Which?, 2 Marylebone Road, London, NW1 4DF
Date: September 2020

Consultation Response

The Lending Standards Board's Review of the Contingent Reimbursement Model Code for Authorised Push Payment (APP) Scams

Summary

- Reducing the occurrence of APP fraud must be the overwhelming priority of policymakers, industry and consumers. But the Contingent Reimbursement Model (CRM) Code's primary objective should be to increase the proportion of customers protected from the impact of authorised push payment (APP) fraud.

- While there has been an increase in the share of victims being reimbursed by signatories to the CRM Code, firms are not consistently meeting the Code's standards in how they approach reimbursement decisions and treat victims.

- To ensure that firms approach reimbursement decisions fairly, the Lending Standards Board should urgently work with firms to ensure they:
    - test warnings to see if they are 'effective';
    - base their judgements of what is reasonable on evidence of actual customer behaviour; and
    - evidence that they have implemented Confirmation of Payee in a way that customers can understand and respond to, before this provision can come into effect.

- If firms are unable to provide evidence of the above, then they should not be rejecting reimbursement based on the relevant consumer standards. These provisions in the consumer standard should therefore not apply, either for individual firms or all firms.

- Firms should ensure they train all relevant staff in how to support customers who could be, or may have been, vulnerable to APP fraud. They should also provide victims with specific reasons to explain their reimbursement decisions.

- Firms should have the option to self-fund reimbursement in 'no blame' cases, to help encourage firms to sign up to the Code. However, an industry fund would be a better long-term approach.

- More broadly, Which? agrees with the Treasury Select Committee and UK Finance that standards for reimbursement should be set out in regulatory rules, rather than the existing voluntary CRM Code. The government should clarify whether the Payment Systems Regulator can introduce these rules for reimbursement, and if necessary

provide the regulator with suitable powers or direct the action it expects the regulator to take.

Introduction

It is four years since 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 most significant change since our super-complaint has been the launch of the voluntary CRM Code, in May 2019, following a proposal by the Payment Systems Regulator and subsequent work by industry and consumer representatives. We welcome the work that the Lending Standards Board has done since it took on the governance of the Code. And we welcome the opportunity to respond to the Lending Standards Board's review.

In August, Which? published the report *Reimbursement for authorised push payment fraud: Consumer experiences of the Contingent Reimbursement Model Code*. The report shares some experiences drawn from around 150 victims who have contacted Which? since the CRM Code was launched. It was intended to help inform the Lending Standards Board's review of the CRM Code, as well as making recommendations to other policymakers. In this submission we summarise our findings and answer specific questions from the Lending Standards Board's consultation.

The Code's primary objective should be to increase the proportion of customers protected from the impact of APP fraud

The CRM Code sets out three overarching objectives:
1. To reduce the occurrence of APP fraud
2. To increase the proportion of customers protected from the impact of APP fraud, both through reimbursement and the reduction of APP fraud
3. To minimise disruption to legitimate Payment Journeys.[1]

Reducing the occurrence of APP fraud must be the overwhelming priority of policymakers, industry and consumers. However, there are a wide range of factors outside the control of firms that also drive the level of fraud. The whole ecosystem needs to do more, including

[1] Note, we use the term 'fraud' throughout but the CRM Code uses the term 'scams'.

telecommunications providers and social media platforms. Banks and building societies are just part of the solution, so there are limits to what the Code can achieve.

Nonetheless, the significant increase in the number of cases and the amount of money lost to APP fraud over recent years is highly concerning. While data are not directly comparable between years, because fewer banks provided data on APP fraud in 2017, there were 114,731 recorded cases involving customers with personal bank accounts in 2019, up from 38,596 in 2017. Across these cases, fraudsters stole £317 million in 2019 compared to £108 million in 2017.[2] The latest figures for the first half of 2020 show that recorded cases have increased further compared to the same period last year.[3]

While it is difficult to evaluate the extent to which the Code has helped to prevent the occurrence of APP fraud and firms' preventative measures predominantly remain out of sight, we believe the Code has helped to provide renewed impetus for signatories. In particular, we've seen firms introduce warnings for customers that are tailored to the purpose of the payment. As we discuss below, though, we have yet to see evidence on the extent to which these warnings prevent APP fraud.

The CRM Code's second objective, of increasing the proportion of customers protected from the impact of APP fraud, should be the primary objective of the CRM Code. It should also be focused on reimbursement, as this can be more directly impacted and measured than prevention. Below we focus on the evidence so far on this objective.

The third objective, of minimising disruption to legitimate payment journeys, should not be a primary objective of the CRM Code. The drive to minimise disruption to payment journeys in the way that Faster Payments and firms' systems have developed over recent years has made it much harder to prevent APP fraud. Given that firms are clear that it is not possible to identify all fraudulent transactions, legitimate journeys will have to be disrupted to help prevent fraud. Indeed, many of the protections that firms have introduced, including warnings and Confirmation of Payee, involve greater friction. Minimising disruption to payment journeys could, though, be a design principle of the Code that is considered alongside others.

Reimbursement rates have increased but firms are not consistently meeting the Code's standards in their reimbursement decisions and in how they treat victims

In the past year, we have seen an increase in the share of victims being reimbursed. 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%.[4] In the second six months, 38% was reimbursed by signatory firms.[5] Rates of reimbursement were also

[2] 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 (2019), 2020 Half year fraud update, p.23
[4] UK Finance (2020), Fraud – The facts 2020: The definitive overview of payment industry fraud, pp.46
[5] UK Finance (2019), 2020 Half year fraud update, p.23

higher for some types of scam. Which? has 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, 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'.[6] Which? agrees with the Payment Systems Regulator's assessment.

The Payment Systems Regulator has also published anonymised data for individual firms relating to reimbursement rates, which showed 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.[7]

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.

Firms are not meeting the Code's standards in how they approach reimbursement decisions and treat victims

Which?, the Payment Systems Regulator,[8] the Financial Ombudsman Service[9] and the Lending Standards Board's interim review[10] have all found issues with reimbursement decisions. Which? has seen and helped intervene in cases where there have been issues with:

An over-reliance on victims having ignored warnings

---

[6] Payment Systems Regulator (2020), Authorised Push Payment (APP) scams conference call – 30 March 2020, p.5
[7] Payment Systems Regulator (2020), Authorised Push Payment (APP) scams conference call – 30 March 2020, pp.23–24
[8] Payment Systems Regulator (2020), Authorised Push Payment (APP) scams conference call – 30 March 2020
[9] Payment Systems Regulator (2020), Authorised Push Payment (APP) scams conference call – 30 March 2020
[10] 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

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 that we have been involved with, the customer's bank or building society cited the warnings that they had provided. But the victims we spoke to often didn't remember seeing these, or they did but felt the warning wasn't relevant. Other victims were coached by the fraudster to respond in particular ways and ultimately to ignore the guidance offered in any warning.

Despite these issues with warnings, Which? has seen that many firms did not sufficiently consider the circumstances of the fraud and how the warning was perceived by their customers. Firms were primarily concerned with establishing that a warning had been provided, and that the customer had still proceeded with the payment. This was in some cases sufficient reason to reject a reimbursement claim.

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

Firms can reject reimbursement if 'the customer made the payment without a reasonable basis 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 does not state that customers are required to have taken active steps when making a payment. This is because steps that may seem rational to bank staff may not align with how people actually behave. APP fraud can be so convincing that a consumer could have a 'reasonable basis for believing' even without taking extra steps, and they may be rushed into making the payment.

However, in some of the examples we have seen, firms have assumed that customers should have taken steps in order to be reimbursed. These issues are partly due to firms not sufficiently taking into account the circumstances of the payment and the sophistication of the fraud, as the Code requires. In some of these examples, the fraudster contacted the victim using the same email, phone or SMS details as a legitimate organisation, including their bank. In other examples, the fraudster was able to convince individuals to download software that then enabled them to access the victim's device remotely. 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.

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. One victim was initially rejected for reimbursement. 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

Which? has seen many examples where firms have not provided the customer with the 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 point on responsibility is unclear and 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.

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 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.

Firms should test warnings to see if they are 'effective' and base their judgements of what is reasonable on evidence of actual customer behaviour

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'.[11]

Furthermore, 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. 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.

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 that are likely to be more informed about how to protect themselves from fraud. 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 has found evidence of, is unlikely to be sufficient to meet the requirements of the CRM Code.

Which? would 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.

If firms are unable to provide reliable evidence that their warnings meet the 'effective' requirements or regarding what is reasonable actual customer behaviour, then decisions on

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

reimbursement should not be made using the provisions in the consumer standard that reference these. Until such time, these provisions of the consumer standard should not apply, either for individual signatories or for all signatories.

We also do not believe that the provision in the consumer standard on Confirmation of Payee, which is not currently live, should come into effect until firms have evidenced that they have met the Code's requirement to 'implement Confirmation of Payee in a way so that the Customer can understand, and respond to it'.

Firms should ensure they train all relevant staff and provide victims with specific reasons to explain reimbursement decisions

Which? was particularly concerned by the Lending Standards Board's finding 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 has also already found that it was not always clear that all staff who are impacted by the Code had received training.[12] This lack of training is likely to disproportionately affect customers who were 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. 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.

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. Firms should also explain that they will assess whether the victim has met the consumer requisite level of care when making the payment. If the firm chooses not to fully reimburse the victim, they should specify 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.

Firms should have the option to self-fund reimbursement in 'no blame' cases but an industry fund would be a better long-term approach

[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, p.8

We believe that a permanent funding model should urgently be agreed for cases that are deemed to be 'no-blame', where the firms involved and the victim have all met the Code's standards. Following the rejection of the proposal for a levy on Faster Payments, until a solution is agreed firms should be able to self-fund reimbursement in the no-blame scenario if they would prefer not to pay into the existing interim no-blame fund. This would remove one of the main barriers that non-signatories cite to signing up to the Code, without changing the outcome for individual victims. However, 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.

Standards for reimbursement should be set out in regulatory rules rather than the voluntary CRM Code

As well as the Lending Standards Board's review of the implementation of the CRM Code, Which? is calling on the Payment Systems Regulator to evaluate the effectiveness of the voluntary approach it has opted for to tackle the harm identified by Which? in its super-complaint. This is not something that the Lending Standards Board can fully do.

Which? believes that the evidence over the past year shows that standards for reimbursement should be set out in regulatory rules, rather than the existing voluntary CRM Code. This would be much more likely to lead to fairer and more consistent outcomes than we have seen under a voluntary approach. It can also ensure that all payment providers are included. Which? notes that 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. Given that the Payment Systems Regulator has repeatedly stated that it does not believe it is currently able to mandate reimbursement, the government should clarify whether this is the case, and if necessary provide the regulator with suitable powers or direct the action it expects the regulator to take.

About Which?

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.

For more information, contact Alastair Reed, Principal Policy Adviser
alastair.reed@which.co.uk
September 2020