets fraud enablers. So Which? believes the whole ecosystem needs to do more, including telecommunications providers and social media platforms.

Given the life-changing amounts of money that some victims lose, we also need to reduce the impact of APP fraud. In the past year, we have seen an increase in the number of victims being reimbursed. We have seen examples where the CRM Code has been used as the basis for much fairer decisions. We have also started to see a shift in firms being more compassionate and understanding of the sophistication of fraudsters' practices, as well as the emotional and financial harm caused by this crime.

However, Which? is 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's recent evaluation of the way firms have approached parts of the consumer requisite level of care highlighted inconsistencies in how different firms are applying the Code. The Financial Ombudsman Service has highlighted similar issues, and the Payment Systems Regulator also expressed its concern that rates of reimbursement are lower than expected.

In this report we share some experiences drawn from around 150 victims who have contacted Which? since the CRM Code was launched. Some are major success stories for the Code: examples of innocent victims who had been facing financial ruin being fully reimbursed by their bank or building society. But many others involve firms unjustly refusing to reimburse their customers, and highlight the inconsistent approaches being taken by firms in response to APP fraud. Which?

has helped some of these victims to overturn an original decision by their bank not to reimburse them, through the support offered by the Which? Money Helpline and by cases pursued by our investigative journalists. In other instances, we've suggested that individuals take their complaints to the Financial Ombudsman Service, and they are yet to find out if they will be reimbursed.

If the CRM Code was being implemented appropriately, Which? would not have to intervene as often as we have in the past year. We also recognise that the cases we have seen represent a fraction of those that have been perpetrated, and we almost only hear from people who have yet to receive their money back. Many other victims will understandably struggle to challenge decisions by themselves or to take a complaint to the Financial Ombudsman Service at what can be a hugely distressing time. So it is crucially important that firms seek to provide fair outcomes in their initial decisions.

We hope that this report will help inform the Lending Standards Board's one-year review of the CRM Code. We outline the key issues affecting victims:

- An over-reliance on victims having ignored warnings
- Unreasonable expectations of how victims should have verified who they were paying
- A failure to properly assess vulnerability
- Poor communications with victims

Urgent action is needed to ensure firms adhere to the Code. We call on all firms that have signed up to the CRM Code to:

- 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
- Provide victims with specific reasons to explain reimbursement decisions

We also call on the Payment Systems Regulator to evaluate the effectiveness of the voluntary industry code that it proposed.

Which? believes that the evidence over the past year shows that the CRM Code should be made mandatory. Regulatory oversight of how firms treat victims with regards to reimbursement is much more likely to lead to fairer and more consistent outcomes than we have seen under a voluntary approach. It can also force all payment providers to reimburse victims, where appropriate. UK Finance and the Treasury Select Committee have both also called for the Code to be made mandatory.

The Payment Systems Regulator should have the powers and the appetite to act to make reimbursement mandatory. We want the government to clarify whether this is the case, and if necessary direct the action it expects the regulator to take.

Which? remains committed to working with consumers, policymakers, industry and other consumer groups to continue to prevent APP fraud and to establish a stronger and more consistent system of redress for victims.

**Anabel Hoult**
Chief Executive
Which?

# Background

In 2016, Which? submitted a super-complaint to the Payment Systems Regulator calling on them to investigate:

- the extent to which banks could reduce consumer harm from authorised push payment (APP) fraud; and
- 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.

The Payment Systems Regulator proposed a voluntary contingent reimbursement model, where reimbursement depends on whether the payment service providers involved have met required standards, and whether the victim has taken a requisite level of care. In February 2018, the Payment Systems Regulator established a steering group to lead the development of an industry code for the reimbursement of victims. The Contingent Reimbursement Model (CRM) Code came into effect on 28 May 2019.[1] On 1 July 2019, the Lending Standards Board became the governing body for the Code.

The CRM Code sets out a set of standards that sending and receiving payment providers should follow to mitigate the risk of authorised push payment (APP) fraud. The Code is based on the principle that the starting point should be to assume that victims of APP fraud should be reimbursed in full. Firms have to show that a victim has failed to meet their requisite level of care when making the payment if they are to reject reimbursement. All victims considered vulnerable to the particular APP fraud should be reimbursed regardless of how they acted when they made payment.

Eight banking groups and one building society signed up to the CRM Code at the beginning: Barclays, HSBC Group (includes First Direct and M&S Bank), Lloyds Banking Group (includes Bank of Scotland and Halifax), Metro Bank, Nationwide, NatWest Group (includes Royal Bank of Scotland), Santander and Starling Bank. The Co-operative Bank is the only firm to sign up to the Code since its launch.

1 Lending Standards Board (2019), *Contingent Reimbursement Model Code for Authorised Push Payment Scams*

# The evidence to date

The CRM Code sets out two clear aims:

- to reduce the occurrence of APP fraud; and
- to reduce the impact of these crimes.

The first of these aims is a long-term challenge, with the CRM Code just one part of the fight against fraud. A wide range of factors outside the control of firms can also drive the level of fraud. The significant increase in the number of cases and the amount of money lost to APP fraud over recent years is nonetheless highly concerning. There were 114,731 cases involving customers with personal bank accounts in 2019, up from 38,596 in 2017. Fraudsters stole £317 million in 2019 compared to £108 million in 2017.[2] It also underlines the need to achieve the second aim, to reduce the impact of these crimes via fairer decisions on the reimbursement of victims.

The second aim can be measured more directly. In the last full year before the Code launched, just 19% of the amount lost by individuals was returned to them. In the first six months of the Code's launch, signatory firms reimbursed 41%. This is clearly a significant increase. Rates of reimbursement were also much higher for some types of scam. Signatory firms reimbursed 53% of the amount lost to impersonation fraud, whereby the criminal contacts the victim purporting to be from either the police or the victim's bank and convinces the victim to make a payment to an account they control.[3]

It is encouraging to see a higher share of victims being reimbursed as a result of some banks and building societies applying the Code. However, the Payment Systems Regulator has stated that rates of reimbursement are 'well below' what they expected 'given the Code presumes that customers should be reimbursed unless there are clear grounds for holding them liable'.[4] Similar issues were raised as part of the Lending Standards Board's recent evaluation of the way that firms have approached parts of the consumer requisite level of care. The Lending Standards Board concluded that:

*'Judgements about reimbursement were not always made in the light of the full circumstances of the case or a judgement of what consumers may have believed at the time, but were often driven by narrower process considerations. 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.'*[5]

The Financial Ombudsman Service has since stated that its findings 'broadly mirror' those of the Lending Standards Board. The Financial Ombudsman Service concluded that 'the presumption in

2 Note that UK Finance states that the 2017 data are not directly comparable to later years because four additional UK Finance members began reporting APP data as of January 2018, and new reporting standards were adopted in January 2018. UK Finance (2019), *Fraud the facts 2019: The definitive overview of payment industry fraud*, p.42; UK Finance (2020), *Fraud – The facts 2020: The definitive overview of payment industry fraud*, p.46

3 UK Finance (2020), *Fraud – The facts 2020: The definitive overview of payment industry fraud*, pp.46 & 60

4 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.5

5 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

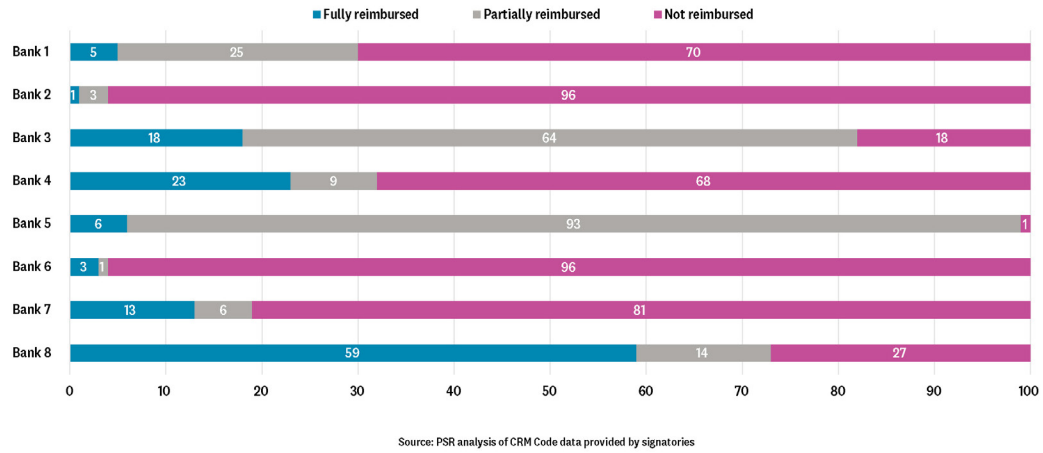
favour of reimbursement is in practice, in many of the cases we have seen, effectively reversed'.[6] It has yet to publish case studies from since the CRM Code launched, but from its pre-Code cases it has highlighted that firms should have taken into account relevant rules, codes and best practice standards that would have meant they 'shouldn't have taken their customers' authorisation instruction at 'face value' – or should have looked at the wider circumstances surrounding the transaction before making the payment'.[7]

The Payment Systems Regulator also recently published anonymised data for individual firms relating to reimbursement rates. As the following charts show, this exposed 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; whereas 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.[8]

The sheer scale of the differences between the approaches taken by each firm, as seen in the Payment Systems Regulator's findings, suggests this is highly unlikely to be explained just by differences in the types of cases that firms deal with or their customer bases. The findings clearly show that some firms are taking a much more supportive approach to the reimbursement of their customers. While firms are likely to be continually evolving how they approach the implementation of the Code and how they make judgements on specific provisions in the Code, there is enough evidence to date from the Payment Systems Regulator, Financial Ombudsman Service and the Lending Standards Board to suggest there are major inconsistencies and poor outcomes for many victims.

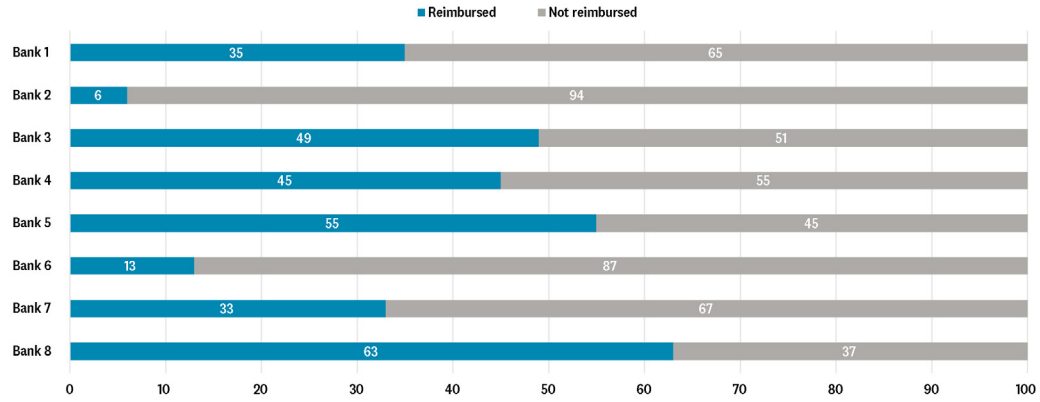
**Figure 1: % of total APP fraud cases, May 2019 – February 2020**




Source: PSR analysis of CRM Code data provided by signatories

6 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.17
7 https://www.financial-ombudsman.org.uk/businesses/complaints-deal/fraud-scams
8 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, pp.23–24

**Figure 2: % of total APP fraud value, May 2019 – February 2020**




Source: PSR analysis of CRM Code data provided by signatories

The inconsistencies in how the industry is dealing with victims are even starker when firms that haven't signed up to the CRM Code are included. Across all the firms that UK Finance collects data for, just 26% of the amount lost by victims of APP fraud was reimbursed to them in 2019.[9] But there are actually more than 400 firms that offer Faster Payments in the UK,[10] and there is no reliable data to show how all of them deal with victims.

9 UK Finance (2020), Fraud – The facts 2020: The definitive overview of payment industry fraud, p.46
10 https://www.fasterpayments.org.uk/about-us

# The key issues affecting victims

Behind the data are individuals whose lives have been upended by APP fraud. It is vitally important that we understand their perspectives and experiences, both of the crime and of trying to seek redress. While the emotional impact of being a victim of an APP fraud will be difficult to overcome, some of the victims in the following stories had their finances restored by their bank or building society. In doing so, they averted much greater financial turmoil and emotional distress.

### About the case studies

The case studies in this document provide just a snapshot of victim experiences, and do not cover all types of APP fraud or even all signatories to the CRM Code. Nonetheless, they help highlight key issues that Which? has seen more widely among victims who have contacted us.

The names shown are not those of the real victims. In each of the cases, Which? intervened. In examples where individuals were reimbursed at the first decision, our role was often simply to raise the urgency and sophistication of the case with each customer's bank or building society. We don't know whether we impacted the final result, but we've assumed that a firm's decision to fully reimburse their customer would have been the same had we not intervened. In those cases where victims were rejected for a full reimbursement by their bank or building society, we helped the person to understand the decision by asking for further details. We also helped victims to challenge these decisions, through the support offered by the Which? Money Helpline and by cases pursued by our investigative journalists.

Some of the victims were subsequently reimbursed in full, after their bank or building society reassessed their case. While this is ultimately a good outcome, each firm's initial decision highlights inconsistencies with how firms are approaching cases and questions the fairness of the initial outcomes for customers. In some other cases, the firms involved have maintained their original decisions not to fully reimburse. Which? has suggested these victims take their complaints to the Financial Ombudsman Service, however they face a nervous wait that could stretch for months or even years due to a significant backlog of Financial Ombudsman Service cases.

Having reviewed the cases of around 150 people who have contacted Which? over the first year of the CRM Code, we have identified four key issues with how the Code is being implemented.

## 1. An over-reliance on victims having ignored warnings

Firms are able to reject reimbursement if the customer 'ignored Effective Warnings'. 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'.

In many of the cases in this report, 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, such as Thiti (below) and Ava (page 10), were coached by the fraudster to respond in particular ways and ultimately to ignore the guidance offered in any warning. Thiti, for example, was convinced by a fraudster over a period of 24 hours, after they were able to show him that a payment had been made into his account. Ava was on the phone to a fraudster when she saw the warning, and was led to believe that the 'safe' account transfers that her bank was warning her about were not relevant.

In such situations individuals are more likely to go ahead with the payment because they have already committed to it. More generally, people tend to think that they're unlikely to be victims of fraud and therefore can discount warnings as irrelevant.

In assessing cases, Which? has seen that many firms did not sufficiently consider the circumstances of the scam and how the warning was perceived by their customers. They 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 sufficient reason to reject a reimbursement claim.

The Lending Standards Board's review found similar issues. They did not see many instances where a customer appreciated the detail of a warning or were able to relay what the warning said. Even when a customer had considered the alert, the Lending Standards Board found certain types of fraud meant the customer was engineered into ignoring it, or the customer still had reasonable grounds for believing the payment to be genuine. In terms of reimbursement decisions, the Lending Standards Board found that the issuing of a warning was sometimes treated as a strict liability regardless of how effective the warning was or whether the customer had a reasonable ground for not acting on the warning.[11]

### Thiti: remains without £15,000 after fraudsters posed as BT

Thiti was contacted by someone claiming to be from BT who told him his internet line had been hacked. Over a period of 24 hours, the scammers gained access to his computer and mobile phone using remote access software. They were able to access his online banking accounts. On Thiti's screen he could see that a £15,000 payment had been made by so-called 'fraudsters' into his Nationwide account. The real fraudsters then convinced him that he needed to go into his bank branch to transfer £15,000 to 'flush out the hackers'.

After realising he'd been the victim of fraud, Thiti reported this to Nationwide, who managed to recover just under £5,000 from the recipient's account. The rest, however,

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*, pp.2 & 9

had been already transferred. Nationwide reviewed Thiti's case and chose not to reimburse him, so Thiti contacted Which?.

Nationwide told us that all customers making a payment in a branch are read a scripted warning. Thiti does not recall this. In response to Thiti's subsequent complaint, Nationwide stated that its branch advisor 'specifically remembers reading the warning script'. It also said the branch manager had 'witnessed the advisor reading the statement on other occasions' and was therefore 'confident it would have been read'.

The warning that Nationwide indicated would have most likely been provided included a series of questions followed by a tailored warning. Prior to this, customers are told: 'Please ensure you're honest and take the time to consider which option best fits so I can ensure we offer you the best protection against the relevant fraud. If someone has told you to lie to us about the reason for the payment it will be a scam. Please tell us the truth so we can safeguard your money.'

In response to Which? asking Nationwide whether they deemed the warning given in branch to be an 'Effective Warning', as set out in the CRM Code, Nationwide responded by saying it did because if Thiti 'followed the advice in the warning, the loss would have been prevented. An effective warning is one where we identified an APP scam risk when setting up a new payee. (He) chose not to act on the warning'. Nationwide added that despite receiving a warning, Thiti 'said he wanted to carry on with payment and was untruthful about the reasons'.

Thiti took his case to the Financial Ombudsman Service. He is still waiting for an outcome to his case, almost a year on from when he became a victim.

### Ava: remains without £33,000 having responded to a text that appeared to be from her bank

Ava received a text message about a 'suspicious payment to Airbnb'. It appeared to come from Lloyds Bank's usual phone number, sandwiched between two genuine messages, so she called the number supplied. Over the course of an hour, Ava was persuaded to transfer her money into a new account, in the belief that her original one had been hijacked by criminals.

Lloyds Bank sent a letter informing Ava that she would not be reimbursed on the grounds that she 'did not take sufficient steps to verify that either the text message or the person she spoke to on the phone were genuine', and that she authorised the payments despite receiving 'clear warnings' stating that Lloyds Bank would never ask a customer to move money to a 'safe' account.

Ava had no reason to believe the text was fake, and Lloyds Bank is yet to explain the 'sufficient steps' she ought to have taken. And, while she did notice an online warning about fraud when she made the first payment, the criminal on the phone was able to quickly dismiss her concerns. 'It was very urgent and compelling,' she recalls. 'My two-year-old daughter was running around while I was on the phone to them for an hour. I saw the warning about Lloyds Bank never asking me to move money into a safe account and flagged this over the phone. I was assured that these were not 'safe' accounts but 'new' accounts.'

A Lloyds Bank letter in response to Ava's subsequent complaint begins by saying that it will explain how the original decision not to reimburse was reached. However, even though

it acknowledges that the case is covered by the CRM Code, it does not provide any basis for the decision not to reimburse under the Code. It instead only talks about funds that have been recovered from the receiving banks, which could suggest to the customer that it's only recovered funds that can be passed to a victim.

Ava subsequently took her complaint to the Financial Ombudsman Service in December 2019. At the time of publication, she had not yet received a decision.

## 2. 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 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.' This 'reasonable basis' test is perhaps the most controversial part of the consumer requisite level of care.

The CRM Code does not state that customers are required by this provision 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 for believing' even without taking extra steps, and they may be rushed into making the payment.

However, in some of the examples in this report and others that Which? has intervened in, we have seen firms assume that customers should have taken steps in order to be reimbursed. In the case of Jakub (page 15), Lloyds Bank originally told us that he had not been reimbursed as he 'didn't conduct sufficient checks before making the payment'. They suggested he should have called the organisation that the cold caller claimed to be from, using a number, for example, found on their website. But Jakub was, in part, convinced by the caller quoting the full details of his bank card, as well as his full name and address, so he didn't think to hang up and call back on another number. Worryingly, Lloyds also explicitly told us that the CRM Code requires customers to take steps to confirm any payee is genuine. While Kayleigh (page 13) did take a number of steps before making a large investment, and was reimbursed at her bank's first decision, this is a high level of due diligence that is unlikely to be commonplace for most bank transfers.

These issues are partly due to firms not sufficiently taking into account the circumstances of the payment and the sophistication of the scam, as the Code requires. In some of our examples, the fraudster contacted the victim using the same email, phone or SMS details as a legitimate organisation, including their bank. Ava (page 10), for instance, received a text message from what appeared to be her bank's usual phone number, sandwiched between two genuine messages. Reggie (page 14) received an email that appeared to be sent from his builder, which was for a specific payment he expected to pay and followed the usual pattern – an initial email then a follow-up a few days later. Abdul (page 16) asked for proof the call was genuine, before the fraudster then called him back on a number with Halifax's name and number. Abdul even called the bank's official number and reached Halifax's main menu, taking this as a sign that the original caller was genuine. Unfortunately, he hung up without speaking to an advisor and the fraudster called him back.

In other examples, the fraudster was able to convince individuals to download software that then enabled them to access the victim's device remotely. Thiti (page 9) and Reshma (page 18) were both unaware that this had happened. In these cases, the fraudster was able to make it appear as though suspicious activity had taken place or to make it look like the victim had been refunded. Only someone from their bank would ordinarily be able to see their account activity, so this also helped to establish the fraudster's credibility.

In its work to date, the Lending Standards Board has found that firms' assessments were often conducted on the basis of finding blame at some point in the payment journey, rather than

reviewing the circumstances of the case to understand the rationale for customers making the payment. This was in part because some firms were using a scorecard or system-driven process to help determine liability, which the Lending Standards Board found often resulted in an outcome which was not in the customer's favour. The Lending Standards Board found that some firms did not document their decisions to reject reimbursement at all. They also discovered that where customers offered evidence of the fraud operation and the checks they had completed, this evidence often was not taken.[12]

The Financial Ombudsman Service has similarly concluded that 'some firms are inappropriately declining reimbursement' on the basis that the consumer did not have a reasonable basis for believing the transaction or recipient was genuine. In those cases, the Financial Ombudsman Service has found examples of firms making decisions based on assertion, rather than on the evidence. It has also found some firms not taking into account or recognising the full circumstances of the scam, such as social engineering. Firms have also expected customers to make additional checks before making the payment than might ordinarily be reasonable for consumers generally, or in the particular circumstances of the transaction. The Financial Ombudsman Service also cited examples where firms then go on to offer 50% reimbursement for this reason when 100% reimbursement would be appropriate, which it argues may deter consumers from pursuing what may be valid complaints.[13]

### Kayleigh: reimbursed £160,000 after falling victim to an elaborate investment scam

Kayleigh was searching for investment opportunities on Google. She clicked on an advert and entered some contact information. Shortly after, she received a call from someone claiming to be an investment manager at Aviva. Through a series of calls and emails containing convincing-looking Aviva logos and footers, she was offered the chance to invest £160,000 in three-year bonds with a modest and realistic 2.5% guaranteed return.

Kayleigh took steps to ensure it was genuine. She checked the Financial Conduct Authority register for Aviva and found no impersonation warnings (though one appeared just days later). The fraudster had assumed the name of a real Aviva employee, who Kayleigh looked up on LinkedIn and Aviva's official website. She transferred the full sum in two £80k instalments (one in her own name and one for her husband) from her Santander current account to achieve Financial Services Compensation Scheme protection. The fraudster supplied fake Aviva-branded bond certificates in response.

All seemed well until Kayleigh's brother spotted a Financial Conduct Authority warning about Aviva impersonators and alerted her. She contacted Santander immediately, which began to investigate. She also turned to Which? for support. Kayleigh was distraught at what had happened. Her mother was also very ill at the time. These two events led her to see a counsellor to help her cope.

After Which? emphasised Kayleigh's due diligence efforts to Santander, it decided she was not to blame and reimbursed her in full. Kayleigh described the decision as a 'huge relief' at a 'terrible time in my life'.

12 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*, pp.3 & 10–11

13 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.16

### Reggie: initially offered only partial reimbursement after fraudsters posed as builders and asked for £4,000

Reggie was using the services of a builder who had worked for him a number of times before. On each previous occasion, he had received an initial email from the builder with an invoice. Reggie then usually received a follow-up email a few days later reminding him to make the payment within seven days of the date shown on the invoice.

As expected, Reggie received the email requesting payment for the builder's most recent work. It set out that he needed to pay around £4,000, as he had anticipated. It also specified the bank account that this needed to be paid into, which was different to the account that Reggie had previously paid. He didn't transfer this immediately, as per usual. A few days later, another email arrived requesting payment within seven days of the date of the invoice. Again, this was the norm.

Later, however, when Reggie was on the phone to the builder, he mentioned that he'd made the payment as requested. The builder announced no money had been received, so he went into a state of panic. Reggie phoned the police, who told him to log the case with Action Fraud – which he did later on. But first he went in person to a local Nationwide branch to report the incident. It was later discovered that the builder's email account had been hacked and Reggie had, in fact, been receiving fraudulent emails.

While awaiting a decision on reimbursement, Reggie contacted Which? for help with his case. Nationwide later wrote to him, confirming that he had been a victim of APP fraud. The letter stated that 'we have checked the control measures we have in place on our payment platforms and have concluded that we could have done more to protect and/or advise you of the risks associated with the payment, but also you could have carried out sufficient checks to confirm the validity of the beneficiary'. However, no details are given as to what checks Reggie could have conducted, or the specific circumstances of the fraud referenced. The letter also said Reggie would only be partially reimbursed due to his 'shared liability' and that only half the amount, around £2,000, would be credited to his account.

Nationwide told Which? that Reggie should have carried out more checks to confirm the validity of the recipient, even though by its own admission it had failed to provide adequate warnings. If 'bill or invoice' had been selected as the payment type, Nationwide said its warning would have been relevant to that particular type of fraud and therefore more effective.

Reggie was initially accepting of this decision and felt pragmatic about it, thinking that he was lucky to get half back. However, he then contacted Which? again and we provided further details of the CRM Code and a template letter to challenge Nationwide's decision. Reggie was confused by Nationwide's decision, given that they implied he was partly to blame. He fully believed that at the time he was making payment to the correct beneficiary, and had no reason to be suspicious due to the nature of the emails he had received.

Nationwide's complaints department subsequently reviewed the building society's original decision of shared blame. It concluded that Reggie should be fully reimbursed as he was not to blame. Nationwide subsequently told Which? that 'on review of this case we became aware that the member was able to amend the existing payee details and as such, didn't receive the tailored warning required under the CRM, so we took the decision to refund our member in full.'

### Jakub: eventually reimbursed £30,000 after fraudsters posed as BT staff and National Crime Agency investigators

Jakub faced a two-pronged attack involving fraudsters claiming to be from both BT and the National Crime Agency. The first caller told Jakub that he'd won a loyalty bonus worth £35 off his next BT bill and quoted the full details of his bank card, as well as his full name and address, to confirm his eligibility. Although Jakub shared no sensitive data over the phone, this laid the groundwork for the second stage of the scam.

A few days later he received another call, this time from the 'National Crime Agency' warning him that £400 had been taken from his Lloyds Bank current account due to a series of fraud involving BT and complicit banks. The caller explained that the authorities knew he had been targeted by a caller pretending to be from BT. They then asked him to help with their investigation into his local Lloyds Bank branch, by moving his money to a 'safe' account. Jakub agreed and, as instructed, went to the local library to print off an email that appeared to confirm the opening of this safe account – with Clydesdale Bank – in his name. However, this account was not as it seemed and was actually controlled by the criminals.

Jakub then visited his nearest branch to transfer £30,000 from his account, telling them that he wanted to move the money so that his savings weren't all in one place, as he was coached to say. Lloyds Bank says staff followed the correct procedures, as per the Banking Protocol – a rapid response scheme through which branch staff can alert police and Trading Standards to suspected frauds. Nothing gave the bank cause for concern. However, Jakub says no concerns were raised or questions asked. It was only the following day when he attempted to move more money from his account that staff blocked the payment and became concerned about potential fraud. They asked him to sit down with them and the fraud quickly came to light.

Having banked with Lloyds for decades, Jakub was shocked to hear that he wouldn't get his savings back because he 'didn't take steps to verify the identity of the cold caller'. He says he was subject to unsympathetic and protracted questioning, making him feel 'like an idiot'.

A close family friend encouraged Jakub to escalate his complaint to the Financial Ombudsman Service, write to the Financial Conduct Authority and approach Which? to raise his concerns about the way Lloyds Bank handled this case.

Lloyds Bank said that Jakub 'didn't conduct sufficient checks before making the payment'. When we asked what this means in practice, Lloyds told us that the CRM Code requires customers to take steps to confirm any payee is genuine: 'An example of this would be to contact the company/organisation that the cold caller claimed to be from on a genuine number, for example, on their website before transferring money.' Lloyds Bank also told Which? that when Jakub reported the fraud, he said he 'should have contacted the genuine company before making a payment and had recognised attempted scam calls in the past'.

Lloyds Bank has since decided to reimburse the full amount. A spokesperson said: 'Before being contacted by Which?, we had already reviewed this case and refunded the full amount he lost after having taken everything into consideration about his circumstances. We have apologised for the service he experienced during what was already a very distressing time and have paid compensation in recognition of this and the delay in our investigation.'

## 3. 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. 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.'

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. Maya (page 17), for example, was initially rejected for reimbursement by Santander. It was only when Which? intervened that Santander considered fully that she had been undergoing extensive medical treatment when she became a victim.

In some cases, what victims have said when reporting the fraud, about what they might have done to prevent the fraud, has then been used against them. In Jakub's case (page 15), Lloyds Bank told Which? that when Jakub reported the fraud, he said he 'should have contacted the genuine company before making a payment and had recognised attempted scam calls in the past'. Having just realised he had been defrauded out of a life-changing amount of money by criminals who he'd been speaking with for over four days, it's understandable that Jakub may have reflected on what more he could have done to prevent this from happening. But firms should not be trying to catch out victims. Not only is this unfair and not in the spirit of the CRM Code, it could put victims off from sharing the full facts of their case, which could undermine attempts to catch the criminals.

As part of its review of how signatories to the CRM Code have assessed whether their customers had a reasonable basis for believing the payment was legitimate, the Lending Standards Board has also concluded that firms have not put in place well-developed mechanisms for identifying vulnerability and customers' susceptibility to APP fraud. Questioning of customers who reported falling victim to an APP fraud was often closed and did not allow for the clear identification of any vulnerability. In some cases, evidence of vulnerability was available, but was not always used as a consideration for reimbursement.[14]

### Abdul: fully reimbursed £102,000 after fraudsters spoofed his bank's phone number

Halifax customer Abdul was left distraught after criminals, who posed as the bank's fraud team, tricked him into sending them money. But Halifax refunded the money after Which? explained that social isolation during the coronavirus pandemic had left him unusually vulnerable to fraud.

Abdul said, 'I work in finance and consider myself to be on the ball. I just can't believe this has happened to me.' Panicked and tired, Abdul's ordeal started when a caller on his landline claimed his bank account had been breached. All his money needed to be moved to safe new accounts, he was told. Suspicious, Abdul asked for proof the call was genuine. The fraudster then called him back on his mobile, using a trick known as 'spoofing' to

14 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.3

display Halifax's name and number. Abdul called the bank's official number and reached Halifax's main menu, taking this as a sign that the original caller was genuine.

Unfortunately, he hung up without speaking to an advisor and the fraudster called him back. During a lengthy conversation Abdul was tricked into approving bank transfers and revealing account details. By now, he said: 'My state of mind was panicked, tired and I couldn't think straight.'

It was only the following day that he discovered the fraud, after the fraudster's £20,000 loan application in Abdul's name triggered a fraud alert on the bank's system. Abdul was stunned to learn that his entire £100,000 retirement savings had been transferred out of the bank. The criminals also took £2,000 from his overdraft.

After Halifax began investigating the case, Abdul contacted Which? and it became clear to us that the coronavirus pandemic had played a major role in the fraudster's success. With underlying health conditions, Abdul, who lives alone, had already been isolating at home for two months. An expected new job had fallen through and a friend had been battling cancer. 'It was her birthday that same week, but she was suffering so badly with the effects of chemo... I can't stop thinking about her.'

As Abdul explained: 'If we weren't in this lockdown situation, I may have acted differently and maybe my state of mind would have been more alert.' Halifax subsequently reimbursed Abdul in full and in line with the CRM Code, cancelling the fraudulent loan and correcting his credit report. A spokesperson told us the bank has 'a great deal of sympathy' for Abdul and branded the fraud 'sophisticated'. Halifax added: 'It's important for people to remember that their bank will never contact them out of the blue and ask them to share their account details, log on to their internet banking or transfer money to another account.'

### Maya: eventually reimbursed having lost £20,000 while undergoing extensive medical treatment

Maya received a call from someone supposedly from Santander's fraud department. She was told that her bank account was at risk from fraudsters and that she needed to move her money to safeguard it. As a result, she transferred £20,000 from her current account. It was almost a week later when she realised that there was an issue, and got in contact with Santander.

Santander later told her that she wouldn't get her money back because she went ahead with the online bank transfer despite ticking a box confirming that she had read the fraud message and was comfortable to continue with the payment.

Maya then got in touch with Which? for help with her case. Santander told us that Maya had been provided with a series of warnings which included information about moving money to a safe account and that Santander will never ask customers to transfer money. Santander also told us that part of the reason Maya had not been reimbursed was that around two weeks after the scam took place, she had been called by a Santander fraud investigator and had indicated to them that she was unsure whether the fraudster identified which bank they were calling from.

Only after we asked the bank to review the case, in light of the fact that Maya was undergoing extensive medical treatment at the time, did it agree to refund the full amount.

Santander told Which? that after reviewing Maya's case, 'in light of the new information that was shared about her medical condition, we have refunded her the full amount that was taken from her account.'

### Reshma: initially refused reimbursement for £7,000 after a five-hour hoax phone call

Reshma was called by someone claiming to be from the fraud department of her bank, NatWest. The caller alerted her to fraudulent activity on her account, and during a conversation lasting almost five hours, she was convinced to help with a fraud investigation and told not to mention it to anyone, in case this alerted the fraudsters.

To help catch the 'fraudsters', the caller asked Reshma to use her card and card reader to make a payment. The payment failed so the caller convinced her to ring NatWest and unblock her card. The caller then persuaded her to install an app on her computer to allow the caller remote access to her device. Reshma was convinced to set up a bank transfer of £70, assured that this would be returned and that she was only helping to catch the thief.

Reshma was then asked to go to her local branch and transfer £7,000. To avoid alerting the alleged thief, she was told to pretend the money was for a friend to help her buy a car. The caller even got her to practise how she would respond to the questions that bank staff would ask before processing the payment.

Reshma's suspicions were raised the following morning, when she reflected on what she'd been asked to do. She called the NatWest fraud team to explain what had happened and was told she was the victim of an elaborate fraud.

Later that day, Reshma received yet another call from the person she now believed to be a fraudster, who was trying to convince her to transfer even more money. She refused and challenged them, so the fraudster put £7,000 back into her current account, making it look like she'd be refunded by the bank as promised. The money had, however, simply been transferred from Reshma's ISA account.

NatWest later told Reshma no funds remained with the beneficiary bank and that the bank accepted no liability, so Reshma contacted Which? for help. We raised the case directly with NatWest and asked a series of questions about its decision not to reimburse her. Reshma was later told that NatWest had reviewed her case and would reimburse her in full.

NatWest confirmed that Reshma was reimbursed under a no-blame scenario. They also said: 'If a customer receives an unexpected call purporting to be from their bank, asking them to provide remote access to their phone or PC, or to move their money to a safe account, they should decline this and report it to their bank immediately on a phone number they can trust – this can be found on the back of their bank card or from our website. If the person is using a landline, we would also recommend that they call back from a different device.'

## 4. Poor communications with victims

In the stories in this report, there are examples where firms have not provided the customer with the reasoning for their decision not to reimburse. This could make it more difficult for the victim to challenge the decision or put them off altogether. For example, Ava (page 10) was told by Lloyds Bank that she 'did not take sufficient steps to verify that either the text message or the person she spoke to on the phone were genuine', but the bank did not explain what these steps might have been. A subsequent Lloyds Bank letter begins by saying that it will explain how the original decision not to reimburse was reached, but it actually provides no reasoning.

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'. The point on responsibility is unclear and not in any way related to the CRM Code. These letters also do not provide any specific suggestions as to the types of checks that the victims could have conducted.

Perhaps the worst examples we have seen, however, state that the victim will not be reimbursed simply because they authorised the payment. 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 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.'

Which? has also seen numerous examples of firms sending letters to their customers regarding a decision not to fully reimburse them 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 CRM Code or that the firm has assessed their customer's actions and the firm's actions against the requirements of the Code. Some only mention funds that have been recovered from the receiving bank, which could suggest to the customer that it is only recovered funds that can be passed to a victim. One victim who had lost more than £1,000 who was told by his bank that they were 'happy to inform you that we have been able to recover £0.61 in relation to your case'.

The Financial Ombudsman Service similarly concluded that some firms are not providing a clear rationale for their decision to not reimburse under the CRM Code, with some firms not even mentioning the Code.[15] The Lending Standards Board also found that customers were often not informed of how a decision had been taken to deny reimbursement and customers were often given no opportunity to address the grounds on which the firm was holding them liable for the success of the fraud.[16]

15 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.16

16 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.3

# The urgent action needed to ensure firms adhere to the CRM Code

Based on the cases that Which? has reviewed and the findings of the Lending Standards Board, the Financial Ombudsman Service and the Payment Systems Regulator, we have concluded that firms are not consistently adhering to the main principle of the Code that a victim should be reimbursed unless they can be shown to have failed to meet their requisite level of care. This fundamentally undermines the protection offered to consumers.

Below we set out the urgent action that signatories to the CRM Code should take.

## Test warnings to see if they are 'effective'

When a customer has been presented with a warning and gone on to become a victim of fraud, clearly the warning has not prevented the fraud from succeeding. What matters is whether firms can provide evidence that their warnings meet the criteria set out in the Code, including reducing the likelihood of an APP fraud succeeding. Which? has not seen any such evidence from firms. 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'.[17]

In the long term, even warnings that have been shown to meet the requirements in the Code might elicit little or no response, particularly if firms don't modify the text, placement and design. This is because individuals tend to ignore something that has no new information to impart. So banks and building societies need to continually test and evaluate their warnings. They should also consider how fraudsters can undermine warnings by coaching victims to ignore them or to respond in particular ways.

**Recommendation 1: Firms should evidence that their warnings are continually meeting the Code's requirements for different groups of their customers, if they are to rely on using a customer's response to warnings to reject reimbursement.**

***How might firms test and evaluate their warnings?***

Firms could do some or all of the following:

- Gather consumer feedback on warnings during or immediately after bank transfers. Feedback should be gathered on consumer attention, comprehension, beliefs, motivation and behaviour to identify reasons why warnings might be effective or ineffective.[18]
- Use randomised control trials to assess whether changes to the design and wording of warnings makes them more effective at affecting behaviour.

17 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, p.16

18 Following Wogalter's C-HIP model for warning effectiveness. See Wolgater et al (2002), 'Research-based guidelines for warning design and evaluation', *Applied Ergonomics (33)*, pp.219–230

- Examine reported fraud data over time both before and after the introduction of the warnings to identify any statistical breaks in the reported incidence of fraud among users.
- Explore online or lab-based experiments where more granular feedback can be obtained from consumers undertaking bank transfer tasks. These techniques have been used frequently by academics studying the effectiveness of warnings against phishing fraud.[19]

## Base their judgements of what is reasonable on evidence of actual customer behaviour

For firms to properly assess whether victims had a reasonable basis for believing that the payment was legitimate, they need to make judgements about what is reasonable behaviour. This has to be based on actual evidence, rather than merely on the opinions of bank staff. Firms also need to consider the full circumstances of each case. This would suggest that relying on a scorecard approach, which the Lending Standards Board found evidence of, is unlikely to be sufficient to meet the requirements of the CRM Code.

Which? would like to particularly urge firms to consider the impact of fraud enablers, such as fraudsters using the same email, phone or SMS details as a legitimate organisation or convincing victims to download remote access software. These enablers can fundamentally alter the circumstances under which victims are making judgements about who they are transferring money to. In most circumstances, Which? believes that firms should not refuse reimbursement in cases where fraudsters have impersonated a legitimate organisation by:

- contacting the victim using the same email, phone or SMS details as a legitimate organisation, including their bank; and/or
- citing confidential information only held by a legitimate organisation, even if this was enabled by the victim providing access to remote access software.

**Recommendation 2: Firms should base their expectations of their customers on evidence of actual behaviour among similar consumers in similar circumstances.**

## Train all relevant staff in how to identify customers who could be or may have been vulnerable to APP fraud

Which? was particularly concerned by the findings of the Lending Standards Board which highlighted that some firms have been using scorecards for assessing claims. While we acknowledge the challenges that firms have faced in implementing the Code, it's difficult to see how such an approach could meet the Code's requirements. In particular, when assessing vulnerability the Code requires firms to consider the circumstances of each case, to assess whether it was reasonable to expect the customer to have protected themselves from the particular APP fraud and to consider the impact that the fraud had on them. The Lending Standards Board also found that it was not always clear that all staff who are impacted by the Code had received training.[20] This lack of training is likely to disproportionately affect customers who could be vulnerable to becoming victim to an APP fraud as they are likely to need greater support to help them recover, and to receive a fair handling of their case.

19 See for instance Egelman et al (2008), 'You've been warned: an empirical study of the effectiveness of web browser phishing warnings', *Association for Computing Machinery*, pp.1065–1074

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*, p.8

**Recommendation 3: Firms should ensure that all of their relevant staff members have been trained in how best to identify and support customers who could be vulnerable to APP fraud or may have been a victim of an APP fraud.**

## Provide victims with specific reasons to explain reimbursement decisions

If individuals are going to be able to understand their bank or building society's decision on reimbursement, they need to be clearly told that they have been a victim of an APP fraud, and that this is covered by the CRM Code which involves their bank or building society making a decision on whether they have met the consumer requisite level of care when making the payment. If the firm chooses not to fully reimburse the victim, then they should clearly state which part of the requisite level of care they have decided the victim has not met, and state their reasoning. Firms should also make clear that the victim can challenge the decision and make a complaint, and that this complaint can subsequently be taken to the Financial Ombudsman Service.

**Recommendation 4: Firms should set out in their communications with victims the part of the CRM Code that they are relying on if they have taken an initial decision not to fully reimburse, and explain their reasoning.**

# Establishing a stronger and more consistent system of redress

While the Lending Standards Board can work with firms to help address the issues that we have identified with how the CRM Code is being implemented, the evidence and experiences of consumers over the past year suggest that a voluntary approach to protecting consumers from the significant harm caused by APP fraud is unlikely to be sufficient.

The Payment Systems Regulator should evaluate the effectiveness of its approach through a voluntary industry code compared to the legislative, regulatory and scheme-wide protections provided for card payments. The Payment Systems Regulator should also consider what wider reforms are required to help prevent APP fraud and improve how firms make decisions on reimbursement.

To build on the progress made so far, Which? has identified three key reforms that would establish a stronger and more consistent system of redress, which can be enforced by a regulator and cover all payment providers.

## Industry-wide standards for reimbursement

While some firms required more time to implement the requirements of the CRM Code in time for its launch in May 2019, the pace at which new signatories have signed up to the Code has been disappointing. Major firms such as Clydesdale and Yorkshire Bank, Monzo and Tesco Bank are yet to sign up.

Which? believes that the CRM Code should be made mandatory to establish a set of minimum industry standards. This is a view shared by UK Finance[21] and the Treasury Select Committee.[22] As well as ensuring that all payment providers offer these protections, it would also help enable the requirements to be enforced effectively.

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.[23]

When the Payment Systems Regulator recently concluded that rates of reimbursement are lower than expected, it set out three possible paths forward: working within the current voluntary scheme; changing the rules of the Faster Payments Scheme, developed and proposed by industry; or action by the Payment Systems Regulator.

The Payment Systems Regulator made clear that, in its view, it currently lacks the powers to take action on reimbursement. This is based on the Payment Systems Regulator's interpretation of the

21 The Guardian (2020), *Which? calls for all banks to adopt anti-fraud measures*
22 House of Commons Treasury Committee (2019), *Economic Crime: Consumer View*, p.29
23 TSB (2020), *TSB reveals 100 percent reimbursement rate for innocent victims through the TSB Fraud Refund Guarantee*

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. As a result, the Payment Systems Regulator argues that it cannot currently require reimbursement to be made to APP fraud victims. The Payment Systems Regulator did note that this position may well change in the near future, and as the UK's future relationship with the EU becomes clearer, it is possible that the Payment Systems Regulator will be able to take action.[24]

**Recommendation 5: The Payment Systems Regulator should have the powers and the appetite to act to make reimbursement for APP fraud mandatory. Which? wants the government to clarify whether this is the case, and if necessary direct the action it expects the regulator to take.**

## Greater transparency of firms' approaches to reimbursement

The CRM Code aims to reduce the occurrence of APP fraud, and to reduce the impact of these crimes.[25] Both aims can be measured at an industry level using data that is currently collected and published by UK Finance.

The first of these aims is a long-term challenge, with the Code just one part of the fight against fraud. A wide range of factors outside the control of firms can also drive the level of fraud. The significant increase in the number of victims and the amount of money lost to APP fraud over the past two years is nonetheless highly concerning. It also underlines the need to achieve the second aim, to reduce the impact of these crimes via fairer decisions on the reimbursement of victims.

The second aim can be measured more directly by industry figures. However, these industry aggregate figures do not show whether individual firms are being fair in their reimbursement decisions. The Payment Systems Regulator's figures cited earlier in this report are broken down by firm, but are anonymised. They do, however, highlight that there are huge differences in reimbursement rates by firm.

Separately, the government has already committed to implement a recommendation by the Public Accounts Committee to 'press the banking industry to make relative online fraud vulnerability performance data publicly available'. The government noted that this could 'help incentivise performance and allow consumers to be more informed about anti-fraud measures', but that 'there may be risks and unintended consequences with publishing some fraud performance data'.[26] The Home Affairs Committee has since endorsed the Public Accounts Committee's approach, and made a similar recommendation to government. The Home Affairs Committee also disputed that publishing data on fraud could help criminals.[27]

The government has since said that its approach would involve 'a publicly available assessment of activity undertaken to reduce vulnerabilities' such as 'a number/star-system approach, akin to hotel rating standards or sector specific wide kitemarks'.[28] But this system has yet to be implemented.

The risk that publishing certain information could help fraudsters to identify weaknesses in the system is a risk we take very seriously at Which? when we research and investigate fraud.

24 Payment Systems Regulator (2020), *Authorised Push Payment (APP) scams conference call – 30 March 2020*, pp.9–10
25 APP fraud Steering Group (2018), *Draft Contingent Reimbursement Model Code: Consultation Paper*, p.4
26 HM Treasury (2018), *Government response to the Committee of Public Accounts on the Fourth to the Eleventh Reports from Session 2017–19*, p.12
27 House of Commons Home Affairs Committee (2018), *Policing for the future*, p.31
28 Home Office (2018), *Letter to Meg Hillier MP from Sir Philip Rutnam Permanent Secretary, Home Office, 25 June 2018*, p.2

However, we do not think that publishing data by firms on reimbursement rates of victims poses a significant risk. Instead, we suggest that publishing these data could primarily help to drive improvements in how firms treat victims.

**Recommendation 6: The Payment Systems Regulator should require all payment service providers to submit data on the level of APP fraud and reimbursements, and the Payment Systems Regulator should publish reimbursement rates for each provider.**

**Recommendation 7: The Financial Ombudsman Service should publish data for each provider on the level of APP fraud cases that it receives.**

## Industry-wide take-up of Confirmation of Payee

Since the start of July 2020, the six largest banking groups have been required by the Payment Systems Regulator to offer Confirmation of Payee. This is an important security measure to help protect customers against fraud: it means that when a customer makes a bank transfer to another participating firm they can check whether the account name matches the account number. Fraud is often highly sophisticated, and fraudsters will still find ways to convince victims that the account name is the payee they intend to pay. Nonetheless, Confirmation of Payee should make it harder for fraudsters to operate. It will also add an extra risk warning for both customers and payment service providers to help them identify fraud.

Lloyds Banking Group, which began offering this service in March 2020, has reported that Confirmation of Payee has already helped to reduce fraud by 31% among customers who had used the service.[29] Based on analysis by the Payment Systems Regulator, Which? has estimated that approximately £320 million of losses to customers could have been prevented in total if Confirmation of Payee had been introduced at the beginning of 2017.[30] This is based on Payment Systems Regulator estimates that 70% of misdirection fraud will be prevented in its first year, and 75% each year afterward.[31]

Despite these huge potential benefits, Confirmation of Payee was considered at least as early as 2011 by the then Payments Council[32] but has only just begun to be implemented for customers this year. Without the Payment Systems Regulator's mandatory rules, it may have taken even longer. Yet many payment firms fall outside of the Payment Systems Regulator's requirements to implement Confirmation of Payee. Some banks have indicated that they will choose to offer Confirmation of Payee,[33] but only Monzo and Starling have begun to offer the full service to their customers voluntarily.[34] Metro Bank told Which? in March 2020 that it had no current plans to implement Confirmation of Payee at all, despite this being a requirement of the CRM Code, which Metro Bank signed up to. It has more recently told Which? that it is currently exploring the options for implementing Confirmation of Payee for its customers, but has not committed to any deadline.

We strongly disagree with the Payment Systems Regulator's decision to limit the requirements to implement Confirmation of Payee to six banking groups. This is likely to mean that many

29 ThisisMoney.co.uk (2020), *Name-checking fraud prevention system has already reduced bank transfer scams by 31% says Lloyds*
30 Which? (2020), *Which? calls for mandatory transfer scam protections as losses set to hit £1 billion*
31 Payment Systems Regulator (2019), *Confirmation of Payee: Consultation on specific direction*, p.29
32 Payments Council (2011), *National Payments Plan*
33 Which? (2020), *Confirmation of Payee deadline: how will it affect your online banking?*
34 Payment Systems Regulator (2020), *PSR confirms widespread implementation of name-checking system, Confirmation of Payee*

customers are not offered the benefits of Confirmation of Payee at all. Even the customers of the six banking groups are not always able to use Confirmation of Payee because the service requires both the sending and receiving firms to participate. Many people are also customers with more than one payment service provider: 44% of people with a personal current account have more than one current account, according to the Financial Conduct Authority's Financial Lives survey.[35] So these people may be offered the service with one of their providers but not another. And perhaps most worryingly, fraudsters are likely to shift their behaviour and target payment service providers that do not offer Confirmation of Payee.

**Recommendation 8: The Payment Systems Regulator should mandate all payment service providers to introduce Confirmation of Payee. For any firms that require more time, the Payment Systems Regulator should set out a subsequent deadline or series of deadlines for these firms to introduce Confirmation of Payee as soon as is practically possible.**

35 FCA (2017), *Financial Lives Survey, Weighted data tables: Main*, Table 181

Which?, 2 Marylebone Road,
London NW1 4DF
Phone +44 (0)20 7770 7000
Fax +44 (0)20 7770 7600