Lending Standards Board

Contingent Reimbursement Model Code for Authorised Push Payment Scams

Thematic review of provision SF1(2) – Effective warnings

Summary Report

December 2020

Contents

1. Introduction

The Contingent Reimbursement Model Code ('the Code') launched on 28 May 2019. The Code provides important protections for customers where they fall victim to authorised push payment (APP) scams, where customers are tricked into authorising a payment to an account that they believe belongs to a legitimate payee. 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. There are currently nine payment service providers ('firms') signed up to the Code.

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

Within the Annual Business Plan 2020, the LSB committed its intention to undertake a thematic review of how firms have implemented provision SF1(2) in relation to effective warnings. This review took place during August to November 2020, and involved all nine Code signatories.

The Code requires that where firms identify APP scam risks in a Payment Journey, they should take reasonable steps to provide their customers with effective warnings, which should include appropriate actions for those customers to take to protect themselves from APP scams.

2. Executive Summary

Background

All nine firms signed up to the Code as of 1 July 2020 were included within this review. Within all firms visited, there continues to be an element of embedding processes and operations, and an ongoing cycle of review and learn, with an aim of improving the types and content of warnings provided across all digital and interactive dialogue channels.

2.1 Key Findings

Overall, we found that firms had approached the implementation of effective warnings as a key tool in efforts to prevent APP scams taking place. It was acknowledged by all participants that warnings could be improved and enhanced but they could not prevent all occurrences of customers falling victim to scams. Most firms were in the process of reviewing the warnings in place and many had change programmes underway with a view to improving the design and impact of warnings.

Some of the change programmes were intended to create more dynamic and targeted warnings based on the type of transaction taking place. From the evidence provided, the proposed improvements and enhancements could lead to the design of warnings that would cause a customer to stop and think before proceeding with a payment which may be at risk of being a scam. To be truly effective, firms need to continually evolve warnings to take account of an ever-changing scams landscape.

We noted that firms are trying to find a balance between displaying impactful warnings and not having too much friction in the payment journey for genuine transactions. In addition, all firms have improved the level of consumer education information provided, for example through fraud 'hubs' on websites, banner advertising and aftercare.

We did, however, identify some breaches of the Code within individual firms, together with key areas for improvement across the industry. However, the breaches are not systemic across the industry, and we will be working with firms to ensure where these have been identified, they are resolved as a matter of priority.

As detailed below, there are some key areas where we believe improvements are necessary and indeed found instances where no, or insufficient, warnings were provided in payment journeys which resulted in breaches of the Code. Further, there was a noticeable difference of approach, in some firms, between digital and branch/telephony channels, with the latter being focussed on colleague intervention and conversation as opposed to providing purely static warnings.

Our concluding view is that there is still work to be done to meet all the requirements of the Code and reach a situation where all firms are displaying warnings which are effective in making a customer stop to carefully consider whether the payment should be made. Any findings identified will also be considered as part of the wider work we are undertaking in reviewing the whole of the CRM Code.

The key areas for improvement fell within five areas:

- **Effective warnings not provided** – There was an absence of warnings in some payment journeys, which has resulted in breaches of the Code. This was identified in a limited number of firms across differing payment channels. This is taken into account when firms assess liability for reimbursement of claims.

- **Assurance and oversight** – There was a lack of defined assurance programmes or oversight within some firms. Quality Assurance (QA) often relied upon existing processes but without any evidence of how these have been adjusted to take account of the Code.

- **Arbitrary thresholds** – Thresholds are being applied which are usually based on monetary amounts, often resulting in transactions below these thresholds either not receiving a warning, or receiving only some static text as a warning. Whilst the Code provides for warnings to be delivered on a risk based approach, particularly to avoid overuse and this then becoming ineffective, we were unable to evidence the basis for these thresholds. Our concerns therefore are based on the increased risk to customers who may fall victim to scams below these threshold amounts.

- **Formalisation of process** – There is a varied approach to governance of the Code, with some firms needing to develop more formalised and documented policies and procedures to aid in the design, implementation, review and enhancement of warnings.

- **Warning criteria –** The content of warnings still requires further development across all nine firms. Firms are at different points in the evolution of warnings but all require some element of improvement. Firms are not always using the data and MI available to help enhance and improve warnings.

It should be noted that the scope and purpose of this review was not designed for the LSB to provide an opinion on whether the warnings we reviewed had been, or would be, effective in preventing a customer from becoming a victim of a scam. The provision of effective warnings is just one of a number of different elements within the CRM Code which are designed to reduce the occurrence of scams and offer protection to customers.

2.2 Objectives and Scope

The objective of this review was to assess the interpretation and implementation of provision SF1(2), as detailed within Appendix 1 – Key provisions, and its effectiveness in delivering fair outcomes for customers, with a view to ensuring consistency across signatories of the Code.

The review assessed whether the systems, processes and controls in place maximised the opportunity to create and provide warnings, which would reasonably be expected to be effective in discouraging a customer from proceeding with a payment which might result in them being a victim of an APP scam. Where 'warnings' are referenced below, these refer to warnings as required under the Code. The review encompassed the following areas:

- The governance for creating and introducing warnings, including: any approval process, management information (MI) and internal quality assurance (QA), risk and control management, and ongoing oversight to ensure warnings meet the requirements of the Code. (OP) 3.1
- Policy and process around the creation and implementation of warnings, throughout the whole life cycle, with particular focus on how the warnings are deemed to be effective, and ensuring all warnings and education are clear, fair and not misleading (e.g. written in plain language) including within any aftercare offered. (OP) 3.1
  - How firms consider vulnerable and potentially vulnerable customers within policy, process design, controls and oversight for warnings to ensure greater levels of protection. (OP)3.1 (SF)3.5
- The training and education provided to staff who are involved in the provision of warnings, including branch and telephony staff. (OP)3.1 (GF) 3.2
- How warnings are considered and created for each transaction channel available to the customer where they may fall victim to an APP scam. This included how focussed and prominent the warning is to the customer, in that a reasonable expectation can be evidenced that the customer will not miss or misinterpret the warning. Dependent upon the composition of each firm, the channels where warnings may be delivered are:
  - Digital (potentially online and via mobile app)
  - Telephony
  - Branch (SF) 3.3
- The decisioning process for determining which warnings will be given and where in the payment journey these are deemed as required. (SF) 3.3
- How firms have considered tailoring warnings to the specific nature of the scam and channel of payment, in order to evidence how the warnings can be deemed effective across all channels and recognised scam types. (SF) 3.4
- Any limitations with regard to where a warning is provided. For example, whether monetary threshold limits apply which may impact the provision of a warning. (SF) 3.3

- How system and user acceptance testing of the warnings firms intend to put in place is considered, to ensure their effectiveness is considered pre-implementation. (SF) 3.4
- How the effectiveness of each warning is assessed post implementation, and how lessons learned from previous scam transactions are used to improve warnings. (SF) 3.4
- Provision of consumer education related to warnings, including as part of any aftercare provided in line with requirements under the Code. (GF) 3.2

Out of Scope

The scope of the review did not include any APP scam case sample testing to determine and conclude on the operating effectiveness of the design of warnings across their relevant payment channels.

Future thematic reviews conducted by the LSB will include APP scam case sample testing, as appropriate to the scope of the assessment.

2.3 Methodology and Approach

The review was conducted across several stages set out as follows:

- Firms were asked to complete a request for information. This was to provide the LSB with an overview of key processes, including supporting information and documentation.
- The LSB completed a desktop review of the information received, which was followed up with a series of online meetings with each individual firm involved (due to the Coronavirus pandemic, travel restrictions and associated remote working conditions). These meetings were undertaken to help aid understanding in how, following the launch of the Code, the policies, procedures and training in respect of provision SF1(2) have been implemented across all relevant channels during the pre and post implementation process for delivering effective warnings.
- During conclusion of the online meetings, the LSB held a close out session 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 complete the assessments.
- An individual report, setting out the LSB's findings from the review assessment, has been issued to each firm, including any required actions which will be tracked through to completion.

3. Detailed Report

We have focussed the detailed report on the specific test areas reviewed in relation to the requirements of the whole of SF1(2), with areas of the scope related to governance, controls and oversight concentrated within the Overarching Provisions. Reference to each test area has been included within the scope noted earlier in the report. Appendix A contains the specific Code wording in relation to this thematic review.

3.1 Overarching Provision (OP)

All firms have in place clear governance structures with defined accountabilities across their businesses for the Code. We found that firms held regular discussions, with information being escalated throughout committees, to assist with the design and approval for the implementation of warnings. We believe that for some firms, the focus of the Management Information (MI) within these meetings needs to be adjusted. Currently the MI is often focussed on level of claims and post scam information, and whilst this is valuable information, we believe that firms should expand the level of data provided at an Executive level to ensure sufficient focus is also given to the prevention of scams.

Firms are beginning to make use of data obtained directly from within the payment journey, both before and after the transaction has occurred, as well as when a transaction does not proceed. This work is in the very early stages and therefore results are not fully visible. Whilst we cannot comment directly on the impact of this work on effective warnings it is an area that we would encourage firms to continue analysing.

The visibility of effective warnings through the differing governance structures was clear, however we did identify a lack of oversight and assurance in this area across a number of firms. A lack of quality assurance and oversight across any of the three lines of defence could leave firms at risk of not fully meeting their responsibilities under the Code.

Within the branch and telephony offerings, we identified that quality assurance processes were in place. However, we were unable to evidence that these had been adjusted sufficiently to take account of all the requirements of the Code when providing an effective warning.

The policy and process followed by firms for implementing effective warnings is established within all firms. This often includes an element of test and learn processes, with outputs being used to refine the warnings. We noted that, within some firms, these processes were rather informal and not recorded. This formalisation would better evidence the procedures undertaken for the provision of warnings, and how the success of these are quality assured across various channels. In addition, we believe that formal recording of processes would

help with succession planning, or where design of warnings is currently operating as a change programme, so that there is an opportunity to ensure 'business as usual' standards are in place.

The final area of scope for this test was focussed on the training of key members of staff involved in the provision of warnings. Structured training and competence programmes have been implemented by all firms, with a general focus on all aspects of the CRM Code. In addition, more job specific training has been provided in relation to effective warnings. For example, digital teams are provided with insight as to the reason and purpose of warnings, whereas branch and telephony staff receive training on how to converse with customers around scam dangers.

Within the scope of our review we could not confirm how successful the roll out of training was and we would recommend that firms continually review the refresher training given to staff in order to meet the requirements of the Code.

Areas for improvement:

- Governance approaches should not be focussed purely on claims and data related to APP scam cases. Firms should use all MI at their disposal to assist with the development of warnings and to report on their impact in preventing scams.
- Firms should formally document the procedures in place for designing, testing, implementing and assessing warnings across all channels to allow better evidence of reiterative review and to allow for succession planning.
- Increased analysis of MI and data at key points should continue to be developed for use in both monitoring the success, or otherwise, of warnings and continual development.
- Improvements are necessary to the oversight and assurance frameworks across all three lines of defence. Focus should be appropriate to the channel being overseen.

Examples of Good Practice:

- CRM specific forums and committees, incorporating key internal stakeholders, are helpful in ensuring warnings are regularly discussed and assessed.
- Focussed customer outcome initiatives, whereby firms are making better use of behavioural science and beginning to develop improved means of increasing customer feedback about the payment journey, are being used to design and improve warnings to increase customer protection.
- Accountability for the design and delivery of warnings is clearly defined and understood across firms.

3.2 General Expectations of Firms (GF)

The raising of awareness and consumer education has increased across all signatory firms since inception of the Code. Throughout our review, we saw many examples of consumer education being developed or implemented which is aimed at APP scam prevention. A significant number of firms have developed a 'hub' within their main website containing information on scam awareness and prevention. There are many other examples being employed by firms such as: in-branch posters; digital advertisement banners; social media posts; and case study videos being made available.

At present a large proportion of the education is generic across the whole of the scams landscape. However, it is clear that firms' intentions are to be more innovative and impactful in providing targeted education to both customers and staff.

Areas for improvement:

- Firms should consider the development of more targeted education based on specific scam types. This is particularly important as part of any aftercare for customers.

Examples of Good Practice:

- The use of social media as a format for providing education on how to protect against scams is a useful tool, particularly given the rise in online spending over recent months.
- Links to external organisations are being utilised by firms to ensure the targeting of messages to specific customer types.
- Detailed 'hub' pages within websites are a good source of general information for customers.

3.3 Standards for Firms (SF); Prevention SF1(2) (a), (b) and (c)

All firms within the scope of this review were able to evidence their approach to the provision of warnings across digital, branch and telephony channels. However, we did note some examples where warnings were not being provided, impacting all payment channels, which is a direct breach of the Code, resulting in a risk to customers and their ability to take any actions to protect themselves from scams.

This issue is not systemic across the industry, but we are working as a matter of urgency with individual firms to ensure that they comply with the Code where this issue has been identified. If a customer falls victim to a scam and no warning was provided, all firms have confirmed

that this is taken into account when assessing liability in reimbursement claims, while also considering all the circumstances at the time of the scam.

Firms' use of analytics, MI and identification of scam risks and scam payment types forms the basis of when effective warnings are displayed to customers. Warnings within the digital channels are typically provided where a customer has selected a new payee, or is amending an existing payee, with such warnings being displayed in a manner that would require the customer to take action to proceed, generally by making a positive election to continue with the payment despite the warning. We found varying approaches to how customers were able to abort transactions following the provision of warnings within digital channels. In some instances, the option to abort a transaction was less obvious on-screen than the option to confirm receipt of the warning and proceed. These options should both be clear and prominent, ensuring a customer is able to make an informed choice about whether to proceed or not. Firms should also ensure that the option to proceed does not amount to a customer declaration which could be construed as enforcing a customer to accept liability should they subsequently be found to have been a victim of a scam.

Within branch and telephony channels, the approach to the provision of warnings was often more script based, although as the Code is embedding further, there has been a move to more conversational approaches, during which staff are able to deliver any relevant warnings. On occasion, we were unable to clearly evidence the wording of the actual warnings given, particularly where this is more conversational and not recorded within the firm's system.

We identified some variations between firms 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. Thresholds for the provision of warnings should not be used based on operational constraints or commercial costs. The provision of an effective warning should be based on the scam risks identified within the payment journey.

Areas for improvement:

- Firms should provide an effective warning at key points within the payment journey across all channels as specified within the Code.
- Warnings should be tailored to the scam risks and payment type to provide the best protection for customer relating to the payment type.
- Firms should ensure clear records are maintained of conversations with customers and the warnings which were provided, including consequences of proceeding, when dealing with customers in branch or by telephone.

- Thresholds for the provision of warnings should not be used based on operational constraints or commercial costs. The provision of an effective warning should be based on the scam risks identified within the payment journey.
- Firms should consider the wording used within warning messages to ascertain if a customer wishes to proceed with a payment to ensure this does not become a declaration of liability.

Good Practice:

- Dynamic feedback from customers in the development of warnings, together with feedback from those who have been a victim of a scam, is used by some firms as part of their cyclical process for reviewing and redesigning warnings.

3.4 Standards for Firms (SF); Prevention SF1(2) (d) and (e)

Overall, we found that firms have made progress, since inception of the Code, in the design and content of effective warnings. Some have sought engagement from external sources to assist with how warnings are written and presented to ensure these are clearly understood by customers whilst making them aware of any actions necessary and the consequences of continuing with a payment.

The Code requires specific areas to be included within the content of warnings. There is further work for some firms in ensuring warnings are tailored to their customer base, particularly between personal and business customers. The changing nature of the scams landscape means that warnings need to be reviewed and amended regularly to reduce the risk of scams occurring. The example warnings provided to the LSB as part of this review, identified that some firms are further advanced in the design of content which could reasonably be expected to make customers stop and think before proceeding with a payment. However, this should not be a reason to avoid reviewing or updating warnings.

Some firms are still using static warnings, where every customer receives the same information regardless of scam risk or payment type. As mentioned previously, warnings should be tailored to the scam risks and payment type. This is an area where firms should ensure their continuous improvement programmes address the risks that a static approach has from a customer outcome perspective.

Typically, within digital channels, firms used a design, test and learn approach which incorporates an element of User Acceptance Testing (UAT). In many cases this testing was carried out by actual or prospective customers to obtain 'real life' feedback. We believe that this provides firms with a good opportunity to ensure the requirements of the Code were working in respect of warnings. An alternative model of internal testing of warnings by the

firm itself carries a risk of losing the view of the actual end users. We noted, however, that some firms had conducted little post implementation testing or review of the impact that warnings were having on customers.

The branch and telephony channels have a mix across firms of scripted and conversational process for the delivery of warnings. The content of any scripts is usually designed to reflect that which is provided within the digital channel. Conversely, some firms have implemented a process to engage customers in more of a conversation to probe further before providing a warning. However, records are not always updated to confirm the conversation or delivery of the warning is left to the discretion of the staff member. Our view is that this could result in key messages being missed depending on the direction of the discussion.

Areas for improvement:

- Firms should make use of all MI, data and feedback from victims of scams to understand how the effectiveness of warnings can be improved to fully protect customers. Testing and review should not be a one off process but continue on a regular cycle.
- A mix of scripting and free format discussion would be most appropriate for voice channels. This would ensure key warnings are provided but leaves discretion to staff as to the point at which this is introduced within the conversation, with suitable oversight in place to ensure controls are embedded and learnings are drawn out.
- Whilst warnings should be tailored to the payment type, firms should also ensure the customer type, i.e. personal or business, is also considered when creating the content.

Good Practice:

- Firms have engaged with a number of external sources to assist with the development of warnings, including behavioural scientists, consumer representatives and law enforcement.

3.5 Standards for Firms (SF); Prevention SF1(4)

Most firms acknowledged the challenge of designing warnings to provide enhanced protection for customers identified as being vulnerable to scams, especially when considering the digital channels. Firms typically rely on organisation-wide vulnerable customer policies and processes, rather than a CRM specific version.

Given the prevalence of transactions conducted digitally, it is acknowledged that challenges exist in identifying customers vulnerable to scams, without prior knowledge of customers' circumstances or customers self-identifying where they have vulnerabilities. Some firms have begun to use claim data to identify customers who had fallen victim to a scam in the past due

to vulnerability and have implemented system rules which result in those customers being contacted to try to prevent them becoming a repeat victim. These rules ordinarily last for a fixed period of time.

Within branch and telephony channels, firms tended to rely on staff judgement and system flags to identify customers who may be more vulnerable to a scam. Staff have been provided with enhanced training covering scam types, and other key factors such as social engineering and how this affects customers.

Areas for improvement:

- Firms should continue to test, learn and adapt to ensure that customers who are vulnerable to scams are considered in the design and delivery of warnings.
- Firms should ensure that any vulnerability policies are adapted to take account of the requirements of the CRM Code.

Good practice

- Due to the current situation in relation to COVID 19, firms have increased their monitoring of customers who are vulnerable to scams beyond the usual parameters. Whilst this is a temporary position, it is helpful to ensure there is enhanced support at a time where there may be increased risk of scam activity due to the current global situation.

4. Conclusions and next steps

This review was undertaken to understand how the requirements of provision SF1(2) – Provision of effective warnings - have been interpreted and implemented by firms.

Our purpose was to ensure there was a consistency of approach across the industry whilst delivering fair outcomes for customers.

During 2020 we have experienced unprecedented times caused by the coronavirus pandemic, one element of which has been the increased usage of digital banking and online shopping. It is therefore more important than ever that firms have in place suitable effective warnings to protect customers and help to stop the occurrence of scams, particularly given how scammers have taken advantage of the pandemic to socially engineer and adapt existing and new scams.

Our view overall is that whilst firms have demonstrated a commitment to enhancing the provision, and content, of warnings to ensure better protection for customers, further work is needed within the industry to ensure warnings are achieving their aim. The LSB acknowledges that to be truly effective, firms need to continually evolve warnings to take account of an ever-changing scams landscape. There are a number of change programmes underway to continually review, enhance and implement effective warnings which will go some way to achieving this.

We did not find any industry-wide systemic non-compliance or breaches of the Code. However as detailed in this report, we identified breaches of the Code within some individual firms, along with a number of key areas for improvement across the industry.

We have issued individual reports to each firm which contain recommendations and required actions to resolve any breaches or areas for improvement as a matter of priority. We will be working with firms to ensure these are implemented, including tracking through to completion. It is our intention to complete a follow up review exercise during 2021 to ensure that all breaches are remedied and all actions are fully embedded.

Any findings from this review will also be considered as part of the wider CRM Code review consultation we are undertaking. Recommendations from the Code review will be published in early 2021.

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.

Appendix 1 – Key provisions

Overarching Provisions (OP)	
OP1	*In implementing and complying with this Code, Firms should act in a way which advances the following overarching objectives:*
(1)	*to reduce the occurrence of APP scams*
(2)	*to increase the proportion of Customers protected*
(3)	*to minimise disruption to legitimate Payment Journeys*
Definitions and Scope (DS)	
DS1(2)(h):	*Effective Warning – a warning designed and given in accordance with the provisions in SF1(2)(a) to (e)*
General Expectations of Firms (GF)	
GF(1)	*Firms should participate in coordinated general consumer education and awareness campaigns.*
(a)	*Firms should take reasonable steps to raise awareness and educate Customers about APP scams and the risk of fraudsters using their accounts as 'mule accounts'. Firms should do this by undertaking their own campaigns, and/or participating in, contributing to, or promoting, campaigns undertaken by other relevant parties.*
Standards for Firms (SF)	
Prevention	
SF1(2)	*Where Firms identify APP scam risks in a Payment Journey, they should take reasonable steps to provide their Customers with Effective warnings, which should include appropriate actions for those Customers to take to protect themselves from APP scams.*
(a)	*Firms should take reasonable steps to make their Customers aware of general actions that could be taken to reduce the risk of falling victim to an APP scam.*
(b)	*Where the Firm identifies an APP scam risk, it should provide Effective warnings to customers. This may occur in one or more of the following:*
(i)	*when setting up a new payee;*
(ii)	*when amending an existing payee; and/or*
(iii)	*during the Payment Journey, including immediately before the Customer authorises the payment, before the Customer's account is debited.*
(c)	*Effective warnings should be risk based and, where possible, tailored to the APP scam risk indicators and any specific APP scam types identified through the user interface with which the Customer is initiating the payment instructions.*
(d)	*Effective warnings should enable the Customer to understand what actions they need to take to address the risk, such as more appropriate payment methods which may have additional protections, and the consequences of not doing so.*
(e)	*As a minimum, Effective warnings should meet the following criteria:*
(i)	*Understandable – in plain language, intelligible and meaningful to the Customer*
(ii)	*Clear - in line with fair, clear and not misleading standard as set out in Principle 7 of the FCA's Principles for Businesses;*
(iii)	*Impactful – to positively affect Customer decision-making in a manner whereby the likelihood of an APP scam succeeding is reduced. This should include steps to*

	ensure that the Customer can reasonably understand the consequences of continuing with an irrevocable payment;
(iv)	*Timely – given at points in the Payment Journey most likely to have impact on the Customer's decision-making;*
(v)	*Specific – tailored to the customer type and the APP scam risk identified by analytics during the Payment Journey, and/or during contact with the Customer.*
SF1(4)	*Firms should apply additional measures to protect Customers that are, or may be, vulnerable to APP scams under the provisions at R2(3)*
(a)	*Firms should take steps to identify Customers who are or might be vulnerable to APP scams under the provisions at R2(3)*
(b)	*Firms should implement measures and other tools to reduce the likelihood of such Customers becoming victims, or repeat victims, of APP scams. Leading examples can be found in the Annex to the Practitioner Guide.*
(c)	*Firms should include consideration of relevant industry standards, for example the BSI PAS 17271*