Lending Standards Board

Contingent Reimbursement Model Code for Authorised Push Payment Scams

Review of approach to reimbursement of customers – provision R2(1) (c)

Summary Report

April 2020

Contents

Introduction

The Contingent Reimbursement Model Code (CRM Code), launched on 28 May 2019, provides important protections for consumers where they fall victim to authorised push payment (APP) scams, with eight payment service providers (PSP) signed up from this date. The voluntary code was developed by the APP Steering Group and is aimed at reducing the occurrence of APP scams, and the impact that these crimes have on consumers, micro-enterprises and small charities. A separate consumer facing document was published to promote awareness of the Code, informing consumers of the various ways in which they can reasonably protect themselves from falling victim to an APP scam.

On 1 July 2019, the Lending Standards Board (LSB) became the official governing body for the Code, with responsibility for oversight of its implementation and ongoing adherence by the industry. The role of the governing body is to ensure the Code is adhered to and remains effective in preventing and protecting customers from APP scams.

The LSB committed to undertake a thematic review of provision R2(1) (c), as detailed below, within the first year of the Code being launched. The timescales for the review were agreed at the Steering Group, with the review set to take place from October 2019 to allow enough time for PSPs to have embedded and operationalise the Code.

The Code requires that where a customer has been the victim of an APP scam, Firms should reimburse the customer. Provision R2(1) (c) sets out that if the customer has not met a reasonable level of care when making a payment, reimbursement can be denied. However, Firms must be able to demonstrate that in all the circumstances at the time of the payment, in particular the characteristics of the customer and the complexity and sophistication of the APP scam, the customer made the payment without a reasonable basis for believing that:

- the payee was the person the customer was expecting to pay;
- the payment was for genuine goods or services; and/or
- the person or business with whom they transacted was legitimate.

1. Executive Summary

Background

All Firms signed up to the Contingent Reimbursement Model Code (CRM Code) at point of inception in May 2019 were included within this review. To allow time for the requirements of the Code to be operationalised, the review took place between October 2019 and January 2020. LSB acknowledges that within all Firms visited, there continues to be an element of embedding processes and operations, and an ongoing cycle of review and learn.

1.1 Key Findings

Overall, we found that all Firms have taken positive steps to implement the requirements of the Code for reimbursing customers, whilst showing a willingness to work through a continually improving process to ensure a correct approach. It was evident that Firms were keen to participate in the review, as this has been an opportunity for an early stage post-implementation assessment. During the review, management and staff were very open and transparent in confirming areas where they are aware further work is required to fully embed the Code. This enabled us to hold challenging conversations with Firms around the key findings from the review, but also on areas of perceived good practice and where to avoid poor practice.

It was encouraging that Firms had broadly formalised their approach to reimbursing customers who fall victim to scams in documented policies and processes, and many had completed quite extensive training on APP scams to the staff involved. Further, it has become clear that Firms are moving towards having full quality assurance measures in place, and towards full 2nd and 3rd line of defence involvement. Work continues to develop better ways of providing effective warnings and we did see good examples of aftercare being provided to customers who had fallen victim to APP scams. We saw many examples of agents speaking with customers in an empathetic manner, displaying a genuine wish to help.

However, we did see several examples where the customer outcome was not as we would have expected. We reviewed individual cases within our sample to understand how the decision to reimburse, or decline reimbursement, was reached and recorded.

We found that the key areas for improvement fell within four areas:

- **Reimbursement -** Judgements about reimbursement were not always made in the light of the full circumstances of the case or a judgement of what consumers may have believed at the time, but were often driven by narrower process considerations. The presumption in the Code that victims should be reimbursed unless there is a clear ground for attributing blame to the consumer was sometimes reversed so that the customer was held liable in many cases where the bank was not.

- **Effective warnings -** The issuing of a warning was sometimes treated as a strict liability regardless of how effective the warning was or whether the customer had a reasonable ground for not acting on the warning. Warnings themselves varied in the extent to which they engaged customer attention and in their level of specificity and were typically not available on all channels. (We expect to make the effectiveness of warnings the subject of a separate review in 2020/21).

- **Customer vulnerability -** The identification of vulnerability and customers' susceptibility to scams was not very well developed. Questioning of customers who reported falling victim to a scam was often closed and did not allow for the clear identification of any vulnerability. In a small number of cases, evidence of vulnerability was available, but was not always used as a consideration for reimbursement.

- **Record keeping -** Documentation of the rationale for the decision to decline reimbursement varied across Firms and at some was non-existent. Customers themselves were often not informed of how a decision had been taken to deny reimbursement and were often given no opportunity to address the grounds on which the firm was holding them liable for the success of the scam. Customers offered evidence of the scam operation and the checks they had completed but often this evidence was not taken.

Further detail with regard to key areas of concern is contained with the following sections. However it is clear in our view, from the reviews undertaken, that the highlighted areas of concern are of the highest risk to Firms of non-adherence of the Code, and therefore the areas likely to be the largest barriers to good customer outcomes.

Areas for improvement and good practice

While completing our reviews, we identified a number of examples of good practice as well as areas requiring improvement from Firms. Where possible, we have tried to include these points in the relevant section of the detailed report.

The LSB will continue to work with Firms to ensure the provisions of the Contingent Reimbursement Model Code are fully embedded. This will provide a consistent approach for customers in being reimbursed when they have been the victim of an APP scam, taking into account the circumstances of the individual and the scam.

1.2 Objectives and Scope

The objective of this review was to understand: how Firms have interpreted and applied the requirements of the Code for reimbursing customers; its effectiveness in delivering fair outcomes for consumers; and consistency of approach across signatory firms having regard to the circumstances of the individual and the scam.

The review included an assessment of the key controls and processes Firms have in place to demonstrate compliance with the provision and encompassed the following areas:

- How Firms have interpreted and defined the requirements of provision R2(1) (c) and the extent to which this is consistent across the industry;
- The policies and processes Firms have in place to assess claims under the Code, and consider how the requirements around reasonable level of care are applied in the assessment of customer liability;
- The level and depth of staff training in place across all relevant teams, to support the provision of customer liability assessments and the interpretation of reasonable level of care;
- The effective warnings Firms have in place to safeguard the customer from falling victim to a scam;
- When considering the characteristics of the customer in an assessment of an APP claim, the processes Firms have in place to identify customers vulnerable to APP scams, including triggers and methods of identification and the extent to which this impedes the customer's ability to protect themselves from falling victim to the scam;
- Where a Firm's investigation into a claim determines the customer has not met a reasonable level of care, the after-care support provided to customers to prevent the customer from falling victim to APP scams in the future;
- The governance, oversight and controls in place to ensure there is adequate visibility and accountability for decisions, and the dissemination of key management information to deliver fair and, where appropriate, consistent outcomes for victims of APP scams;
- The level and depth of oversight Firms have in place to assess the effectiveness of the policies, processes and controls in place, in relation to provision R2(1) (c).

We also assessed the application of the provision across a representative sample of APP claims at each Firm. This was to understand the considerations that are made by Firms when assessing customer liability under the Code, having regard to the circumstances of the scam and the individual.

The review was conducted across the eight Payment Service Providers (PSPs) that signed up to the Code from 28 May 2019. The review did not encroach on the jurisdiction of the Financial Ombudsman Service (FOS).

Out of Scope

The review scope did not include a detailed assessment of any other provision within the CRM Code, although as highlighted above, consideration and a degree of understanding was required on other areas of the Code in order to allow for conclusions to be made in relation to the objectives of the review.

The processes and approach within the 'receiving bank' regarding these scams were not reviewed.

1.3 Methodology and Approach

A detailed information request was required from all participants in this review, to allow for an initial desktop assessment of how Firms have interpreted and implemented the requirements of the Code.

The onsite review then tested the design and operational effectiveness of Firms' policies and processes. As part of this assessment, the LSB reviewed a sample of cases across a broad spectrum of APP scams, where the Firm's investigation into a claim concludes that the customer has:

- met the reasonable level of care expected of them; or
- not met the reasonable level of care expected of them.

Where the Firm's assessment has concluded that the customer has not met the reasonable level of care expected of them, the LSB also reviewed a range of cases where the customer has:

- accepted the decision; or
- disputes the decision, which has resulted in a complaint, but the customer has not escalated their complaint to the FOS.[1]

Structured discussions with a population of relevant staff members involved in the investigation of claims and customer liability assessments, across all relevant channels, were designed to support the information gathered during the desktop assessment. The aim of these discussions was to test staff understanding of the Firm's policies, processes and training and the application of this knowledge when considering cases under the Code.

With regard to the approach, the review was conducted across a number of key stages set out as follows:

- The LSB consulted with UK Finance and the eight PSPs that are signed up to the Code through a roundtable discussion. The purpose of this meeting was to run through the terms of reference, set out the LSB's approach to undertaking the review and provide PSPs with an opportunity to feedback, ask questions or seek clarification.
- To make the process as efficient as possible, the LSB asked Firms to complete a request for information. This was to provide the LSB with an overview of key processes, including the availability of supporting information and documentation to support its assessment.
- The LSB completed a desktop review of the information received, followed up with an onsite visit to meet with key representatives from the relevant business areas to understand how, following the launch of the Code, the policies, procedures and training in respect of the scope of the review have been implemented.
- Following the on-site meeting, the LSB held a close out meeting with each Firm to discuss the initial findings from the review. This was followed up with a further request for information where the LSB considered this necessary to its assessment.
- An individual report, setting out the LSB's findings from the assessment, has been issued to each Firm, including any required actions which will be tracked through to completion.

[1] The purpose of this review is to assess Firms' interpretation of provision R2 (1) (c) and the practical implementation of this in customer claims under the Code. The LSB will not opine on the outcome of individual customer claims.

2. Detailed report

This section of the report breaks down each area assessed within the scope of this review. Our assessments were made by paying attention to how each area contributed to ensuring an aligned and consistent approach across Firms. Our sample testing was an opportunity to assess whether this subsequently led to fair outcomes for customers who had fallen victim to APP scams.

2.1. Governance, controls and oversight

The CRM Code is clearly visible and has been brought to the attention of executives, with each Firm providing a detailed breakdown of reporting lines and committees engaged to ensure the requirements of the Code, and decisions on policy, are made at a senior level.

Whilst we saw good visibility through Firms' governance structures, we did not always see evidence of sufficient 2nd line compliance and 3rd line audit oversight. In some cases, the end to end process is managed within fraud operations, with little engagement evident across the 2nd and 3rd line from a governance perspective. Firms are beginning to identify and develop controls for CRM to mitigate any associated risks, however this is still a work in progress.

Areas for improvement:

- Firms should ensure that oversight arrangements for the CRM Code are fully implemented as soon as possible;
- Oversight programmes should include a focus on record keeping and decision rationale;
- Cases that had been escalated for management review, and as a result had produced a different customer outcome, were not always updated on reporting systems. Scam case and decision reporting needs to be accurate, to provide a clear view of customer outcomes and also to ensure there is clear visibility for senior management on the performance of operational teams and the effectiveness of the Code.

Examples of good practice:

- Some Firms have ensured operational responsibility for the Code sat at an appropriate level, with CRM discussion forming part of key Senior Management Committees;
- Firms were completing regular test and learn sessions, whereby agents and supervisors can calibrate decisions made and escalate cases where necessary. Where this occurred, we saw clear signs that, over time, agents were upskilling;
- Firms that had implemented a case escalation route allowed for disputed case decisions to be reviewed in a timely manner and potentially overturned, enabling reimbursement to be provided.

2.2 Policy and process

Firms approached the implementation of policies and processes at different times up until the launch of the CRM Code in May 2019. At this point, all Firms had either in place, or began putting in place, the necessary structure to fulfil the requirements of the Code. In most Firms, the responsibility for operationalising the Code requirements rested with the Fraud operations teams. We do acknowledge a considerable amount of work has been undertaken in developing the necessary policies and processes, however some Firms still have additional work to complete in this space.

Where available, Firms shared the detailed policy and process documents including confirmation around how these were being implemented, updated and embedded within the operational teams.

It was apparent that at some Firms, there had not been any review or testing of the policies and processes, nor had they been updated as operations developed. However, these Firms did indicate that they intend to complete a more thorough investigation regarding their effectiveness following our thematic review.

We found that some Firms were trying to strike a balance between reviewing each scam case individually and adopting a scorecard or system-driven process to determine liability. While we appreciate individual assessment of each case takes time and resource, we found that cases where a scorecard was used were typically much more focussed on completing a process, which often resulted in an outcome which was not in the customer's favour. Typically, such cases had insufficient rationale to evidence why the customer was not felt to have shown a reasonable level of care or why they were being held liable.

Likewise, we found that many processes provided staff at the first point of contact with the ability to determine the liability decision. Whilst this can be the quickest and sometimes most efficient manner in which to deal with customers to ensure they are reimbursed as soon as possible, our evidence showed that upon review by an investigator, there was often no further challenge or attempt to contact the customer for further information. As a result, we found some cases where the focus was on following process rather than establishing full facts.

Areas for improvement:

- In some cases, processes were leveraged off the back of existing fraud processes, which in general are designed to deal with card and other types of first party fraud. In addition, in most cases, the staff dealing with APP scams were those with previous experience of dealing with fraud. While there is logic in making use of teams already engaged in this type of work, we felt in some Firms that they approached the management of APP scams and fraud cases in a similar manner. This, at times, resulted in Firms seeking to apportion blame in all cases. Firms should ensure there is a clear difference in the management of fraud and scams cases, specifically in implementing the requirements of the CRM Code;
- We saw evidence where a firm was heavily reliant on a checklist process for apportioning blame, resulting in claims being declined without being fully considered. Declining a customer claim without due consideration and rationale around whether the customer had met a reasonable level of care would result in non-adherence with the Code;
- We saw examples where there was an over-reliance on the process when it came to assessing reimbursement which led to 'customer to blame' decisions being reached before the customer was given the opportunity to fully explain the circumstances of the scam.

Example of good practice:

- Cases where the customer is held completely or partially liable are referred to a team leader for a further check prior to the decision being recorded. Where this occurred, we evidenced that customers were more likely to receive a fair outcome.

2.3 Training and support

In order to prepare for the launch of the Code, Firms arranged for training to be delivered to key staff across the organisation. As expected, there were different approaches across Firms, with some favouring detailed training packs with supporting materials, some allowing for distance learning with training packs and case studies issued, while others arranged detailed and formalised classroom training session.

Primarily the focus of training was based on three main topics: the detail and purpose of the CRM Code; the Firm-specific processes for dealing with scams; and material regarding the types of scams likely to be encountered.

Typically, the training was followed up by discussions with team leaders, where further support was offered and questions answered.

While we saw some good material being used to assist staff in preparing for the launch of the CRM Code, it was apparent that training tended to be limited to those staff directly involved in the process, such as first point-of-contact scam teams and investigators. Most Firms did not provide detailed training within, for example, branches and telephone banking channels but limited this to scam awareness training. In addition, while some Firms extended detailed training to other key departments, for example complaints teams, this was not consistent across all Firms.

We did see that Firms were looking to ensure staff dealing with APP cases received ongoing support. A number do utilise staff who have extensive experience in dealing with scam queries, allowing them to share their knowledge with less experienced team members.

We would urge Firms to consider developing their training and support, as the skills of staff are key to ensuring compliance with the Code.

Areas for improvement:

- It was not always clear that all staff who are impacted by the Code had received training. For example, we saw instances where the complaints team had not been fully trained on the expectations of the Code;
- There were examples where more formalised training was required. While we appreciate some Firms are using experienced staff to deal with these claims, a structured training plan, considering the needs of all staff involved, can help ensure the training is embedded;
- Firms should consider whether the training programme they have in place is offering protection to customers across all channels, including transfers made in branch and through telephone banking;
- Once a training framework has embedded, Firms should ensure there is a clear plan for reviewing the materials and providing refresher training.

Examples of good practice:

- Completion of a full training needs analysis ahead of the implementation of the Code, with a differentiated approach based of the experience of staff, assisted in implementation of the Code across various workstreams;
- The use of regular discussion sessions/forums within the scam teams resulted in informal upskilling of staff through discussion of cases and the outcomes.

2.4 Effective warnings

We are aware that there is continued development taking place regarding effective warnings across all channels. Firms are aiming to develop more tailored and dynamic warnings and the LSB will undertake a review of the effectiveness of warnings at a later date.

For this review, we have looked at the extent to which Firms used the warnings when considering whether customers met a reasonable level of care and took heed of the warnings rather than the effectiveness of the warnings themselves. Firms did provide us with details of the various warnings used, both online and verbally, however we often found that it was difficult to view the evidence of what had been displayed or said to the customer.

There were two distinct issues around effective warnings:

1) Whether the warning was effective in capturing the customer's attention and relevant to the transaction completed.
2) Whether, despite the warning, the customer had a reasonable basis for proceeding with the transaction.

We saw a few examples where a Firm acknowledged that the warnings are not fully in place and therefore would hold themselves partially liable for the success of the scam. Conversely, there were examples of Firms using the warning as automatic evidence of customer liability, holding the customer liable in any case where a warning was given, regardless of its effectiveness. In assessing whether reasonable care has been taken, Firms should consider all aspects of the case and not rely purely on the warning as a measure of liability.

We identified some variations in terms of threshold limit amounts, below which no effective warning is given, leading to a lack of protection for victims of lower value fraud. This naturally leads to inconsistency in customers receiving warning messages which in turn may result in unfair customer outcomes.

Within the branch and telephony channels it was not always clear if or when a warning had been given as there are weaknesses in recording of this information. This in turn caused difficulties when investigating a claim in understanding whether the customer had understood or taken heed of a warning.

From our review of cases, it became clear that customers themselves were not sure they understood the context of these warnings, with some saying they either did not register the warnings or the importance of them and simply thought they were just a routine (and unimportant) part of the transaction process. Indeed, we did not see many instances where a customer appreciated the detail of a warning or were able to relay what the warning said.

Moreover, we saw cases where, even when a customer had considered the warning, the type of scam led to the customer being engineered into ignoring it, or the customer still had reasonable grounds for believing the payment to be genuine.

Areas for improvement:

- Firms should consider how they can evidence or record which warning has been provided and whether it was the most appropriate in terms of content and timing;
- A warning should not be used as a strict measure of liability, declining reimbursement to customers. All circumstances in relation to the scam should be considered;

- Warnings provided when a customer transacts through branches or telephone banking should be clearly defined and documented to assist with any potential future investigations;
- Firms need to better evaluate how customers are interacting with the warnings and whether customers are pausing in response to warnings;
- Firms should develop an understanding of why customers did not heed a warning that appears effective.

Example of good practice:

- Firms are constantly evolving their thinking on warnings and how to maximise their effectiveness.

2.5 Approach to reimbursement and the application of provision R2(1) (c) – Reasonable basis for belief

The key focus of this review was to understand how Firms are approaching claims and assessing whether customers had a reasonable basis for believing the payment and beneficiary were genuine. As mentioned previously, the CRM Code requires that customers are reimbursed if they are the victim of a scam unless the Firm can establish that customers made the payment without a reasonable basis for belief.

Most claims were processed via telephone through a centralised team, even if the initial notification was made through a different channel, such as a branch. This initial call was often used to take the details of the payee, amount of payment and background details as to what had occurred and why the customer thought they had been scammed. The detail obtained was used as the basis for determining whether customers had a 'reasonable basis for belief' and the subsequent outcome from a liability perspective.

At this point, we rarely heard any Firms explain that the claim would be assessed under the requirements of the Code and, in some instances, customers were left with the impression that it was more of an administrative process for them to receive their money back.

Upon completion of this initial call, cases are typically passed to an Investigations Team to determine whether the customer would be reimbursed. From our testing, we found very few cases where the investigator contacted customers for additional information, instead relying on that which was obtained on the initial call. In fact, in some cases, it was very difficult to confirm from the records kept what activity an investigator had undertaken. Firms need to take care they do not place an over-reliance on initial calls, as at this point customers can be most concerned, distressed and unable to think clearly.

When assessing claims, we found that this often resulted in a Firm determining they had met their responsibilities, with the same response being received from the receiving Firm. Therefore, they reasoned that the customer must be liable and no reimbursement was provided, rather than considering what steps the customer had taken and that this was a case of no blame across all parties. We felt that across a number of Firms, the assessments were conducted on the basis of finding blame at some point in the payment journey, rather than reviewing the circumstances of the case and the scam to understand the rationale for customers making the payment.

There was also a very broad range of consideration around what is deemed to be 'reasonable steps' completed by a customer. We found a number of cases during our review where it appeared the customer had completed sufficient diligence, or been convinced to such an extent by the scammer, to

provide confidence that the recipient and purpose were legitimate and so proceeded to complete the payment. There was often a high expectation around the level of knowledge or number of checks a customer should have conducted before proceeding. This led to inconsistencies in decisioning and raises concern around whether customers are receiving a fair outcome in such circumstances. The inconsistency was not only between Firms but sometimes by case to case in the same Firm.

Our concerns around unfair customer outcomes is also driven by several cases reviewed where claims were rejected but it was not clear why the customer was deemed to have not taken a reasonable level of care. Our testing involved listening to calls, where available, and a review of case file notes. The level of record keeping was poor across a number of Firms: rationale for decisions was sometimes missing; there was no record of the type of warning provided, especially where this was used as the basis for rejection of a claim; and there was often no mention of assessing claims against the requirements of the Code.

This meant that customers were given little opportunity to address the grounds under which they were being held liable, and instead they were often left with the outcome that the Firm had tried to recover the funds but, as none remained, there was nothing further to be done.

It is worth noting that a number of the cases we assessed under the scope of this review were received soon after the CRM Code came into effect. Since then, various governance, controls and processes have developed further, and some improvements were seen in cases handled more recently.

Areas for improvement:

- Customers should be informed about how the firm would be making the assessment for liability under the Code when considering reimbursement, giving them the opportunity to expand on the circumstances and detail of the scam or the level of checks and diligence undertaken;
- Firms need to be realistic in their expectations of what constitutes 'reasonable' when understanding the level of checks, diligence and any element of social engineering which has occurred given the circumstances of the scam and the customer. There is a risk of non-adherence to the Code and poor customer outcomes if expectations are set too high;
- As stated previously, the provision of a warning should not be used as a strict basis for denying reimbursement, which would not be in compliance with the Code;
- Good record keeping, detailing the rationale for the decision reached, is particularly important especially in those cases where decisions were made following the initial call or further investigation is not deemed necessary;
- Discussions with customers should not be process-led but determined by the customer's circumstances. A 'scorecard' or system-driven approach used for assessing liability should ensure assessments take into consideration the circumstances of the customer and scam and do not follow a 'tick-box' approach ;
- Documenting of decisions and the quality of record keeping should be such as to enable a Firm to justify the decision reached when challenged. Justification of decisions around liability assessments and rationale for reimbursement, or decline, is a key part of being able to evidence compliance with the Code.

Examples of good practice:

- During testing we noted that the first point of contact teams, in all Firms, approached conversations with customers who are victims of scams in a very professional manner, displaying real empathy with the customer;

- During the course of the review, we assessed cases across a range of dates, from immediately after the Code came into effect through to the latter part of 2019. We saw that the processes within Firms and the skillset of the agents have improved during this time.

2.6 Vulnerability

Where a customer makes a claim after falling victim to a scam, Firms will routinely check their system and use some questioning to establish whether the customer has any vulnerability that would need to be considered. In many cases, the firm will start by looking for any existing vulnerability flags. We found that often questioning in this area was very closed which sometimes meant opportunities to identify any vulnerability were missed.

The Code states that where a customer is identified as vulnerable then they '*should be reimbursed notwithstanding the provisions in R2(1) (c)'.* Our review found that this requirement was not followed consistently. In some cases, we saw the customer being held liable even though they were recorded as being vulnerable. Typically, such cases contained notes stating that the Investigator did not believe that the vulnerability would prevent the customer from making payment, but without any rationale as to why. We acknowledge that not all customers with a previously known vulnerability will affect their susceptibility to being scammed, however if this is the basis for Firms not to reimburse, this needs to be clearly documented.

We saw examples where the firm did not consider potential vulnerabilities that became apparent both during the call and at the point of the scam. This included the customer circumstances at the time the scam took place which made them potentially vulnerable and more susceptible to the scam. Indeed, there were cases where the discussions clearly indicated the customer may have been more susceptible to the scam as a result of life events, current circumstances or potential vulnerability, but this information was not recorded, and consequently not fully considered within the investigation.

It is clear that staff have received generic training on dealing with customers in vulnerable situations, but it is felt that there is more to be done in this space due to the specifics of the Code.

Areas for improvement:

- Where a customer raises circumstances which were likely to impact on their ability to protect themselves from the scam, this information should either be passed on to the Investigator or considered within the assessment;
- Firms should review their vulnerability triggers to ensure customer circumstances are fully considered;
- Where a vulnerability is identified which impacted the customer's ability to protect themselves from the scam, they should be reimbursed, in accordance with the Code;
- Firms should review and update their vulnerable customer policy to ensure this is aligned to the requirements of the CRM Code.

Examples of good practice:

- The ability to spend time on the call with a vulnerable customer, taking care to ensure the customer's safety whilst explaining how to stop re-occurrence of scams, is to be encouraged. Where we evidenced this occurring, the calls were extremely well handled with professionalism maintained throughout;
- Following conclusion of the claim, customers would sometimes be handed across to more specialist teams with experience of dealing with customers in vulnerable circumstances. This

helped to provide additional support outside of the scam claims process, where it was deemed helpful.

2.7 Communications

In the majority of cases, customers were informed of the outcome of their claim by letter, although we did see evidence of the outcome being provided by text message.

The letters or text messages which were issued often did not offer explanation of the rationale for the decision reached or how claims had been assessed in line with the requirements of the Code. Text messages, by their very nature, would be difficult to include enough information for the customer to reasonably understand the rationale for the decision.

The lack of rationale and the way decisions are communicated to customers could have the effect of not allowing customers to challenge the decision, or provide further evidence. Indeed, it may deter customers from making a complaint.

Generally, we found the record keeping throughout the customer journey in relation to the scam claim could be improved.

Areas for improvement:

- Sufficient rationale within the documentation should be provided to clearly explain to a customer why the claim had been rejected;
- Communication after the 'first point of contact' call was often minimal. Investigators rarely contacted the customer for further information, even where the customer had offered evidence showing why they believed the transaction to be genuine. This led to Investigators completely relying on the information gathered from the first point of contact call;
- The information provided to customers should not be standardised, but bespoke to the customer. For example, the reason for rejecting a claim should be specific rather than generic and information provided to help the customer ensure they do not fall victim to the scam in the future should be tailored to the type of scam;
- Communication given to the customer should clearly inform the customer that the decision was based on the information provided by them, rather than focussed on the fact that the funds could not be retrieved from the beneficiary bank. The customer should be made aware of their options if they wished to challenge the outcome.

Example of good practice:

- Some Firms provided regular updates to customers regarding the status of their claim, outside of the Code-required timings. This was generally followed by a telephone call on completion of the claim, which customers seemed to find helpful.

2.8 Aftercare support

The final element of handling claims was in relation to aftercare. As mentioned earlier in this report, whilst the review was focussed on a specific element of the Code, other aspects were also linked into the claims journey.

Aftercare support included the provision of information through leaflets or via website links, designed to help customers learn more about scams, including useful advice around how they can avoid falling

victim in the future. All firms have dedicated resources within their websites relating to APP scams and how to avoid them, and customers were advised to visit these pages of their website. Customers were also consistently informed of the role of Action Fraud and encouraged to report the detail of the scam.

Whilst this information is very helpful, we found that Firms were providing mainly generic information resources rather than tailored aftercare support related to the specific scam the customer had fallen victim to. There was a heavy reliance on letters providing aftercare with little evidence of this being provided verbally during calls or as a follow up call to customers. However, we do appreciate that in some Firms, there are resource constraints and therefore education through letters is preferable to nothing at all.

Where we did see good examples of agents providing useful advice to customers, this tended to be those which were focussed on the specific type of scam involved in the claim. We found that where this level of care was provided, customers were more engaged.

Areas for improvement:

- Firms should consider when and how best to provide aftercare to customers who have been the victim of a scam. It is important to provide good quality support and advice, aimed both at preventing a scam taking place and supporting those who have been victim to a scam;
- Consideration should be given to ensuring customers are provided with information and the offer of support verbally wherever possible, as customers were noticeably more engaged where support was provided during a conversation. Where a discussion is not possible, Firms should review the closing letters to increase the prominence and relevance of support information;
- Record keeping of communications should be improved in order to provide a clear single end-to-end case file.

Examples of good practice:

- Where agents took the initiative to hold a meaningful discussion with customers around how to avoid the specific scam relating to the case, customers were appreciative and appeared more likely to take the advice on board;
- The leaflets and information sheets available from Firms are very useful to customers, and we have found further work being done to improve these communications. Whilst we acknowledge it is difficult to quantify how effective these are in preventing scams, the quality and ease of understanding of these documents provides benefit to customers.

3. Case Studies

The following case studies are based on claims we reviewed as part of our assessment and are taken from a cross section of Firms. The intention is to provide further insight into how the Code has impacted the handling of claims.

3.1 Reimbursement

Good practice

A customer met someone via a dating website, which developed into an online relationship. During the course of the relationship the scammer informed the customer he had to go overseas on business. He provided the customer with details of his business etc; which she checked via Companies House and the business appeared to exist. Whilst purportedly overseas, the scammer also alleged his account was frozen due to fraud, so over a period of 2-3 weeks the customer was scammed into transferring money for import/export duty. She informed him during their chats that she had recently lost her son and it would be the anniversary of his death soon. The scammer picked up on this and alleged his daughter was seriously ill and he just wanted to get back to visit her.

The advisor who took this call was very calm, empathetic and went through the details carefully and checked the customer was OK to talk. She also provided feedback on where and when the scammer appeared to have taken advantage of the customer through the various personal information she had disclosed. The claim was refunded in full due to circumstances of customer, the social engineering aspect and length of time the scam occurred over.

3.2 Effective warning

Improvement required

The customer had building work completed and was awaiting an invoice. An email was received asking for the outstanding payment. The customer double-checked the email which seemed to have come from the builder's correct email address and referenced payment made previously by cheque. The latest payment was made in a branch and a warning was read out. However, the customer proceeded with the payment as the warning focussed on 'care if you are not expecting to make this payment', which he was. The customer was held liable, as he proceeded with the payment despite staff reading out a warning statement, with the decision based on him not taking enough care and ensuring the payment was legitimate.

3.3 Record keeping and rationale

Improvement required

A small business customer runs a supply and distribution company, supplying machinery parts to blue-chip manufacturing companies. The Company was approached by what appeared to be large blue-chip organisation requesting them to supply a part. The part was sourced, and the customer requested payment up front from the client. This was initially declined as they stated the normal process is to pay on receipt, however they subsequently contacted the customer and requested they proceed with the order. The part was ordered but didn't arrive. The customer continued to engage with the third-party supplier, by telephone and email, to chase the part until the point they no longer responded to contact attempts.

At this point the customer's own internal IT department then conducted their own investigation and realised the same IP address was used for both the blue-chip company and supplier. This showed the whole order and supply was staged to scam customers out of funds. Despite the very complex nature of the scam, the customer was still held liable.

On numerous occasions the customer offered to share emails etc; but these were declined by the Investigator handling the case. The customer was not given any guidance or insight as to how the investigation process worked nor how the claim would be assessed against the requirements of the Code. The rationale was not recorded on the case file nor included in the decision letter when advising the customer they were being held liable.

3.4 Vulnerability and aftercare

Good Practice

An elderly customer had fallen victim to an impersonation scam. Upon contacting their Bank an agent talked through the circumstances of the case, to understand what had happened, whilst explaining at each stage how the scammers managed to get an advantage and obtain sensitive information about them. It transpired that the customer had completed a text message form purporting to be from TV Licencing and the agent talked them through how scammers do this to get information. The agent then went on to explain the various ways in which the customer could protect themselves in future, as well as warning them that it is likely that the customer could be targeted again, and explained they need to be vigilant.

Due to the circumstances of the claim and the vulnerable nature of the customer they were refunded in full.

4. Conclusions and next steps

This review was undertaken to understand how the requirements of section R2(1) (c) - Assessment of a customer's reasonable basis for belief - has been interpreted and implemented by Firms and understood by staff when considering APP scam claims. Our purpose was to ensure there was a consistency of approach across the industry and how this was impacting customer outcomes.

We have issued individual reports to each Firm which contain recommendations and required actions and will be working to ensure these are implemented, including tracking through to completion. It is our intention to complete a follow-up review exercise later in 2020 to ensure all actions are fully embedded and customers are being reimbursed when they have been the victim of a scam, having regard to the circumstances of the individual and the scam.

In addition, we will be using our findings from this assessment as part of the wider Code review which is due to begin in the coming months. This review is designed to look at the specifics of the Code and will decide if any adjustments are necessary.

Our view overall is that firms are endeavouring to implement and embed the requirements of the Code within scope of this review. We do not feel Firms are systematically using the reasonableness test as a barrier to stop reimbursement. However, as detailed within the report, there is still further work required to reach a consistent approach across the Firms.

It is our opinion that Firms need to complete further work to fully operationalise the requirements under section R2 (1) (c) , including improvements to governance, oversight and training for staff within the dedicated teams dealing with customers who have been scammed.

The LSB is committed to working with the industry to increase the number of Firms signed up to the Code. Whilst current signatories account for a large majority of market coverage, it is important that customers of other Firms also benefit from the protections of the Code.

We would encourage those Firms not already signed up to consider the contents of this report and review their arrangements for dealing with APP scam cases.