Lending Standards Board

2022 Review of adherence to Contingent Reimbursement Model Code for Authorised Push Payment Scams

Summary Report

September 2022

Contents

Introduction

The Contingent Reimbursement Model Code (CRM Code) sets out good industry practice for preventing and responding to Authorised Push Payment (APP) scams. The CRM Code was developed through collaboration between consumer and industry groups, to reduce the impact of APP scams on customers, micro-enterprises, and small charities.

The Code aims to achieve this by requiring that signatory firms put in place measures to reduce the occurrence of APP scams, and by ensuring their customers will be reimbursed if they have been the victim of an APP scam and were not to blame for the success of the scam.

The Lending Standards Board (LSB) is the independent governing body of the CRM Code whose role is to monitor signatory firms' implementation and ongoing adherence to the CRM Code, to ensure its effectiveness, and to maintain and refine it, as required.

The LSB is the primary self-regulatory body for the banking and lending industry, driving fair customer outcomes within financial services through independent oversight. Our registered firms comprise the major UK banks and lenders, credit card providers, debt collection agencies and debt purchase firms. Adherence to our Standards of Lending Practice and the other Codes of Practice which sit within our remit is a clear indication that a registered firm is committed to best practice in the treatment of its personal and business customers.

1. Executive Summary

Background

The LSB became responsible for the governance and oversight of the CRM Code in 2019. To date we have conducted three thematic reviews, covering the Code requirements focussed on provision of effective warnings and reimbursement of customers who have fallen victim to an APP scam. The most recent of these reviews was conducted in 2021, a copy of the report can be located here.

As part of our business plan, we committed to completing a full assurance review, with coverage across the Code provisions associated with the customer's entire payment journey. The intention of this work has been to assess how firms have completed and implemented any actions raised by the LSB within the previous three reviews, whilst ensuring the Code is now fully embedded three years on from becoming effective.

This is particularly important as Brexit, the pandemic, the war in Ukraine, and the cost-of-living crisis, are creating a perfect storm of challenges within our society. An increasing number of people are experiencing new or heightened personal struggles and financial hardship, which may drive an increase in customers seeking opportunities to maximise on income and reduce expenditure where they can. This creates an ideal environment for scammers to exploit customers.

As the Code is the only set of protections to prevent, detect and respond to APP scams, it is more important than ever that signatory firms and the wider industry take note of the areas of improvement set out within this report to reduce customer harm.

The review was conducted across the nine firms that were signatories to the Code as of 1 February 2022.

1.1 Key Findings

We are encouraged to see that, overall, firms have put in place clear plans to address issues raised in our previous reviews, with this review providing us with an opportunity to validate those actions. We have seen progress across a number of firms and some good practice now emerging which we have commented on later within this report.

The key areas of improvement have included the following:

- Firms generally have adopted sound governance structures relating to the Code and have suitable Executive accountabilities in place with a clear understanding of the requirements of the Code.

- Firms have placed increased focus on scam prevention, with most making better use of customer transactional behaviour and data analytics to prevent suspicious payments. This, at times, has led to firms contacting customers about suspicious transactions before the customer realises they have been scammed.
- Firms have made better use of educational and awareness material, including use of email and social media, with increased focus on proactive awareness-raising of prevalent scams.
- There was felt to be a marked improvement across firms in the manner in which they approached the discussions held with impacted customers, both in probing the circumstances and detail of the scam to assess the claim.
- It was evident that firms have been focused on development of effective warnings with these being designed to be more targeted and tailored in content, particularly within digital channels.
- Where firms have improved the initial engagement with customers, to understand the circumstances of the scam, this has helped in providing customers with a clear rationale for the reimbursement decision.

Whilst it is acknowledged there have been a number of key improvements, there is still a need to ensure that activities relating to the Code are fully embedded and applied consistently, in order to continually provide good outcomes for customers.

Therefore, there remain some areas where further work is required to ensure all firms are consistently applying the requirements of the Code when dealing with both the prevention of APP scams and assisting customers who have fallen victim to a scam.

The key findings identified from this review where further improvements are required include:

- **Use of effective warnings in face to face interaction[1] -** We continue to have concerns where payments are made through face to face interaction that warnings were not always sufficient to prompt customers to take action prior to making the payment. In many cases, such warnings in these channels are only provided once a payment threshold is exceeded.
- **Oversight** – While we acknowledge that some firms are actively reviewing and embedding internal oversight requirements applicable to the Code, we found that for a number of firms, there is some element of oversight or assurance work which could be improved. Often, oversight was focussed on an assessment that the process for claims had been correctly followed, rather than a detailed assessment of the reimbursement decision rationale. At times, we found it difficult to confirm the depth

[1] Where we refer to 'face to face interaction' this means non-digital, typically referring to branch and telephony channels.

of quality assurance work undertaken, given that in many cases the reporting was at a high level and did not provide granular detail or full records of the oversight activity undertaken.

- **Reimbursement decision rationale** – Overall, our sample testing identified that there were still many examples whereby firms were unable to demonstrate how the reimbursement decision had been reached based on the rationale provided. This means that customers were then unable to understand the reason for the decision, in particular where reimbursement was declined. We continued to see examples where the rationale was based on specific checks the firm deemed were not completed by the customer, or that customers had not met a 'standard of care' or the requirements of the Code, despite the Code not being binding on customers.
- **Perception of customer responsibility** – We saw firms continue to make reference to a requirement on customers under the Code to take a 'requisite level of care'. As we have stated in previous reports, it is entirely the firm's responsibility to demonstrate when and how it has assessed that an exception allowable under the Code is utilised in reaching a decision to not reimburse the customer. There is no standard of care or specific responsibilities placed on customers via the Code, and in any event, the Code does not bind customers. This should be reflected in firms' processes.
- **Customer vulnerability** – During our 2021 review, we noted that firms' ability to successfully identify and provide support to customers who may be vulnerable to a scam was not as developed as it should have been. We continue to see inconsistent application of the Code in this area and therefore a risk of potential customer detriment. Firms should enhance training and oversight of this important area.
- **Customer communications** – We noted that the content of firms' decision letters appeared to be very templated in content, typically providing a list of checks highlighting what could have been done by the customer to avoid the scam and often with an element of hindsight. Reimbursement decision letters should provide a clear rationale to enable customers to understand how their claim has been assessed, the decision reached, and to help them avoid scams in the future.
- **Customer communications -** Where a claim response is likely to take longer than 15 business days (or 35 business days in exceptional circumstances), the Code requires that customers are provided with updates informing them of the reason for delay and to advise that they may make a complaint to either the sending or receiving firm. In a number of firms, we continued to see cases where customers either did not receive the notification or did not receive sufficient information as required by the Code within the notification provided.

It is acknowledged that firms have, and continue to, embed the requirements of the Code. Whilst we have identified some areas where there remains inconsistency of application, overall signatory firms are committed to ensuring the Code is working and customers are protected from APP scams.

1.2 Objectives and Scope

The objective of the review was to understand how each firm has interpreted, implemented, and embedded the requirements of the CRM Code across the whole payment journey, including validation of any actions raised as part of previous thematic reviews, whilst ensuring consistency of approach across the signatories to the Code.

We assessed the practical application of the Code by firms across the principal requirements of Governance and Oversight, the payment journey for both sending and receiving firms, and the reimbursement of the customer following an APP scam. There was also consideration of any other provisions which may be relevant. At all stages of the review, we assessed how firms considered vulnerable and potentially vulnerable customers. The work did not encroach on the jurisdiction of the Financial Ombudsman Service (FOS).

The review included an assessment of:

- The governance, controls, monitoring, and oversight in place to ensure adherence to the Code. This incorporated: knowledge and awareness; the risk management framework; management information; complaints and root cause analysis; breach reporting; and employee training.

- The general expectations of firms: including general consumer education and awareness campaigns, and the process and procedures in place to help with customer aftercare.

- As the sending firm: policy and process around the creation and implementation of effective warnings throughout the payment journey and any other preventative tools firms employ. Measures firms have in place to detect payments at a higher risk of being an APP scam were also considered.

- As the receiving firm: establishing the procedures in place to help prevent, detect, and respond to the receipt of funds from APP scams. This included gaining an understanding of the ongoing transactional monitoring controls and the measures in place for due diligence at account opening and how this is considered when responding as a receiving firm.

- For reimbursement: the policies and processes firms have in place to assess claims under the Code. This included considering how the exception requirements, such as a reasonable basis for belief, are applied in the assessment of customer claims.

- Vulnerability: assessing the procedures firms have in place to identify customers vulnerable to APP scams, and how the relevant Code provisions are applied across the customer journey.

Out of Scope

The review scope did not include a detailed assessment of the Confirmation of Payee (CoP) requirements for all signatory firms, as the relevant provisions within the Code were only activated on 28 April 2022 and the commencement of this review preceded this date.

1.3 Methodology and Approach

The review was conducted in a number of stages. Firstly, firms were requested to submit a range of information through a detailed Request for Information (RFI). This allowed for an initial desktop assessment of how firms have interpreted and implemented the relevant requirements of the Code within policies and procedures.

Following the desktop assessment of documentation, we conducted a number of structured discussions with management to understand how the Code has been implemented and embedded, together with assessment of how any actions from our previous thematic reviews have been resolved. These meetings also provided an opportunity to raise any queries arising from the desktop assessment.

The final element of the review was sample testing of case files, undertaken on-site at each firm, across a range of scam types and channels. The purpose of this was to test the design and operational effectiveness of each firm's policies and processes in managing scam claims.

It should be noted that our sample testing was focussed on the actions of the sending firm. We did not conduct any specific testing from a receiving firm perspective. This part of our review was focussed on a desktop assessment of policies and procedures and discussion with management at firms to understand how they are meeting the requirements of the Code as a receiving firm.

On conclusion of the above, we held a close-out meeting with each firm to discuss the initial findings from their respective review. This was followed by an individual report being issued to each firm, setting out the LSB's findings from the assessment.

2. Detailed report

2.1. Governance and Oversight (GO)

In June 2021 the LSB introduced new provisions into the Code, focusing on requirements for Governance and Oversight. These provisions were introduced to assist signatory firms with the embedding of an effective governance framework and to support the ongoing oversight of the Code's requirements. This element of the review was designed to assess how well these frameworks were providing the required visibility of adherence to the Code throughout firms.

Generally, we found firms had in place structured frameworks with clear roles and responsibilities defined to meet the governance requirements of the Code. Some elements of the GO provisions still require embedding, of which further detail is set out below. The committee and forum structures in place have remained largely unchanged since the launch of the Code, with these typically focussed on more complex scam cases and operational assessment.

Reporting and management information

We found that, since our previous review, most firms had undertaken work to improve their collation of, and analysis of, Management Information (MI), which leads to better reporting to firms' Executive Committees. However, we saw inconsistencies in the quality of reporting and the extent to which informative MI was being presented to relevant governance committees, with a focus continuing to be on claims volume and monetary value data. Our view is that adherence to the Code should be driven 'from the top'. Without full visibility of how the Code is being applied and working, Executive and Senior Management are unable to ensure customers remained protected by its provisions.

Where we found that assessment and use of MI was working well, this tended to be where firms were exploring ways to better analyse system and behavioural data to identify success measures relating to scam prevention. Where firms were using these initiatives, they were better able to react to scam trends more quickly and expedite the change process, where required, through governance in order to provide education and scam prevention tools to customers soon after a trend is identified.

Assurance and oversight

Most firms have adopted a three lines of defence model when considering oversight of the Code. We found that oversight within the first line of defence tended to focus heavily on whether the internal process was correctly followed rather than reviewing the assessment of the case, which should include determining whether the correct rationale for the outcome

decision had been applied. We also found that, in some firms, the level of independent assurance conducted by second and/or third line of defence was limited in coverage. In some instances, this was due to the various change programmes needed to implement actions as a result of our previous reviews.

However, it is noted that by including the assurance and audit functions within the change management programmes, this ensured there remained a level of oversight of revisions to policy and process prior to implementation.

Oversight functions are critical in ensuring compliance with the Code across all aspects of the customer journey and the results of such oversight should form a key part of the MI as mentioned above, to ensure visibility at Executive level.

While we found that further embedding and enhancement to oversight was required, we also found that firms' understanding of the requirements of the Code, and how this should be applied operationally, was much improved.

Staff training

We consistently found that training and coaching for customer facing staff had improved. For those who are directly involved in customer claims, some firms were moving towards these being specialist roles, with training and competence standards put in place to ensure competency and Continuous Professional Development. For staff in branch or telephony channels, firms had moved to improve APP scam specific training modules, with localised team meetings also being used to discuss scams.

As a result, we were able to determine that scam specific training has become more structured within most firms, with Training and Competency frameworks being introduced. Firms now need to focus on ensuring that this training is fully integrated into the customer experience and continue to develop continuous learning for all staff involved in the customer journey, rather than relying on ad hoc refresher training. In order to be able to better evidence the required embedding of knowledge and consistency of application of the Code requirements, as mentioned above, it is important that firms are conducting suitable oversight through their three lines of defence on all areas of the Code. Feedback from such oversight should be followed up with additional training, and coaching, where necessary.

Complaints and breach management

During our previous reviews, we found limited evidence that firms were using root cause analysis when considering trends within complaints. When we considered firms' compliance with requirements of the GO section of the Code with regard to complaint handling, we noted

that most firms now place greater emphasis on root cause analysis and are more proactive in discussing internally any changes or improvements identified from complaints analysis.

However, we did note that not all firms have a robust complaint handling process in place, and we found that some firms still need to enhance their use of root cause analysis in order to ensure that any trends are addressed. Where we found complaints handling processes and root cause analysis are working well, firms would use the information to help inform policy or process changes and to notify the business of training needs.

Complaints and analysis information is important when firms are considering the risks of incurring breaches of the Code. Generally, we found that firms have robust breach management processes in place, however these tended to be standard processes applicable to the business as a whole. Where breach management works well, the firm would consider how potential Code specific breaches are identified and recorded, considering the firm's approach to evidencing its application of the Code.

Areas for improvement:

- First line controls require further embedding , to ensure that CRM oversight fully considers all aspects of the payment journey, including sending and receiving requirements and reimbursement claim decisions. The output of these assessments should be clearly recorded with relevant feedback provided to staff.
- Firms need to complete, and embed, training and competency arrangements to ensure that appropriate customer outcomes are consistently achieved.
- While we acknowledge that firms generally have undertaken large programmes of change since our 2021 thematic review, firms need to ensure sufficient second and third line of defence assurance programmes are established and that Code related topics are considered within future annual planning activities.
- Further development of MI should reinforce improved governance reporting of all aspects of adherence to the Code. Focus needs to be across the full customer journey and not limited to claims data.

Areas where firms have demonstrated improvement:

- Generally, firms' understanding of the requirements of the Code and associated accountabilities and governance structures is strong.
- Some firms have recognised that adherence to the Code can be strengthened by having APP specialised customer facing and investigation staff in place and have developed more structured training and competency programmes to further embed knowledge.

2.2 General Expectations of Firms (GF)

In line with this section of the Code, we assessed the depth and quality of tools aimed at educating customers about scams and how to avoid them. In addition, we reviewed post claim aftercare to assess firms' ability to help prevent customers from falling victim to APP scams in the future.

Awareness and education

We found that nearly all firms placed significant focus on the provision of customer education, in order to promote awareness and equip customers with better knowledge to assist in spotting a scam before proceeding to make any payment.

Firms are now providing better quality information relating to APP scams within websites. Digital effective warnings now tend to include direct links to further guidance to encourage customers to 'stop and think' and read additional support material prior to making the payment.

Within digital channels, we saw instances of clear signposting to scam awareness pages which included use of prominent information related to prevalent scams. Firms were also using direct links from website home pages and messaging within digital banking pages to encourage customers to view this information.

We also found that firms were making better use of internal and external data sources, allowing them to spot trends sooner and act accordingly, which may include issuing targeted emails, social media messaging and use of messaging and 'banners' within digital banking pages and during the payment journey. One consistent example of this in action related to a spike in scams originating from 'WhatsApp' messages. In identifying this as an increasing scam type, firms were able to quickly alter messaging, issue relevant communications and raise awareness of this type of scam.

Most firms within scope of this review had increased the number or use of education tools within branch networks, where relevant. It was common for firms to promote scam awareness material on service counters and poster displays within the branch. Some firms also arrange customer forums within branches, at times making use of third-party specialist organisations. Generally, firms were also working more closely with law enforcement and external support groups in order to share knowledge and intelligence around APP scams.

Aftercare

We found that most firms had worked on providing better aftercare to customers. Where this worked well, relevant aftercare was being provided verbally at an appropriate time during the claim process. However, at times we found that there was inconsistency as to when verbal aftercare is provided, with examples of this being discussed at points when customers may not be very receptive to the information, such as when first reporting the scam or when requesting the outcome of their claim. On occasion, we found that no aftercare was provided at all.

It is important that the customer is in the best frame of mind to absorb this information. While we appreciate that each discussion is unique, we would encourage firms to assess relevant considerations around when may be the optimum time to raise aftercare to allow for maximum impact.

We continued to see examples where the decision letter was relied upon to provide aftercare with this information, at times, not being sufficiently tailored to the customer's circumstances. We also found examples where customers did not receive any aftercare at all, either verbally or in writing, usually where the reimbursement claim had been successful.

Where firms have adopted a policy of automatically reimbursing a customer in certain threshold circumstances, as described in section 2.5 of this report, we found that customers do not receive the same level of aftercare offered to customers who have undergone a full claim assessment.

We also found that firms could do more to identify whether the customer would benefit from support from external parties, such as charities or third-party support organisations, and to provide sufficient signposting to organisations that may be able to assist. Falling victim to a scam, in particular one which has involved high monetary value or a continual breach of trust, such as within romance scams, can have significant non-financial impacts on customers, for example on their mental health. While firms are improving practices for identifying such circumstances, the ability to provide enhanced support with the assistance of third parties, or referral to internal customer support functions, could be more consistently utilised and signposted. Customers would also benefit from firms having in place strong processes for identifying and supporting circumstances where the scam has the potential to lead to financial stress or hardship, particularly in light of the ongoing cost of living crisis.

Areas for improvement:

- Firms should continually review and improve website information pages and education on scams, making sure these are easily accessible and contain suitable content.

- Aftercare provided to customers should be delivered verbally, as well as in writing, at the most appropriate time during the reimbursement claim process, in order to achieve maximum benefit to the customer.
- Aftercare should always be provided, whether customers are reimbursed or not. This includes cases where firms have chosen to make automatic reimbursement.

Areas where firms have demonstrated improvement:

- Better use of internal and external data sources, and better sharing of intelligence, have allowed firms to react swiftly in providing education through targeted campaigns, therefore improving scam prevention. This was most evident in updates and targeted customer contact campaigns related to identified prevalent scams.
- We saw examples of customers who had fallen victim to a scam being invited to specific aftercare webinar sessions to assist with future scam protection, together with improved use of direct customer engagement in branch or by telephone.
- Some firms are including useful general scam awareness leaflets, for example within the outcome letters, whilst providing more specific information, relevant to the actual scam, in the letter itself.

2.3 Standards for Firms: Payment Journey - sending Firm (SF)

Our key areas for assessment under sending firm requirements included firms' activities around how they are able to prevent scams from occurring, through use of payment risk assessment tools and technical solutions, together with transactional monitoring. We also assessed how firms are designing and implementing effective warnings during the payment journey across all channels.

Prevention and transaction monitoring

When we considered firms' ability to suspend potentially suspicious payments, or to use transactional data to assess payments at higher risk of being a scam, we noted that there had been an improvement in this important area. Firms were better able to link customer transactional data to be able to identify and suspend out of character payments and doing so in a way that did not add substantial barriers to the general payment journey. During outcome testing, this was most evident in examples where firms were able to identify and stop multiple scam payments, and in doing so prevent further funds being lost. This led to situations where it was, in fact, the firm who was notifying the customer that they had stopped the payments prior to the customer realising they had been scammed. We saw an increase in the number of payments suspended at point of being requested, using trends and intelligence received from internal and external sources and using this information in conjunction with risk triggers within payment systems.

We noted that further use of transactional data and technological advances will allow for continual improvement in assessing and identifying transactions at risk of being a scam. We also found that some firms were better prepared than others to identify high risk transactions, in particular in cases where lower value transactions were involved.

Effective warnings

We considered how firms had developed the provision of effective warnings, together with their ability to identify payments at a higher risk of being a scam and then suspend or stop such payments.

We found that most firms had made progress against the requirements within the Code to supply the customer with effective warnings, in particular where payments are made through digital channels. Warnings have become more focussed on the nature of the payment and potential scam type. Typically, this is done by use of a payment categorisation tool requesting the customer confirm, generally, what the payment is for. The response to this question can then drive a warning specific to the payment type and the likely scam type the customer is at risk of being exposed to. However, often this secondary payment page contained a fairly static warning, albeit reflecting a specific payment type.

We saw some examples of warnings being displayed more prominently, with increased use of visual interruption and direct messaging to encourage customers to take a step back and consider the payment. In most cases, where a warning is displayed within the digital channels, the customer must make a positive election to proceed. These warnings may include a direct link from the warning itself to further educational and guidance material on scam prevention, making relevant information easier to find while in the payment journey.

However, we did find areas where firms could improve further. Not all firms on digital payment journeys are displaying their warnings to maximum effect when considering visuals and content. We continued to see examples of warnings appearing as an additional page in the payment journey, with little to differentiate them from other elements. In addition, some firms were not maintaining a record of which scam warning is provided, instead relying on customers to recall what warning was provided or payment type chosen at the point of transaction. In firms where this was the case, customers tended not to be able to recall the warning information provided to them during the investigation process, with this sometimes having an impact on the decision for reimbursement.

Staff Training

Firms have improved training provided to branch staff, where relevant, and are encouraging staff to query with customers any payment that has indicating factors that it could be a potential scam. In a limited number of firms, staff have available other resources to assist with these discussions, such as scam related learning videos, which can be played to the customer to assist in their assessment of whether or not to make the payment.

However, we found that despite enhanced training, where payments were made via face to face interaction, customers were less likely to receive a warning, and there was often little discussion around the purpose of the payment. This appeared to be particularly apparent within telephony channels. We also identified examples of payment value thresholds continuing to be used before staff were compelled to hold a discussion. While we appreciate that staff are being encouraged to discuss and raise concerns for any monetary value, having thresholds in place can increase the risk of such preventative discussions not taking place. This is important, given that customers may believe that by speaking directly to their bank or building society, before making the payment, this provides a level of validation.

Review and continual improvement

Firms continued to note that assessing the impact of warnings continues to be challenging, however some are making better use of internal and behavioural data sources and customer 'point in time' feedback surveys. This should be seen as an integral part of continual review and adjustment of effective warnings to ensure these continue to meet the requirements of the Code.

Within outcome testing during the review, it was apparent that scammers may adjust their approach during the life of the scam to influence, through social engineering, the type of warning seen by customers, therefore rendering it irrelevant to the customer. We would encourage firms to make sure they are fully exploring and recording, during claim discussions, why customers have not reacted to the warnings provided. This, together with data analysis, should be used by firms to better understand the impact of their warnings to be able to adapt them to be as effective as possible.

We also found that firms typically still do not provide digital warnings where the payment is to an existing payee, and we continued to find examples of payment value thresholds in place for the provision of digital warnings. This can lead to more frequent lower value scam payments proceeding without specific warnings being provided. During our sample testing, we found examples where customers had been scammed for a series of smaller value transactions in an attempt by the scammer to circumvent such thresholds. Whilst the Code does not make reference to thresholds being used for the provision of warnings, it does state

that these should be provided in cases where a scam risk is identified. Firms should ensure, therefore, that they are basing the provision of a warning on the scam risks identified within the payment journey taking all pertinent information into account.

Notification of scam

When customers inform a firm that they have been the victim of a scam, a notification should be raised with the receiving firm, which is usually completed at the first point of contact. It is a requirement of the Code that this is completed in a timely manner to help stop the onward movement of funds and help with repatriation. To assist with this process, firms have in place internal timescales (SLA) to which they hold themselves accountable for notifying the receiving firm. However, these timings had a tendency to differ across firms, as did the decision on reimbursement when the firm missed their SLA.

We acknowledge that there are practical implications to contacting the receiving firm to notify it of a scam, and whilst we would not wish to set specific timings, firms should consider the impact of delays in notification when assessing cases for reimbursement. Where firms miss their SLA, they should ensure there is no customer detriment.

Areas for improvement:

- Firms should ensure that where a warning is provided, regardless of channel, records are maintained to confirm when this was delivered and the content of said warning.
- Firms should also further consider whether the use of payment value thresholds is appropriate, ensuring this is based on the scam risk with supporting justification and not as a result of commercial or resource reasons, when considering both digital and face to face interaction-based warnings.
- We would encourage firms to continue to review and assess the quality and impact of warnings, including those scam types which may apply to more than one payment type within payment categorisation questioning. Firms should ensure that warnings are reviewed and adjusted based on prevalent scams, as well as a programme of continual feedback and assessment.
- Firms should have in place a process for the continual review and assessment of the impact of warnings on the prevention of scams. This should include data from all relevant sources, including customers, to understand their reasons for proceeding with a payment despite the provision of a warning.

Areas where firms have demonstrated improvement:

- The use of technological advances, and better use of transactional data, are resulting in the improved ability of firms to detect and suspend potential suspicious payments. It was clear that some firms have been focussing on preventative measures as well as post claim processes.

- Firms are now making better use of data available, including feedback and customer behavioural analytics, to assist with the review of effective warnings. While we note above that firms should continue to review and update warnings, enhanced tools are being developed to assist in such reviews.

2.4 Standards for Firms: Payment Journey – receiving firm (SF)

As this review was scoped to cover the full customer payment journey, we took the opportunity to look in more detail at the processes firms have in place where they are the recipient of funds from an APP scam.

Prevention and detection

We assessed the processes firms have in place for account opening and account monitoring to detect customer accounts which may be at risk of being used for fraudulent purposes, including being used as mule accounts. We also reviewed the processes for dealing with claims received from the sending firm, including investigation, account suspension, receiving firm liability assessments and the repatriation of funds.

We found that most of this activity sat within a specialist team within fraud departments, which tended to hold wider responsibility for due diligence and monitoring of fraud and economic crime. We found that firms had defined policies and procedures for the opening of accounts, with internal and external data being used to complete customer due diligence. This was mostly a standardised process for account opening, with the automated data checks generally conducted through national fraud detection agencies.

Processes for the monitoring of accounts varied in thoroughness between firms, however all firms did have in place the ability to conduct transactional monitoring across all accounts held by the customer, together with regular updates from fraud reporting agencies. Where receipt of funds was deemed to be higher risk, these cases would be investigated by the fraud monitoring teams, which may involve account suspension and relevant discussions with customers.

Response to APP scam notification

Where a firm receives notification of an APP scam claim as the receiving firm, it will typically apply a suspension on the account. The account would then be reviewed, and the firm would carry out its own assessment of the payment, considering usual payment data. Where necessary, the firm will contact the customer for further information. We found that firms will also make an assessment of whether they would deem the payment to be covered by the Code. Where the receiving firm confirms the payment(s)to be scam activity, it will take action

to block the account permanently and report the activity to relevant fraud databases. The firm will then assess whether any funds are available for repatriation.

On the assessment of receiving firm liability, firms will typically ensure that the account opening procedures were followed, and that account monitoring had not failed. Where a receiving firm assesses that its processes were followed, the firm would typically not hold itself liable under the allocation provisions of the Code.

We are undertaking work looking at the balance of responsibilities between sending and receiving firms under the Code. Currently, its requirements are, in the main, focused towards sending firms. Our Code review process has identified that there is a need to draw out expectations more clearly on receiving firms. To support this work, we established a working group with all CRM Code signatories to explore what changes could be made to ensure that receiving firms do more to help prevent APP scams. Our findings from this review will also feed into the working group for discussion. We will provide an update on this work in due course.

2.5 Reimbursement of Customer Following an APP scam

This section of the Code provides for how firms should assess claims for reimbursement. We reviewed how firms approach the investigation of claims, interact with customers to obtain all information pertinent to the scam and subsequently how the rationale for the reimbursement decision is recorded and delivered to customers. We also reviewed the customer communications issued throughout the claim investigation process.

Firms' approach to claims

During this review, we found that firms had significantly improved their approach to the reimbursement claim assessment, with a move away from process driven or automated claim decisioning in favour of a more thorough conversation and dialogue with customers. This enabled a more holistic and rounded understanding of the full circumstances around the scam for firms to assess whether customers should be reimbursed.

However, at the time of our review, the need to continue embedding changes to process and training as a result of previous review actions continues to impact on how cases are being managed, resulting in inconsistent approaches to management of claims, discussions with customers and rationale for reimbursement decisions. Firms' internal oversight models and activities will therefore continue to be pivotal in measuring the success of such process implementation and embedding within their operational functions.

Some firms have moved to create specialist operational teams dedicated to scams, for example creating dedicated investigation teams for APP scams and building training and

competence arrangements around the specialism of the team's role. In general, we found that firms had committed to expanding resource to allow for stronger processes, including some having a single point of contact for customers throughout the claim process. However, given the need to recruit and train staff to the desired level, it is acknowledged that this will take time to embed but we were encouraged to see firms' progress in this area.

We would encourage firms to also provide more information to customers at the first point of contact around the process for assessing the case under the CRM Code, how the reimbursement decision will be reached, as well as other pertinent elements. This will ensure the customer has the best opportunity to provide all relevant information on the scam or any supporting evidence they may have available.

We found that, where firms' staff were able to clearly understand the circumstances of the scam, either through single point of contact or through high quality case notes, customers were more likely to have been able to provide sufficient information, which created a better opportunity to reach a fair customer outcome.

Where we found case investigation could be improved upon, this was at times due to the claim investigator acting on a lack of information around the case circumstances, and at times reaching decisions based on incomplete information. It is important that, in order to fully assess cases, firm receive and record all pertinent information at the appropriate point, which may include accepting any supporting documentation offered by the customer. We also continued to see examples whereby customers were having difficulty in contacting scam claim departments, due to a requirement to make contact through generic customer service centres.

Claim assessment

The Code requires that customers should be reimbursed when they have been the victim of a scam unless firms can establish that any of the exceptions in R2(1) (a) to (e) would apply. When considering whether a customer should be reimbursed, we found examples where firms were still basing their decision on whether or not the customer met a requisite level/standard of care or had met any of their 'responsibilities' under the Code. We want to be clear that there is no such responsibility placed on customers within the Code and reiterate once again that the Code is not binding on customers in any way and, therefore, has not been drafted to place a specific set of requirements on customers.

It is for firms to evidence that it is appropriate to invoke an exception under section R2. At times, we continued to see claim assessments focussed on checks that customers did not undertake, rather than making assessments of, and understanding, the checks the customer had undertaken. Assessments must consider the characteristics of the customer together

with the complexity/sophistication of the scam which led to the customer proceeding with the payment. This, at times, led to a 'hindsight' approach whereby the level of check required becomes obvious after the event. Firms must fully consider the circumstances at the time of the scam, putting themselves in the customer's shoes, and establish whether it was reasonable that the customer believed the payment to be genuine, rather than working through a list of arbitrary checks the customer could potentially have completed.

During previous reviews, we had identified that firms were using the provision of a warning as a strict reason to deny reimbursement. We were pleased to note that instances of this behaviour were greatly reduced during this review, with firms conducting full investigation assessments prior to making a decision. However, we continue to see a small number of firms' decisions still being predicated on the warning provided, or whether the customer chose the correct payment category to display a warning, as a reason to decline reimbursement. There is also a risk that, with the provision of more directional and targeted warnings, these could again be used in isolation as justification for declining reimbursement. We would remind all firms to ensure relevant discussions are held with customers around the full circumstances of the claim, including whether the customer acted upon the warnings, and fully consider why the warnings may not have had the required impact.

Within a number of firms, we identified that thresholds had been introduced which resulted in customers being automatically reimbursed if their claim was below a certain amount. The threshold differed between firms. The Code does not make mention of specific thresholds in the assessment of claims and it is expected that these are dealt with on a case-by-case basis.

The Code requires that all customers are reimbursed, unless any of the exceptions apply, and whilst we would not wish to discourage firms from providing reimbursement to customers, the use of a threshold to reimburse without assessment should not be based on resource constraints or for commercial reasons. Importantly, where customers do receive reimbursement without assessment, they should also be provided with clear information as to how this may impact any future scam claims, and with aftercare and education on how to avoid scams, and any additional support, particularly if any vulnerability to the scam or the subsequent impact is apparent.

Claim decision

Since our review of reimbursement provisions in 2021, firms have implemented more defined processes for informing customers of the reimbursement claim decision, with most firms attempting to contact customers by telephone to discuss the outcome of their claim. These discussions should provide an opportunity for firms to explain the process that has been undertaken, the decision reached and also to provide additional education on how customers can avoid scams in the future.

However, despite these improvements, we found in a number of firms that staff were still not providing a clear rationale to customers on the outcome of their claim, whether this be full, partial or no reimbursement. This also included a lack of documented rationale for claim decisions within letters, as detailed further below.

Whilst there is, within some firms, still more work to be completed, it is acknowledged that given the change programmes and enhanced training completed, there is a need for these improvements to embed fully and for this to become a business-as-usual approach.

Customer claim communications

Following a reimbursement decision being made, customers will receive a final outcome letter, which should be designed to provide an appropriate level of information to enable the customer to understand the rationale for the decision which has been made. This is also a further opportunity to provide other important information, such as confirming the customer's right to complain, and useful links and tips on how to avoid falling victim to a scam in the future.

Across the signatory firms, we found that most were using some form of templated letter which did not reflect the rationale or information that had been considered in relation to individual cases. Often the letters included a list of checks which had not been deemed sufficient by the firm, generic details on the Code or mention of customers not meeting their requisite level/standard of care, as mentioned earlier. Further work is therefore required to ensure communications with customers following a claim decision are provided in line with the Code.

Areas for improvement:

- Firms should reassess the basis for recording and providing decision rationale, to ensure it provides adequate justification for reaching a decision on a reimbursement claim.
- Firms must reassess decision letters issued to customers to ensure they provide all required information including a full and relevant rationale for the decision reached.
- Claim investigators must be able to access full details regarding the circumstances of the claim, including further contact with the customer where gaps in information are apparent.
- Firms should ensure that customers are aware of the process for determining and assessing the reimbursement claim under the CRM Code, avoiding where possible the use of jargon, and providing customers with easily accessible means to submit any supporting evidence or information which may help their claim investigation.

- When considering whether a customer should be reimbursed, firms should ensure the assessment is made taking fully into account the explanation of why the customer believed the payment to be genuine, not based on arbitrary checks which have or have not been conducted by the customer. The decision assessment should also take into account all of the circumstances of the scam and characteristics of the customer, and that it is for to the firm to determine if any of the exceptions apply, not for the customer to prove otherwise.

Areas where firms have demonstrated improvement:

- Good quality conversations held with customers, including the use of empathy, open questions, and probing, resulted in firms being able to obtain all details of what had happened, the nature of the scam and to understand how this had impacted the customer. By relaying the information back to the customer to ensure nothing was missed, this helped the firm to make a considered decision with regards to reimbursement.
- Where we saw application of the Code working well, this tended to be where clear records and notes around the circumstances of the scam were available, and that customers were contacted to update any information gaps.
- Firms are now making attempts to contact the customer to explain the reimbursement decision and whether any funds can be repatriated from the receiving firm. Whilst there is more to be done in explaining the rationale, within some firms, there is an improvement on what we have identified in previous reviews.

2.6 Customers Vulnerable to APP Scams

Our previous thematic reviews have highlighted a need for firms to improve their identification of customers vulnerable to the scams as well as ensuring that customer vulnerability is considered within the reimbursement assessment.

Identifying vulnerable customers

There have been some improvements since our previous reviews in the identification of customer vulnerability to a scam and the reimbursement process, as well as consideration of how this can be accounted for in other parts of the payment journey. However, we remain concerned that this is not consistently achieved across the industry, with staff still missing obvious triggers or signs that the customer was vulnerable to the scam. This became apparent from the manner in which discussions were held, and whilst conversations were much more open and detailed, staff still did not probe further when customers declared a clear vulnerability to the scam which resulted in the scam succeeding.

As mentioned earlier, firms should clearly explain to customers the process of assessing claims and this presents a good opportunity for firms to encourage customers to disclose any information regarding their circumstances that would be likely to have made the customer more vulnerable to the scam. Whilst this may not mean explicitly asking if there is any vulnerability, open questioning should allow staff to draw out this information.

The identified lack of additional probing or reaction to clear identifiers of vulnerability often resulted in customers having to undergo elongated discussions and claim investigations when these could have been resolved much quicker and reimbursement provided sooner. On occasion, notes clearly identified that the customer was vulnerable to the scam and subsequently fully reimbursed but without any acknowledgement or reduction in timescales for resolution.

In a small number of firms, the identification of vulnerability has sometimes resulted in customers being offered additional support wider than just related to the scam. This would include referral to internal support teams or signposting to external sources of help and advice.

Support for vulnerable customers

Firms have developed more bespoke vulnerability training for customer facing staff in relation to scams, which sometimes allowed for a better standard of conversation during claims. However, we are of the view that vulnerability training could be improved for non-customer facing roles, including within receiving firm and operational oversight roles relating to the Code. This training requires focus on the nuances of the Code relating to vulnerability as per section R2(3), but still with a consideration of wider aspects of customer vulnerability, how this may impact customers and also any additional support required post the scam occurring.

Typically, where vulnerability was relevant to the scam, customers were reimbursed. However, at times the customer had to wait for a considerable period of time before funds were credited to their account. This was partially due to high claim volumes at the time, or firms waiting for a response from the receiving firm before providing reimbursement. We would re-iterate that there should be no unnecessary delays to customers being reimbursed in line with the Code requirements, particularly where they have been identified as being vulnerable to the scam.

Where such customers were reimbursed, this sometimes resulted in less information being requested regarding the circumstances of the scam, and at times resulted in opportunities being missed to provide meaningful aftercare. The Code requires that firms complete a full assessment of the customer's circumstances which resulted in the scam taking place, together with an understanding of the detail of the scam itself. Where firms do not obtain this

information sufficiently, due for example to an early decision to reimburse based on vulnerability, they are unable to then provide the customer with impactful education and aftercare as required under the Code, leaving such customers potentially susceptible to future scams.

Areas for improvement:

- Firms must reassess their ability to identify vulnerability triggers, and to probe vulnerability to the scam skilfully, with better explanation of the claims process, to allow for better interactions with customers, and lower the risk of potential vulnerability being missed.
- Where vulnerable customers are reimbursed in line with the Code, firms must ensure reimbursement is actioned without any unnecessary delay.
- Firms should consider their approach to providing future support or signposting to customers recorded as vulnerable as a result of a scam, considering how this flag is raised and how this links into support in other interactions the customer may have with the firm.

Areas where firms have demonstrated improvement:

- Firms were able to demonstrate more specific training on customer vulnerability specifically relating to APP scams. This will lead to staff better able to identify and support vulnerable customers.
- Where we found discussions with vulnerable customers working well, firms were considering the customer's personal circumstances at the time of the scam, and how this may have impacted the customer proceeding with the payment.

2.7 Claims timeline and complaints

We assessed how firms manage the claims journey timelines, and how they assess whether they are meeting timings when reviewing caseloads. Our assessment had particular focus on the time taken to assess claims, the time taken to reimburse customers where the decision is made to do so, and whether firms communicate delays to customers in line with the Code.

We also assessed firms' complaints handling processes and customer communications in relation to Code related complaints.

Claims timeline

Where delays to claim investigations mean cases will extend beyond the required 15 business days, firms are expected to issue a communication to customers, informing them of the delay, the reason for it, when to anticipate a response and to confirm the customer's right to make a complaint to both the sending and receiving firm as a result of the delay. The same applies

to cases extending beyond 35 business days, however cases should only take this long to resolve in exceptional circumstances.
We found that, while all firms have a process in place to provide customers with communications where claims extend beyond 15 business days, the content of these typically did not include any bespoke details relating to the reason for the delay, and we found that some firms were not providing the complaint details as required under the Code.

We also found more instances, across a larger spectrum of firms, than we would have expected of case investigations moving beyond 35 business days, which would lead to a breach of the Code.[2] Where cases had gone beyond 35 business days, the main reason for this, suggested by firms, included resource challenges due to a rise in the number of scams being reported, together with implementation of process changes and/or related training needing to be fully embedded.

These delays were often exacerbated due to a lack of response from the receiving firm, especially where such a firm was not a signatory to the Code. We would like to remind firms that they should not unduly delay providing a reimbursement decision to customers due to awaiting a response from the receiving firm, although we acknowledge that in some, more complex cases, this may be required.

Complaint handling

Across most firms, we were able to evidence that complaint handling assessments typically involved reassessment of the customer claim. In isolated cases where this was not happening, we have raised as our concern with the individual firms. On these occasions, the complaint handling process was focussed more towards ensuring the procedures had been followed rather than if the case had been managed in line with the requirements of the Code and whether the customer outcome was deemed correct or fair. Overall, we found that complaint handling processes have been designed in line with required DISP rule requirements. It is worth noting that we did not investigate any complaint cases in detail and did not review any assessments that have subsequently been referred to the Financial Ombudsman Service.

We noted that some firms are making better use of root cause analysis, which was an area developed within the Governance and Oversight section of the Code, put in place since our previous thematic review. We saw examples in some firms where stronger feedback loops to governance, MI and fraud operation teams had been created in order to discuss complaints cases and how internal processes could be improved as a result of complaints received. However, this was not the case in all firms within the scope of the review and we would therefore encourage all firms to utilise the tools available to consider root cause analysis fully

[2] Monthly reporting to the LSB of cases exceeding 35 business days including internal remediation plans is completed by all signatory firms.

in order to identify any trends, or enhancements to existing process, that may be required to strengthen the customer journey and achieve the required outcomes.

Areas for improvement:

- Firms should review the communications issued to customers at 15 and/or 35 business days to ensure all information required under the Code is relayed to customers.
- Where firms have a significant number of cases extending beyond 15 and 35 business days, they should ensure they have sufficient monitoring and improvement plans in place to resolve the recurring breach.
- Firms should ensure they are fully considering root cause analysis when assessing adherence to the Code, which also aligns to the Governance and Oversight requirements that were introduced in June 2021.

Areas where firms have demonstrated improvement:

- We found that customer outcomes, and identification of potential enhancements to processes to be made, work well where there was a close working relationship between teams involved in APP scam claim investigations and the complaints teams.
- Customers are being better informed generally around how to make a complaint to the sending and receiving firm, with this not only being highlighted within decision letters, but also in some cases verbally during the decision or investigation discussions.

3. Conclusions and next steps

This 2022 review of firms' adherence to the Contingent Reimbursement Model Code for Authorised Push Payment Scams was intended to take into account the outcomes of our previous thematic review work carried out between 2019 and 2021 and allow us to validate any previously agreed actions within signatory firms, whilst also considering the whole customer payment journey.

This review was very detailed by its nature in covering the whole payment journey. Our oversight process involved a number of requests for information, detailed data, and engagement from firms to enable the review to progress. We would like to thank all those involved in this process for the assistance provided to the LSB's Compliance Team in enabling us to conduct our work.

Our view is that, overall, firms have put in place detailed programmes of work, as a result of our previous thematic reviews, with the aim of addressing the issues we had identified. We have found that this has led to progress being made across a number of firms to drive improved adherence to the Code. Areas showing improvement include implementation and ongoing review of effective warnings, including in some instances more tailored and dynamic warnings; enhanced transaction monitoring prior to payments being initiated; and detailed and focussed conversations with customers to understand the complexity of the scam and customer circumstances.

However, there is not a consistent picture across all firms, with there still being further work required in some areas by all firms to ensure all aspects of the Code are consistently applied to ensure fair customer outcomes are achieved.

We believe that a number of the issues raised during this review are due to a need for the changes to policy, procedure, and staff training to embed further and become a business-as-usual approach within firms. In addition, there is a need for regular, robust, and independent three lines of defence oversight across some firms to gain adequate assurance that the Code is being applied consistently and fair outcomes are being achieved, and that such oversight is not just focussed on internal processes being followed.

It is acknowledged that firms have faced a number of challenges over the last 12 months, and continue to do so, particularly with regards to resourcing and the impact of external factors. However, at the time of our review, some of the practices seen within firms continued to result in a risk of unfair customer outcomes and the potential for customer detriment. It is now imperative that firms consolidate the changes they have made to processes and are able to clearly demonstrate that adequate prevention and detection measures are in place to help stop scams from occurring and protect customers from financial harm.

Where a scam does occur, customers should be reimbursed unless the firm is able to establish that any of the Code exceptions apply. We would reiterate that this is the responsibility of the firm and not the customer to prove otherwise, as customers are not bound by the Code. Firms should bear in mind that staff have the benefit of training, handle cases on a regular basis and have knowledge of various types of scams and how these are perpetrated. Customers do not generally share this knowledge and we would not expect this to be a consideration when assessing scam claims nor applied as a bar or standard that customers must meet in order to be reimbursed.

Next steps

All firms have now received their individual review reports, together with any associated actions raised by the LSB. We will continue to work with signatory firms to ensure actions are remediated to drive consistent application of the Code across the industry.

Whilst this report is focused on the outputs of our review work, we continue to progress other workstreams related to the CRM Code, including the implementation of the recommendations from our review of the CRM Code for Authorised Push Payment (APP) scams conducted in 2020/21 and our 2021 Call for Input to ensure that the Code continues to evolve and provide increased protections for customers.

Key work streams for the LSB include our work with industry and stakeholders to formalise success measures for the Code; the review of the balance of responsibilities between sending and receiving firms within the Code; revisions to the guidance based on the evidence gathered from our reviews; and engagement with the Payment Systems Regulator (PSR) as it sets out its next steps in relation to APP scams.

We will maintain our focus on APP scams and engagement with signatory firms, key stakeholders and regulators to ensure that protections provided by the CRM Code are working effectively to provide good outcomes for customers.