# Lending Standards Board

# Review of the Contingent Reimbursement Model Code for Authorised Push Payment Scams

## January 2021

# Contents

## 1. Executive Summary

The Lending Standards Board's (LSB) mission is to drive fair customer outcomes within financial services through independent oversight.

This report represents the LSB's first full review of the Contingent Reimbursement Model for Authorised Push Payment Scams (the Code) since becoming responsible for the governance of the Code in July 2019.

Authorised Push Payment (APP) scams involve fraudsters, posing as legitimate payees, who trick customers into transferring money to them. Reported losses due to APP scams were £455.8 million in 2019. This was split between personal (£317.1 million) and nonpersonal or business (£138.7 million)[1]. These types of scams can have a harmful impact on victims, and have been subject to attention from government, regulators, consumer representatives and the media[2].

Between 28 May 2019 and 1 July 2020, we found that signatory firms recorded 123,066 cases which fell within the scope of the Code.

This review has considered how the Code has been implemented by firms, adopted into the wider payments landscape, and where improvements are required to the Code to ensure greater consistency in its application. It has encompassed a broad evidence base; including previous LSB thematic reviews, a public consultation, analysis of data from signatory firms and ongoing engagement with stakeholders. **This report sets out our recommendations, to be taken forward by the LSB and stakeholders, to ensure that the Code and the consumer protections which sit at the heart of it work effectively.**

The principles of the Code received strong support across all stakeholders. It was acknowledged that the Code, alongside other initiatives, works to address what was a clear gap in the payment landscape as more customers send and receive payments particularly online, and correspondingly, more scammers view online payments as a target for malicious activity. However, there remain inconsistencies in application and outcomes under the Code and awareness remains low.

Take up of the Code from industry has been slower than we would have expected. In our report, we have set out the importance of collaboration across stakeholders to tackle the issue of APP scams and that **increasing participation in the Code is a collaborative effort for the LSB, regulators and industry bodies**. The Code should also be capable of being adopted by a **wider range of participants** providing payment services to consumers but without diluting the standards of protection provided.

The nature of scams is that they evolve to find ways around regulation, systems and processes that have been implemented to identify and reduce their occurrence as well as finding new ways to exploit and manipulate consumers. We will therefore ensure that the **scope of the Code** does not fall out of step with these developments.

[1] UK Finance, Fraud The Facts, 2020
[2] Sky News; Money Box; BBC.

Our review and wider work has identified that issues remain with the implementation of the Code within firms and that this is driving inconsistencies across signatories and outcomes for consumers. We will address this by setting out **expectations around governance arrangements** and related controls to ensure that the Code is embedded within the culture of Code signatories, from senior management through to customer facing staff. This will help to drive consistency of application across the industry. Further work is also required to ensure that the requirements of the Code **reflect the responsibilities of firms,** especially those of firms who receive funds from an APP scam.

We also found that **work is required to define success measures for the Code**. While the objectives of the Code, developed by the APP Steering Group, are clear, there is no consensus on how to determine if it has been successful in meeting these. We believe that it is vital that the effectiveness of the Code is defined in wider terms beyond solely focusing on reimbursement.

On resolutions of APP scams, we will update the Code to allow **for firms to 'self-fund'** reimbursement of customers who are found to be in a 'no blame' scenario.

We are aware that some firms employ **policies of automatic reimbursement for APP cases** below certain thresholds. We also saw the wish for APP scams to be defined by their value, and the proposal of policies which would amend the scope of the Code to remove lower value and purchase scams from the Code's remit. Whilst we note the proposed rationale for taking this approach, as it would allow for focus to be placed upon more complex, higher value APP cases, we are concerned about the unintended consequences of adopting such policies. We would not want to see the Code protections withdrawn from customers to whom smaller losses represent huge impacts, such those on lower incomes, nor would we want to create a message for scammers that lower value losses will be disregarded, thus creating the potential for repeated targeting. We will continue to monitor developments in this space.

**Summary of recommendations**

In light of the findings we have set out above, we have made 10 recommendations which we believe are required to ensure that the Code is able to work effectively:

1. The scope of the Code should reflect the evolving nature and complexity of APP scams in order to ensure that it is able to provide effective protection for consumers.
2. The Code should recognise the wider range of participants within the payments industry while ensuring that it retains a consistent approach to the standards of protections provided.
3. New governance and oversight provisions should be introduced into the Code. These will require firms to have appropriate processes, controls and governance arrangements in place, ensuring that there is effective senior management oversight of the firm's adherence to the requirements of the CRM Code.
4. The Code should more fully reflect the roles and responsibilities of receiving firms in the customer payment journey.
5. In order to fully assess the effectiveness of the Code, a series of success measures should be defined, which take account of, but look beyond reimbursement levels.
6. Work should be undertaken to ensure that there is a consistency of approach and interpretation to APP related data. Data reporting requirements should be built into the Code to support and inform the LSB's oversight work.

7. The practitioners guide should be reviewed to ensure that it takes account of developments within the wider regulatory environment in relation to the fair treatment of vulnerable customers.
8. The wording of the Code at SF1(3) should be reviewed so that the provision becomes effective within the Code for those firms who have implemented Confirmation of Payee.
9. The information for customers document should be reviewed to ensure that it takes account of any relevant changes which may result from our wider review of the Code. As part of this, consideration should be given to how awareness of the document itself can be improved.
10. Provision ALL2(3) of the Code is updated to reflect that firms may fund no blame cases from the central fund or 'self fund' the reimbursement of customers who are assessed to be in a 'no blame' scenario.

**Next steps**

The actions we plan to take, in order to address the issues which emerged, are discussed throughout the body of this report after each section of the findings. Whilst the suite of recommendations outlined will be driven by LSB, we will inevitably work with our stakeholders as some of the issues which emerged, such as raising customer awareness about the Code, can be most effectively addressed by others, who for example have a direct relationship with customers.

We will begin work on the recommendations set out in this report straight away. Some recommendations require further work and/or input from stakeholders and we will therefore issue a Call for Input by the end of Q1 2021 to inform our thinking across these areas. We have identified where this is required at relevant points of the report. We will also publish a timeline for our work by the end of February 2021.

## 2. Background to the Contingent Reimbursement Model Code

In September 2016, the consumer body Which? submitted a super-complaint to the Payment Systems Regulator (PSR) which raised concerns about the level of protection for customers who fall victim to APP scams. The PSR investigated the concerns raised and published its formal response in December 2016[3]. The response recognised that further work was needed and made recommendations for actions to be taken by industry. In 2017, the PSR published an update on the progress made, recognising that there were still concerns around the reimbursement of victims of APP scams and consulted on the introduction of a 'contingent reimbursement model'.[4] In March 2018, the APP Steering Group (Steering Group) was established to lead the development of a voluntary industry code for the reimbursement of victims of authorised push payment scams. The CRM Code became effective on 28 May 2019.

### a. The role of the LSB

On 1 July 2019, the LSB became the independent governing body of the CRM Code. 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.

Our role is to monitor signatory firms' implementation and ongoing adherence to the Code, to ensure its effectiveness and to maintain and refine it, as required. To support the transition of the Code from the APP Steering Group to the LSB, we established an Advisory Group to support our stewardship of the Code. The Group, chaired by Ruth Evans, has three members drawn from Code signatories and three members who represent the consumer interest. We would like to thank the members of the group for their input and have been appreciative of the challenge and support provided over the course of the past 18 months.

In July 2020, we launched a review of the CRM Code with a public consultation seeking to understand the effectiveness of the Code in its first year of implementation. In addition to undertaking a full review of the CRM Code, we have been monitoring the implementation of, and compliance with, the Code through a series of thematic reviews[5]. This current report takes into account the findings from these previous thematic reviews, especially where recurrent themes emerged.

Throughout the Code review process, we have engaged with a wide range of stakeholders both to garner views, and to test our thinking as we developed the recommendations set out in this report. With the progress of Brexit, and as the Withdrawal Agreement is now in place, government departments such as HM Treasury will be working with a number of regulators and organisations who have responsibility for the payments sector to integrate rules.

---

[3] PSR: Which? Super complaint

[4] https://www.psr.org.uk/psr-kick-starts-industry-wide-effort-tackle-payment-scams

[5] The findings from these reviews are discussed in greater detail below. The reviews are:
LSB, Review of approach to reimbursement of customers, April 2020
LSB, Review of effective warnings provisions of the CRM Code, December 2020.

We will continue to work with the relevant authorities such as the PSR, HM Treasury, the Open Banking Implementation Entity (OBIE), Financial Ombudsman Service (FOS), Financial Conduct Authority (FCA), Bank of England (BoE), the Home Office and others to identify and manage the implications of this on our work and that of the Code.

### b. The Contingent Reimbursement Model Code

The CRM Code was launched on 28 May 2019, and sets out good industry practice for preventing and responding to APP scams. The Code was developed through collaboration between consumer and industry groups, to reduce the impact of APP scams on consumers, micro-enterprises and small charities by introducing measures that would reduce the occurrence of such scams and see victims reimbursed. The Code aims to achieve this by ensuring that consumers, who bank with a firm that is a signatory to the Code, will be reimbursed if they have been the victim of an APP scam and they have taken a reasonable level of care when making a payment. As well as addressing what should happen in the event that a customer falls victim to a scam, the Code also requires signatories to put in place measures to reduce the occurrence of APP scams.

The Code provides protections to customers when they authorise a transfer of funds executed across Faster Payments, CHAPS or an internal bank transfer that turns out to be fraudulent. The Code therefore provides protections against a range of scam types, including invoice and mandate scams, CEO scams, impersonation scams, purchase scams, investment scams, romance scams and advance fee scams.

Currently, there are nine firms, comprising 20 brands, signed up to the Code. The nine firms are:

- Barclays Bank UK plc - *Barclays*
- The Co-Operative Bank Plc – *The Co-Operative Bank plc, Britannia and Smile*
- HSBC UK - *HSBC, First Direct and M&S Bank*
- Lloyds Banking Group - *Lloyds Bank plc, Halifax, Bank of Scotland plc and Intelligent Finance*
- Metro Bank
- Nationwide Building Society
- NatWest Bank plc - *Royal Bank of Scotland plc, NatWest Bank and Ulster Bank*
- Santander UK - *Santander, Cahoot and Cater Allen Limited*
- Starling Bank.

As such the Code provides protections against APP scams for a significant proportion of UK consumers with over 85% of faster payments covered.

### c. Wider environment

The LSB's oversight of the CRM Code takes place alongside a range of stakeholder activity and initiatives across government, regulators, consumer organisations and the industry itself focusing on reducing the level and impact of APP scams. Within the wider environment we are aware that there are calls for the Code, or aspects of it, to be made mandatory through legislation or regulation.

In our role as an independent oversight body, it is not appropriate for us to influence or opine on the issues around the mandating of the Code to any agenda. We believe that the issues which have surfaced as a result of our work will need to be addressed regardless of the form the Code protections take on. Therefore our priority remains focused on ensuring that the best consumer protections are in place and we will continue to work closely with regulators and industry to ensure this happens.

In March 2020, the PSR held a meeting with key stakeholders to discuss progress being made on APP scams.[6] Following this, the PSR published its view and set out options for the future, including the potential to introduce a new rule into the Faster Payments Scheme that would require reimbursement of all customers who have fallen victim to an APP scam. We understand that the PSR continues to develop its thinking in relation to APP scams.

APP scams have also been the focus for the Treasury Select Committee which launched a new inquiry to review what progress has been made in combatting economic crime in October 2020.[7] Meanwhile, the OBIE is due to publish a consultation which will look at the direct participation of Payment Initiation Service Providers (PISPs) in the CRM Code and with Confirmation of Payee. This will sit alongside the publication of research which explores how warning messaging within the payment journey could be optimised to increase consumer attention, reduce fraud, and improve the overall consumer experience.

[6] PSR, APP Scams conference call.

[7] UK Parliament, Committee launches new economic crime inquiry, October 2020

## 3. Method and Approach

Our review has sought to assess overall how the Code is working, seeking views on how it has been implemented and what further improvements may be required to ensure its effectiveness. It encompassed evidence and views collected from four primary workstreams including: the public consultation; data from signatory firms; findings from LSB themed reviews and stakeholder engagement activity. The consultation also considered the content of the Code and supporting documents, that is, the practitioner guide, which is made available to Code signatories, and the customer facing information document which is hosted on the our website.

The findings from this report will provide the basis for our ongoing work to improve the operation of the Code and to ensure it is continually delivering good outcomes for customers.

### a. The public consultation

In July 2020, we issued a consultation document setting out questions in a range of different areas, including:

- Implementation – with questions seeking to establish any challenges firms have faced in adopting the Code, any barriers that exist to new firms signing up, and areas where the Code could be improved to take account of new insight and the broad range of firms involved in the offering of authorised push payment services.

- Customer experience – with questions seeking to establish whether the Code has met its objective to increase the proportion of customers protected from the impact of APP scams, both via reducing incidents of scams and by reimbursement, and to determine what the experience of victims of APP scams has been in the year since the Code was launched.

- Prevention measures – with questions seeking to establish whether consumer education and awareness campaigns, warnings, and Confirmation of Payee are working effectively to support the objectives of the Code.

- Resolving claims – with questions seeking to establish what challenges firms face when making a decision to reimburse a customer, including in relation to how that reimbursement is funded in the case of 'no blame' scenarios.

### b. Respondents

We received 26 responses from stakeholders across: Code signatories; consumer organisations and individual experts; firms providing payment services to consumers; industry and trade bodies and government and regulators. Many of the responses submitted included sensitive operational information and were provided on a confidential basis. We are grateful for the openness of these responses and the nature of information provided which allowed us to look in-depth at the workings of the Code. Given the highly sensitive nature of many of the responses, we have taken the decision not to publish responses we received to the consultation.

### c. Data analysis exercise

To further support our review, data was requested from all nine signatory firms to help support our understanding of how the Code has been implemented and applied since May 2019. The data included information about types of APP scams, resolution decisions and customer reimbursement levels under the Code, and covered the period from 28 May 2019 to 30 June 2020. An external researcher was commissioned to analyse the data, and the report providing a full analysis of the anonymised data has been published alongside this report.

Our report shows that between 28 May 2019 and 1 July 2020, signatory firms recorded 123,066 cases which fell within the scope of the Code. This was similar to the findings reported by UK Finance in its overview of payment industry fraud for a similar period, although the data in our report related to around an additional 12,000 cases[8]. We have assumed that this additionality relates to firms' data reporting systems bedding down as the Code has been implemented within signatory firms.

### d. LSB's compliance work

We have carried out two themed reviews on the CRM Code which have involved all signatories to the Code with a follow-up review currently underway.

**The approach to reimbursement of customers under the CRM Code**

The first of our themed reviews on the CRM Code was published in April 2020, and focused on the approach to reimbursement of customers under CRM Code provision R2(1)(c).[9] The review included an assessment of the key controls and processes firms had in place to demonstrate compliance with the provision, including how firms had interpreted the provision and the level and depth of staff training. Whilst the review found that firms had taken positive steps to implement the requirements of the Code for reimbursing customers, we identified key areas for improvement.

- We found that judgements about reimbursement were not always being 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 of APP scams 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.
- The fact that a customer had been provided with a warning was at times treated as a strict liability regardless of how effective the warning was or whether the customer had a reasonable ground for not acting on it. We found that warnings themselves varied in the extent to which they engaged customer attention and in their level of specificity. They were also not necessarily available across all payment channels.

[8] These relate to data from the nine signatory firms from 28 May 2019 to 30 June 2020 and are available across two reports: https://www.ukfinance.org.uk/system/files/Fraud-The-Facts-2020-FINAL-ONLINE-11-June.pdf and https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/2020-half-year-fraud-report.

[9] LSB review of approach to reimbursement of customers, April 2020

- We also found that 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, we found that evidence of vulnerability was available to the firm, but it was not always used as a consideration for reimbursement.
- 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.

**Provision of warnings within the payment journey**

We undertook a second themed review of SF1(2) on the provision of effective warnings by firms which was published in December 2020[10]. The review assessed whether the systems, processes and controls within firms maximise 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.

We identified a number of areas for improvement:

- There was an absence of warnings in some payment journeys, which we found had resulted in breaches of the Code and was identified in a limited number of firms across differing payment channels. However, we found that the absence of a warning was taken into account when firms assessed liability for reimbursement of claims.
- There was a lack of defined assurance programmes or oversight within some firms. Quality assurance often relied upon existing processes but without any evidence of how these had been adjusted to take account of the Code.
- In some instances thresholds were being applied which were 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 therefore becoming ineffective, we were unable to evidence the basis for these thresholds.
- There was a varied approach to governance of effective warnings, with some firms needing to develop more formalised and documented policies and procedures to aid in the design, implementation, review and enhancement of warnings.
- Firms were at different points in the evolution of warnings but we found that all required some element of improvement. We also found that firms were not always using the data and metrics available to help enhance and improve warnings.

In line with the LSB's oversight framework, we issued individual reports to firms which contained recommendations and required actions identified during the reviews. We are continuing to work with firms to ensure that these are implemented. Work has started on the follow up review on provision R2(1)(c) to ensure that firms have addressed and implemented the recommendations and actions previously identified.

[10] LSB, Review of Effective Warnings Provision of the CRM Code, December 2020

## 4. Findings

The following sections set out our findings from our review which have been addressed across the following areas: implementation; customer experience; prevention measures and resolving claims.

### 4.1 Implementation

#### a. Current version of the Code

The CRM consultation sought views on the current version of the Code. It considered whether it is clear in its purpose and scope, with questions seeking to establish any challenges firms have faced in adopting the Code, and any barriers that may exist to new firms signing up. It also sought to understand whether there were areas where the Code could be improved to take account of new insights and the broad range of firms providing payment services.

It was positive to note that the responses were broadly in favour of the purpose of the Code, with many commenting that the Code is complementary to existing rules and regulations on consumer protection. Feedback on the scope however, was more varied and can be categorised into the following themes, which will be explored in further detail below:

- the objectives and whether these required clarifying;
- the current scope of the Code with regards to types of scams and business models; and
- responsibilities between sending and receiving payment firms.

#### b. The Code's objectives

The Code has three overarching objectives, these are to:

- reduce the occurrence of APP scams;
- increase the proportion of customers protected from the impact of APP scams, both through reimbursement and the reduction of APP scams; and
- to minimise disruption to legitimate payment journeys.

A proportion of respondents, namely those advocating for consumers as well as a minority of payment service provider representatives, asked for clarity on the objectives and whether there was priority amongst them. This was particularly in circumstances where the objectives are perceived to be opposing to one another, for example where necessary friction needs to be added to the payment journey in order to delay a payment that is suspected of being an APP scam.

A small number of responses further suggested that a prioritisation exercise of the objectives should result in narrowing of the scope of the Code, so that the consumer protection element takes precedence, with the other two objectives being left outside of the powers of the Code. This feedback, however, was not shared across all respondents, and the majority saw the inclusion of all objectives to be necessary to the Code. This was on the basis that these objectives link the Code into existing scam prevention initiatives by the industry requiring collective efforts in order to create efficient and safe payment journeys and to reduce the occurrence of scams levels. Respondents felt that these are objectives that cannot be divorced from the aims of consumer protection.

It is the LSB's view that reducing the occurrence of APP scams is an important part of the Code and an integral part of the protections provided under it. We do not believe that the intention of the original drafting was to set out an order of importance in terms of the objectives and it is our expectation that they are considered as a whole rather than isolation to each other. We were not persuaded that the objectives conflict with one another and are of the view that any prioritisation could have unintended consequences and potentially negatively impact on the implementation and/or operation of the Code. While we keep the wording of the Code under regular review, as we do across the Standards of Lending Practice and codes within our remit, we do not intend to progress any further work to amend or review the objectives of the Code.

**c. Scope of the Code: type of scams**

The Code applies to the movement of funds from the customer's account to an account controlled by the scammer (the first generation account). Once received, funds will be quickly moved onwards to potentially a number of accounts. For the purposes of the Code, firms whose accounts are utilised in the onward transmission of APP scam funds are out of scope.[11]

There was some anecdotal evidence provided via consultation responses which suggested that APP scams are evolving in sophistication for example increasing the number of transactions which may be involved in the scam, making it more difficult to track and freeze the funds or changing methods to perpetrating the scams which may not be captured by the Code as it currently stands. The evidence submitted to us was limited but given the potential for customer detriment, the evolving nature of APP scams and how they are taken into account within the scope of the Code requires further consideration.

Given the rewards, those who perpetrate APP scams will continue to evolve approaches and techniques to ensure that they are able to exploit gaps both in consumer awareness around APP scams and the systems and controls implemented by the industry to address them. As the payments journey and movement of funds becomes more complex, involving a wider range of participants, the attribution of responsibility for the consequent remedial actions may become less clear, and may move beyond the scope of current Code protections. It is important then, that we along with industry, regulators and customers are aware of, and understand the nature of such emerging scams, their prevalence and the customer experience in such payment journeys.

**Recommendation**

The scope of the Code should reflect the evolving nature and complexity of APP scams in order to ensure that it is able to provide effective protection for consumers.

**How we will address this**

We will seek further evidence, via a Call for Input, about the nature and prevalence of newer emergent scams, including those involving open-banking technology. The findings from the Call for Input will inform our understanding of whether the scope of the Code requires further review.

[11] Provision DS2(1)(b) CRM Code is between GBP-denominated UK-domiciled accounts.

**d. Scope of the Code: business models**

As financial services and the payments ecosystem continue to evolve, business models outside of traditional banking structures have developed to serve customers' financial and payment needs. Against the backdrop of this evolution, it is vital that protections are afforded to as many customers as possible who use both traditional and newer banking/payment models. We were therefore encouraged by the diverse range of firms that expressed interest in participating in the Code. However, feedback from some respondents also cited barriers to entry which they perceived would prohibit full participation in the current version of the Code by certain types of firms.

Some feedback suggested that the scam risk exposure for firms such as Payment Initiation Service Providers[12], smaller firms and building societies was different than that for current Code signatories. The Code was perceived to be designed for larger firms with little analysis on how it is commensurate with consumer protection policies and initiatives which other types and sizes of firms already undertake. This feedback related, in the main, to business models of building societies, PISPs and electronic money issuers. Some firms felt the Code was too onerous in proportion to the level of APP scams occurring within their respective organisations. In order to comply with the Code, it was suggested that these types of firms would need to invest considerable resource in order to build additional functionality and friction within their systems, as well as training staff and operationalising the Code.

Whilst some firms may have issues particular to their business model, there were some common barriers which were cited in responses, or identified through our wider work, including:

- Behavioural analysis was said to be difficult where transaction volumes are typically low which creates challenges in being able to create a meaningful customer profile;
- Technology changes required to introduce additional controls/warnings can be a challenge for firms, particularly those at the smaller end of the scale or those with limited in house IT resources;
- Feedback on the ability to identify customers who may be deemed vulnerable to APP scams focused on the concerns around the inability for some firms to adhere to provisions around detection and utilising intelligence about customers and transactions. This is particularly the case for firms that enable one-time and specific payments or do not hold a continuous customer relationship, therefore historical transactional data may not be available in the same way it is, for example, current account providers;
- The ability to provide dynamic warnings was said to be difficult to achieve in the absence of transactional or behavioural data to determine which warning should be presented to the customer;
- The ability to provide a 24/7 contact option was said to be challenging where, for example, there is not an existing an option for customers to contact their firm out of office hours;

[12] Firms which enable consumers to make payments from their bank account rather than using a debit or credit card.

- The ability for some business models, given the services they provide, to be able to delay a payment where an APP scam is suspected;
- The implementation of the Confirmation of Payee (CoP) functionality;[13]
- The ongoing uncertainty around the status of the no blame fund; and
- The ability to collate and provide statistics on APP scams to their relevant trade body was considered a challenge as currently, only UK Finance collates these statistics on behalf of its members.

In order for the Code to work as effectively as possible, it should reflect the range of firms operating within the payments system. Involving more stakeholders in the payments ecosystem to work collaboratively will have a number of advantages: improved and greater levels of intelligence about APP scams; a greater number of consumers are protected; better communication between firms; and expedient remediation, to name but a few.

However, the expansion of the number of signatories to the Code has to be balanced against ensuring that the integrity of the high standards of the Code are retained. At the current time, the Code captures over 85% of faster payments, and whilst the LSB is focused on increasing coverage of the Code, we would need to ensure that any proposed amendments to the Code to remove some or all of the current barriers to sign-up do not inadvertently reduce consumer protection. We are also mindful of the risk of creating a two-tier system where different degrees of protections are provided depending on, for example, which firm the customer makes the payment through. This may serve to fragment the Code more generally, lead to greater inconsistencies in outcomes and create confusion for consumers.

**Recommendation**

The Code should recognise the wider range of participants within the payments industry while ensuring that it retains a consistent approach to the standards of protections provided.

**How we will address this**

The LSB will undertake a programme of engagement with firms providing payment services and PISPs to build on our understanding of the challenges faced by some participants in adopting the Code in its current form. This will be used to inform our work to allow for a broader application and adoption of the Code.

One of the key areas of focus for the LSB is increasing participation in the Code. Whilst we have ongoing engagement with firms with regards to becoming signatories to the Code, take up from industry has been slower than we would have expected. While we recognise the challenges that the requirements of the Code can place on some business models, there are a number of non-Code signatories which are signatories to the Best Practice Standards (BPS). These are a voluntary set of standards for firms to follow when processing an APP scam claim which seek to ensure there is a consistent information flow between firms and a faster response times on scam claims. Responsibility for the content and any associated oversight of the BPS, sits with UK Finance, but the requirements are built into the Code.

[13] Confirmation of Payee provision are discussed in further detail in section 4.3 on Prevention Measures.

Given the alignment between the intention of the BPS and the outcomes of the CRM Code, we would call on firms who are signatories to BPS to extend their commitment further and progress to becoming Code signatories.

While we continue to engage with interested firms, ensuring a wider industry approach to tackling APP scams also requires input and support from wider stakeholders. We would welcome further engagement from stakeholders such as the PSR and UK Finance in the role they can play in supporting our work to increase adoption of the Code. In addition, we would remind firms that in line with the approach we take to the Standards of Lending Practice and the other codes of practice which sit within our remit, we now operate an interim registration process for the Code. This approach allows for firms to demonstrate and publicly commit to becoming a signatory at the same time as working towards full compliance within a timeframe set by the LSB. We would encourage any firms which are interested in becoming a signatory to the CRM Code to contact us to discuss registration.

**e. Embedding the Code within firms: governance and oversight**

The Code is silent on expectations around governance arrangements and related controls. In order to ensure greater consistency in firms' approaches in this area, we have identified that the Code would benefit from the inclusion of relevant provisions to address this. In line with the approach we have taken to the Standards of Lending Practice, these new provisions will set out a clear framework for ensuring that the Code is embedded within the culture of the firm from senior management through to customer facing staff via appropriate governance arrangements systems and controls.

As set out earlier in the report, through the course of our work we have identified that there are varying approaches being taken by Code signatories to governance arrangements in relation to the Code. The need to ensure that there is a more formalised oversight in relation to the effective warnings provisions of the Code is an example of this. In addition, the Code references training and awareness in respect of identification of APP scams, but not of the Code itself which we consider to be a gap, given that it is the main instrument used for the remedy of such scams.

There was also feedback via consultation responses to suggest that when a customer reported a scam there was an inconsistent approach across front line staff in terms of understanding and awareness of the Code. Feedback also suggested that this was a repeated experience throughout the process which followed, from branch staff, contact with fraud teams through to final decision letters. This reflects the findings from our themed review of provision R2(1)c[14] which found that:

*'it was not always clear that all staff who are impacted by the Code had received training (…) Firms should consider whether the training programme they have in place is offering protection to customers across all channels…'*

This review also found similar gaps in communication by firms with customers whereby *'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 requirements of the Code.'*

[14] LSB, review of approach to the reimbursement of customers, April 2020

We continue to reiterate and support the best practice identified in our first themed review, namely for firms to conduct fuller, tailored training with staff, to use regular discussion and sessions to upskill staff, and to improve the content of customer communications outlining any decisioning criteria in accessible terms. We continue to work with signatory firms to ensure these measures are put in place and that action plans have been completed to address any gaps identified. Work is also underway on a follow up review to ensure that the actions and recommendations identified through our first themed review have been embedded within firms.

**Recommendation**

New governance and oversight provisions should be introduced into the Code. These will require firms to have appropriate processes, controls and governance arrangements in place, ensuring that there is effective senior management oversight of the firm's adherence to the requirements of the CRM Code.

**How we will address this**

We will undertake work to develop new Code provisions which reflect the approach taken to the Standards of Lending Practice. The new provisions and a timeline for implementation will be shared with firms in due course.

**f. Responsibilities under the Code**

The Code sets out consumer protection standards to help reduce the number of APP scams. To help protect customers, firms that have signed up to the Code commit to: protecting their customers with procedures to detect, prevent and respond to APP scams, providing a greater level of protection for customers considered to be vulnerable to these types of scams and greater prevention of accounts being used to launder the proceeds of APP scams, including procedures to prevent, detect and respond to the receipt of funds from these types of scams. The Code recognises that there are three parties involved in the payment journey: the customer as they authorise the payment; the customer's firm (the sending firm); and the receiving firm (the account to which the money is moved). It sets out that the sending firm is responsible for the assessment of any claim made under the Code. Feedback from existing signatories, as well as consumer representatives, suggested that responsibilities between sending and receiving firms which are signatories to the Code should be reviewed, with the intention of placing greater emphasis on the role of the receiving firms. This was suggested from the perspective of driving greater prevention activity, for example, by working towards better identification of mule accounts (which are legitimate accounts used in the onward transmission of the proceeds of APP scams); improving the processes which allow for the communication between firms; the associated freezing of funds; and the repatriation processes which can only take place once a receiving bank has been notified of a suspected APP scam case.

However, it can also be the case that either the sending or receiving firm involved in the transaction may not be a signatory to the Code. It was suggested by some respondents that such circumstances can lead to scenarios where firms may be working to different endeavours, processes and timelines in the recovery of funds. It was felt that this can make it challenging to communicate consistently between parties and, ultimately, with customers.

Feedback from the consultation did not make it clear whether this same issue exists where both firms are signatories to the BPS. However, there was a general view that receiving firms have less responsibility and, related to this, there were consequent questions raised around the equitable balancing of responsibilities between sending and receiving firms.

At present, the Code recognises that the payment journey entails three main parties, but the orchestration of an APP scam may involve touch-points with various other parties including social media, telecoms and internet providers. Whilst our remit only extends to Code signatories, we note the importance and value of involving a broader range of stakeholders in the prevention dialogue and we would encourage stakeholders to continue work to explore solutions.

The issues raised illustrate the importance of tackling APP scams in a collaborative manner and further emphasise the importance of wider adoption of the Code across the industry, as the LSB cannot bind or undertake oversight activity of non-signatory firms. We are aware that some firms will be applying the Code but have not yet become signatories to it, therefore the LSB does not have any oversight over how the Code is being applied by these firms.

We will undertake work to review the current Code provisions to ensure that they reflect the roles and responsibilities of sending and receiving firms where they are signatories to the Code. As detailed earlier in this report, we will continue to work closely with stakeholders such as the PSR, UK Finance and others to increase overall adoption of the Code.

**Recommendation**

The Code should more fully reflect the roles and responsibilities of receiving firms in the customer payment journey.

**How we will address this**

Given the need to align this recommendation with work to widen the application of the Code, we will include this within our follow up Call for Input.

### 4.2 Customer experience

The consultation questions within this section sought to establish whether the Code has met its objective to increase the proportion of customers protected from the impact of APP scams, both via reducing incidents of scams and by reimbursement, and to determine what the experience of victims of APP scams has been in the year since the Code was launched. Themes which arose included: issues of assessing the effectiveness of Code, particularly in relation to customer reimbursement and the treatment of customers in vulnerable circumstances.

Through the course of this review and our wider work, it has become clear that stakeholders hold a range of views as to what measures are considered to be the key metric(s) to defining the effectiveness of the CRM Code. The Code is predicated on achieving best customer outcomes, with reimbursement constituting one aspect of that. Wider provisions focus on awareness raising and education of customers, detection and prevention of scams, and timeliness and communication between firms and with customers. Shared understanding of success measures and consistent reporting at the industry level is imperative in order to monitor the Code's effectiveness against outcomes, to understand the prevalence and nature of scams and to devise effective interventions.

### a. Defining the effectiveness and success measures of the Code

On the question of whether the Code has been effective in increasing the proportion of customers protected from the impact of APP scams, the majority of responses cited reimbursement levels to evidence their views that the Code has been effective, but that it could go further. Our analysis of data reported by signatory firms for the first 13 months of the CRM Code being in place showed that the total value of CRM cases recorded by the nine signatories to the Code was almost £257 million, of which £106.5 million was reimbursed to customers (41%). In total, just over a quarter were reimbursed in full (27%). A further 19% of cases were partially reimbursed. Altogether, 46% of cases were either fully or partially reimbursed. This is a significantly higher level of reimbursement than the pre-CRM Code industry average, which was 19% by value in the first half of 2019[15].

However, through the course of this review, we discovered that even the measure of reimbursement is a nuanced concept which had not been reported in a uniformed manner by all firms for the period reported. This can therefore affect the accuracy of the data from which we draw inference and highlights the need to accurately define and record the proxy-success measure that has been used to date. Moreover, while data on reimbursement levels is one measure of the Code's effectiveness, it is not the only measure and defining the effectiveness of the Code on the basis of reimbursement data alone is reductive.

There was also a strong perception from some industry respondents that the Code was perceived as a 'refund scheme' by some parties, rather than a contingent model which assesses individual cases and the circumstances which lead to the occurrence of a scam. This perception could perhaps be linked to the focus solely upon reimbursement levels rather than considering those levels within the context of the wider purpose of the Code to reduce the occurrence of APP scams.

Nonetheless, focusing on reimbursement levels alone, and using these as a proxy for the effectiveness of the Code is likely to exacerbate the view that the Code's purpose is for reimbursement alone, and overlooks other important aspects, such as the prevention and education provisions. It is the LSB's view that the effectiveness of the Code should be accurately defined and measured in wider terms to provide meaningful analysis of its effectiveness, including: the impact of its preventative measures to reduce scams happening in the first place; increased awareness of the Code through the consumer education elements; consistency in the application of the Code and wider adoption across industry. We will undertake further engagement with stakeholders on defining the effectiveness of the Code and the associated success measures which we believe go far wider than reimbursement levels.

[15] LSB, Review of CRM Code for APP Scams, data analysis to support Code review, 2021.

**Recommendation**

In order to fully assess the effectiveness of the Code, a series of success measures should be defined, which take account of, but look beyond reimbursement levels.

**How we will address this**

We will issue a Call for Input and undertake stakeholder engagement to inform our work in this area.

### b. APP scams data

Through the course of the data collection exercise in support of this review, we identified issues of consistency with regards to defining and reporting metrics around the Code and APP scams. For example, our data request covered funds returned to the customer under the CRM Code for two different measures. One related to the value of the original money identified and retained by the customer's firm and which was returned to the customer (funds 'repatriated'). The other related to the total value paid back to the customer to reimburse them for the scam (funds 'reimbursed'); this latter figure should include any funds that were repatriated as well as any further money reimbursed to the customer from the firm's own funds. We are aware from our analysis that there is some overlap between (and some potential additionality across) the two measures – reimbursement and repatriation – but we do not know by how much, as the calculation depends on how an individual firm interprets and records that data. For our analysis, therefore, we considered the two measures. However readers should not seek to sum or subtract one set of figures to or from the other. We also found that, in some instances, firms' systems and/or processes did not enable them to capture, and in turn provide, some of the data we had requested. To that end, our work has identified some areas of concern with APP related data, linked to the limitations in the data that some firms were able to provide as well as lack of consistency, across various areas, in interpretation.

There is therefore, a need to set consistent data metrics across all firms so that the Code can be accurately monitored and evaluated. As the Code requires APP data to be collated, a consistent set of data metrics will also be key when considered in the context of widening participation in the Code to ensure that there is consistent interpretation of data across current and future signatories. In turn, consistent data recording and reporting will also support the wider work required around overall success measures for the Code itself.

In addition, we will build a requirement into the Code, via the governance and oversight provisions mentioned above, for signatories to report these metrics to us so that we can monitor and make informed assessments both at the industry level, and about individual firms, with regards to progress against defined outcomes. This will also assist firms to identify gaps in their service or process and in turn should improve outcomes for customers.

**Recommendation**

Work should be undertaken to ensure that there is a consistency of approach and interpretation to APP related data. Data reporting requirements should be built into the Code to support and inform the LSB's oversight work.

**How we will address this**

We will work in collaboration with industry and experts to standardise definitions and measures for the Code to allow for greater consistency in CRM Code data.

We will build in a data reporting requirement into the governance and oversight provisions outlined earlier in the report.

### c. Vulnerable customers

The expected approach to customers vulnerable to APP scams is set out in the Code in SF1(4) and R2(3). These provisions provide for customers to be reimbursed if it would not be reasonable to expect those customers to have protected themselves, at the time of becoming a victim of an APP scam, against that particular scam.

General feedback suggested that the approach taken by the Code to vulnerable customers aligns with, and complements, the existing work on vulnerability within the industry and regulatory spheres. However, there is a need for us to ensure that any guidance issued to firms takes account of the FCA's final guidance for firms on the fair treatment of vulnerable customers which is due for publication in Q1 2021.

There was broad agreement with the principled way in which the Code requires firms to take account of the customer's vulnerability in the context of the circumstances of the scam. This ensures that firms are required to consider how that vulnerability interacted with the specifics of the scam. However, responses to the consultation suggested that the application of the Code's vulnerability provisions were inconsistent at industry level. Stakeholders who work with vulnerable customers submitted evidence in the form of decision letters and communications from firms illustrating inconsistent outcomes for customers who displayed vulnerabilities at the time of being scammed.

This feedback reflects the findings from our themed review on provision R2(1)(c) which found that some firms' assessment processes did not allow for the customer's situation to be fully explored and that the identification of vulnerability and customers' susceptibility to scams was not very well developed. Some consumer representatives reported that in their communications with firms, the onus was often placed onto the customer (who is not always aware that their personal circumstances can be material to the assessment carried out by the firm) or a consumer organisation helping the customer, to get in touch with their bank to disclose that sensitive information. This can lead to inconsistent identification of vulnerability and places an extra burden on customers who are already in a stressful situation.

Feedback from both the consultation and our thematic work has identified that while we have identified inconsistency in application of the Code in relation to vulnerability, there were no concerns with the specific wording of the Code itself. While we do not therefore believe that

any substantive amendments are required to the wording of the Code at the current time, it does reference at SF1(4)(c) industry guidance which, at the time of publication of this report, we understand is under review. In addition, since the launch of the Code, the FCA has issued guidance on vulnerability and there are a range of materials focusing on vulnerable customers more generally. As the BSI PAS 17271 is guidance and as such is subject to review and ongoing updates, we are of the view that reference to it would be better placed in the practitioner guide, which will be more frequently reviewed and updated, as opposed to the Code itself. In addition, we will undertake a review of the practitioner guide to ensure that it aligns with the FCA's final guidance for firms on the fair treatment of vulnerable customers.

As previously stated, our follow up review on R2(1)(c) is underway and will assess how firms have addressed our areas of concerns in this area. We will use the findings from this review to inform whether additional guidance for firms is required.

**Recommendation**

The practitioners guide should be reviewed to ensure that it takes account of developments within the wider regulatory environment in relation to the fair treatment of vulnerable customers.

Reference to BSI PAS 17271 should be moved from the CRM Code to the practitioner guide as it is one example of industry guidance.

**How we will address this**

To ensure alignment with regulatory developments, a gap analysis will be undertaken to ensure that the practitioner guide takes account of the FCA's finalised vulnerability guidance which is due for publication in Q1 2021. As part of this work we will move reference to BSI PAS 17271 from the Code to the practitioner guide.

We received suggestions from some respondents which they felt would enhance the effective implementation of vulnerability provisions. One such suggestion was that the LSB could look to improve data sharing across the industry with regards to victims of APP scams, and those in vulnerable circumstances more generally. We have considered this and we are of the view that any work capturing customers' personal circumstances, including specific vulnerabilities, would need to be carefully balanced with GDPR requirements. It would be outside of the remit of the LSB as an oversight body to develop propositions or functionality which collate customer data and information about their circumstances, and it would be prohibitive for us as an organisation with regards to privacy and consent, given that we do not hold customer information. We are aware that there are commercial organisations which already offer these services.

While we seek to be informed and welcome further dialogue on this matter, we believe that there are other organisations which are better placed to drive this work and we would encourage the industry, with the input from regulators, consumer representatives and other interested parties, to explore how this and other innovations which seek to protect customers, particularly those who are multi-banked, can be achieved.

### 4.3 Prevention measures

In the consultation document, this section sought to establish whether consumer education and awareness campaigns, warnings, and Confirmation of Payee are working effectively to support the objectives of the Code. Outlined below are the themes which arose.

The Code is based upon a contingent reimbursement model and recognises that customers should take reasonable steps to assure themselves that they are dealing with a legitimate third party. Prevention methods, such as effective warnings and Confirmation of Payee, provide customers with additional tools to protect themselves. However, it is imperative that such provisions are given focus and implemented effectively, so that customers are enabled to be vigilant to APP scams.

#### a. Provision of warnings within the payment journey

Figures published by UK Finance showed that, in 2019, well over two-thirds of UK adults (72%) used online banking and over half (50%) used mobile banking.[16] The number of remote banking payments processed via the Faster Payments Service (or cleared in-house by banks) during 2019 increased by 24% to nearly 2.5 billion. The ongoing Covid-19 pandemic with rolling restrictions and lockdowns, coupled with bank branch closures, will likely see this number increase, as consumers who may have previously relied on their bank's branch network migrate to online banking and payments. This shift in customer behaviour reiterates the need to put in place effective preventative measures, particularly online, where the fastest payment transaction growth has been driven.

At present, the Code requires that firms should be able to demonstrate that, where relevant, an effective warning had been provided to the customer and that the warning met the criteria set out in SF1(2)(e). Firms should be able to evidence that the warning was designed and tested in accordance with the Code's requirements and that the warning should have had a material effect in preventing the scam from taking place.

As noted earlier, our themed review uncovered areas where improvements are necessary relating to: effective warnings not being provided in some instances; a lack of defined assurance programmes or oversight within some firms; arbitrary thresholds being used and the need to further develop warnings.

Consultation feedback also echoed similar themes, noting the need to balance alertness with the risk of creating customer apathy due to frequency of warnings. There was also a view expressed by industry and consumer representatives, based on direct experience of working with customers, that where even well designed warnings are not effective, this should indicate the presence of vulnerability. This was predicated on the view that if effective warnings prevent most people from proceeding with scam payments, it is possible that the proportion of people who then do fall victim to a scam may be in vulnerable circumstances at the time, or the nature of the scam is such that they have reasonable basis for believing the payment to be genuine, despite the warning.

[16] UK Finance, UK payments market summary 2020

We are also mindful of the increasing range of participants and diversity of business models within the payment journey, such as PISPs. Open banking has enabled customers to make payments via authorised PISPs rather than directly with their bank. This means that responsibility for providing any warning would sit outside of Code signatories' control. We are aware of anecdotal evidence that firms are starting to see a small number of these payments reported as APP scams. However, responses focusing on this area were light and we therefore will need to undertake further work to understand the prevalence of the issue. While PISPs currently sit outside of the Code, as set out above, their integration with the CRM Code is an area which we will be exploring with a view to widening participation in the Code and we will consider this issue alongside this specific workstream.

Our thematic review work has identified issues with firms' implementation and application of the requirements of the Code in relation to the provision of warnings, rather than the specific wording of the Code itself. Firms have individual actions in place to address the LSB's areas of concern and we will consider whether further guidance would support firms in achieving the necessary outcomes under the Code. We also believe that the inclusion of requirements around governance and oversight within the Code will further drive greater consistency in the design and review process for warnings. However, this approach will be informed by our ongoing work, as well as any other significant external developments which may require us to review the Code as needed. The research work being undertaken by the OBIE in this area will also provide useful insight for firms and we will engage with OBIE to understand how the findings can be reflected within the practitioner guide.

**b. Confirmation of Payee**

The Confirmation of Payee (CoP) service is managed by Pay.UK which has developed the rules, standards and guidance that enables the service to run. It is a way of giving customers greater assurance that they are sending their payments to the intended recipient and can help avoid payments being accidentally misdirected.

The PSR issued a direction for the UK's six largest banking groups, covering around 90% of bank transfers, to fully implement CoP by 31 March 2020. However, in light of the Covid-19 pandemic, the PSR issued an update postponing any formal action in respect of delays to the introduction of CoP until 30 June 2020 and setting out that firms must take appropriate steps to roll out CoP even if it means they do not meet the original deadline. While some firms beyond the six banking groups directed by the PSR have voluntarily introduced CoP, further work is also expected to expand the coverage of CoP to other firms. In addition, one Code signatory has implemented CoP voluntarily. We understand that Pay.UK is now further developing CoP as a second phase of activity to create the capability for all account holding PSPs to participate.

As the Code currently stands, provision SF1(3) has a holding date for the implementation of CoP. This functionality elicited strong support in the majority of consultation responses, with the recognition that whilst CoP is not a panacea to stopping all APP scams, it nonetheless provides protection by design. Whilst CoP is in place across a majority of signatory firms, it has yet to be made effective within the Code. Implementing the CoP provision in the Code would mean that whether the customer took heed of the CoP outcome could be taken into account during the firm's subsequent assessment process.

However, we are also mindful that not all signatories to the Code were subject to the PSR's direction. It will therefore be important to ensure that the implementation of the CoP provision would not mean that firms who have not yet adopted CoP, or who fall within phase two of Pay.UK's work in this area, are in breach of the Code, or that the provision creates a further barrier to entry for non-signatories.

Subject to the above considerations, we did not receive any feedback which suggested that CoP should not be made effective within the Code. As part of our Call for Input, we will therefore set out a date for implementation of CoP within the Code, which will allow time for engagement with the PSR and Pay.UK with regards to progress of the second phase of CoP implementation activity. As part of this work, we will also ensure that the wording does not prohibit firms who are not yet able to implement CoP from becoming signatories to the Code.

**Recommendation**

The wording of the Code at SF1(3) should be reviewed so that the provision becomes effective within the Code for those firms who have implemented Confirmation of Payee.

**How we will address this**

We will include a date for implementation in our Call for Input and will engage with the PSR and Pay.UK with regards to progress of the second phase of CoP implementation activity.

**c. Customer payment journey**

A key message from the responses was a recognition that whilst customer care and firm actions are vital after a scam has occurred, in order to remedy the customer and to try to recover funds, a greater focus needs to be placed upstream in the prevention of scam activity, both at the industry level and during the course of the payment journey. Moreover, as a matter of good design, it should be ensured that preventative and protective measures are in place at every point in the consumer payment journey.

As part of our data request, signatory firms were asked to provide information which sought to understand from a MI perspective, what APP scam prevention activity firms had undertaken. One such measure, of the number of transactions abandoned, was used in the analysis as a proxy for prevention levels. However, it should be noted that this was an experimental measure to determine whether it is a useful metric for prevention levels, as transactions may have been abandoned for reasons other than the provision of a warning or other intervention. In addition, not all firms captured this information and there are therefore limitations on how much reliance can be placed upon this data set. Further detail can be found in the accompanying report.

Nonetheless, analysis of abandoned transactions showed variations in the value of scams recorded, which suggests that this type of data can provide insights into how prevention measures are working. We would therefore encourage firms to continue to engage with learning and analysis of different types of data to improve prevention measures.

Responses to the consultation also looked outside of the Code at the wider ecosystem and a number of initiatives were suggested by several stakeholders which could help to detect and prevent criminal activity at the system level. Many respondents advocated for greater collaboration and work with cross-sector stakeholders, such as that being undertaken by Stop Scams, to tackle the impact of issues created by data breaches which enable some scams to happen. In addition to traditional financial services and consumer groups, other suggested stakeholder groups which play an important role in scam detection and prevention activities included the Information Commissioner's Office, telecoms, social media platforms and utilities. The LSB is supportive of initiatives which seek to address APP scams at a cross-sector and system level and we would welcome further engagement as work develops in this area.

**d. Consumer awareness**

Responses about customer awareness focused on three aspects which are covered in more detail in this section: awareness of APP scams, of the Code and of consumer responsibilities.

The majority of respondents viewed customer awareness of the Code itself as low, further stating that the customer information document for use by consumer organisations was not widely known either. It was suggested that this was further exacerbated by poor communications by firms with their customers, especially when it came to outlining decisioning criteria after investigations into a scam case. As we have stated earlier, our review work identified that improvements were necessary in communicating with customers and firms have action plans in place, where required, to address this.

There were suggestions that the LSB could undertake a consumer awareness campaign and use non-financial platforms, particularly where customers are likely to be manipulated and scammed, in order to reach customers. It was proposed that enhanced scam risk customer messaging could appear on platforms where there is a high propensity to scammer focus, such as dating websites, HMRC or other governmental departments, or via organisations that provide critical illness patient and family support. We have considered these suggestions carefully and we are of the view that this type of work is outside of the remit of the LSB, as we do not work directly with consumers. This type of work would, we believe, be better placed with other consumer facing organisations, which have the necessary experience and awareness amongst consumers to ensure its effectiveness. We will, therefore, share the findings from this review with relevant stakeholders and would welcome work which may evolve from this.

As previously discussed, there was also a view to suggest that where customers are aware of the Code, they perceived it to be a 'refund scheme' as opposed to a 'contingent model'. It was suggested that while the Code has driven significant activity through firms, there remains a gap in customer understanding of the role they play and the corresponding actions they take and how these actions can have a bearing on the success of APP scams.

At the core of many APP scams are advanced social engineering methods which range from mimicking legitimate company communications, through to forming romance relationships, so that customers are manipulated, sometimes repeatedly over a period of time, in order to be coerced into conducting such fraudulent payments. It is important that customers have the knowledge and tools to be able to protect themselves against being scammed. Customers need to know what steps to take when they are unsure of a payment, and moreover, have recourse to an appropriate level of support when they do fall victim to a scam. Additionally,

consumers may unwittingly find themselves being targeted and subsequently lured into becoming 'money mules'. Increasingly, social media is being used as a recruiting ground by scammers. Consumer awareness of the recruitment techniques used and the potential consequences of knowingly being a money mule, including difficulty in opening bank accounts and obtaining future borrowing, as well as the potential for criminal prosecution, appears to be low.

We are mindful that the Code was written for firms, however the customer facing document was intended to provide information on the Code and to guide customers to appropriate support, where needed. We will therefore ensure that we continue to engage with consumer organisations and keep them informed of developments with respect to the issue of increasing customer awareness of the CRM Code and APP scams.

We are also mindful that this may result in greater signposting of customers to the LSB's website and information provided there about the Code. In light of this, we will undertake a review of the content of the information for customers document, which is hosted on our website.

**Recommendation**

The information for customers document should be reviewed to ensure that it takes account of any relevant changes which may result from our wider review of the Code. As part of this, consideration should be given to how awareness of the document itself can be improved.

**How we will address this**

We will undertake a review of the content of the information for customers document to ensure that the content remains appropriate and that it reflects any relevant amendments to the Code. Work will be undertaken with stakeholders including firms, consumer organisations and the wider industry to raise awareness of the document and how it can be used more effectively.

### 4.4 Resolving Claims

This section of the consultation sought to establish what challenges firms face when making a decision to reimburse customers, including in relation to how that reimbursement is funded in the case of 'no blame' scenarios. Themes which arose in this section centered around threshold values with regards to reimbursement, access to funds by firms in no blame scenarios and a gap in after care actions for customers.

#### a. Lower value scams: Purchase scams

There was considerable feedback from financial service respondents who called for the exclusion of purchase scams from the Code, stating that they take a disproportionate amount of time to assess, are typically for lower value payments, yet are resourced by skilled fraud teams, and time spent on such cases can distract from more focused attention on customers who have suffered larger monetary losses.

Our analysis shows that the purchase scams account for 59% of the total volume of cases, but only 14% (£37.2million) of the total losses (£257million) incurred by the signatory firms. From this we can deduce that a significant number of customers are incurring losses from purchase scams and excluding these from the Code would result in a withdrawal of the Code's protections from significant populations of customers. Exclusion of purchase scams from the Code could also have further unintended consequences, for example, on low income customers for whom even a figure deemed to be a 'lower value payment' can have a significant impact on their financial situation. The reduction in protections which would result from any exclusion of specific types of scams from the Code may also be exploited by scammers, who may consequently increasingly target specific types of scams or customers.

We were not persuaded that purchase scams should be excluded from the Code simply on the basis that they represent the highest volume of cases being assessed. We are of the view that the level of care and focus given to a customer who has become a victim of a scam is a matter of after-care policy, and not a reason to exclude scams from the scope of the Code. It is the nature of a scam and a customer's circumstances at the time of the scam which should be in consideration when assessing any claim, as opposed to the monetary sum of the loss.

**b. Lower value scams: Monetary threshold values driving policies**

Through the course of our work, we are aware that some firms employ policies with regards to placing varying thresholds on automatic reimbursement of customers, so that when the value of a scam is below a given level, the customer will be automatically reimbursed.

We also noted instances of the policy of implementing monetary threshold values within our recent themed review on the effective warnings provisions of the Code. We noted that that thresholds were being applied, usually based on monetary amounts, which resulted 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 leading to the warning becoming ineffective, we were unable to evidence the basis for these thresholds.

Feedback via the consultation suggested that some firms wanted to focus their resources on prioritising higher value scams or to be able to provide more focused support for specific customers, such as those who had lost large amounts like life savings in the form of pensions, housing deposits and investments. In a similar vein, there were some feedback to suggest that the LSB could look to formalise the practices of excluding lower value scams from the scope of the Code, by amending the Code to include the introduction of a 'de minimis' value, proposed at £250, below which all customers would automatically be reimbursed. As before, it was suggested that this would allow a greater focus of support for those customers who have suffered larger monetary losses.

Based on our data analysis, it is apparent that the average values of individual cases were higher for those involving impersonation scams, and especially investment scams, when compared with other types, such as purchase scams. As expected, investment cases were associated with the highest average sums, at £9,943 per case. At the other end of the range, purchase scams were valued at an average of £509. Scams involving impersonation of police or bank staff were in the middle of the range, with an average case value of £4,424.

We are mindful that exclusionary policies have the potential to create unintended consequences. Such policies can be exploited by scammers who may target particular firms with repeated low value scams knowing that such transactions will not be investigated in-depth. This can lead to victims, who while being reimbursed for monetary losses, are not supported appropriately, particularly if they were targeted to exploit vulnerabilities, and who may therefore become victim to repeated scam attempts. This could exacerbate their detriment further, particularly where a firm may employ automatic reimbursement policies for a defined number of smaller amounts with the conditionality that it excludes the customer from future reimbursement.

We note the perceived advantages of automatic reimbursement for lower value APP scams, in that they can provide more expedient remediation for the customer. However, we are not convinced that the long term unintended consequences of such policies on the customer and impact at the industry level are mitigated by the controls in place at the moment. We are concerned that we noted an inconsistent approach to such policies and their associated conditionalities through our previous review work, which could further confuse customers and fragment industry response to this issue, particularly as we strive to harmonise sending and receiving firms' responsibilities.

We will therefore not proceed with the suggestions to apply Code provisions only to those scams which are above a given threshold value. We will, however, continue to closely monitor approaches to automatic reimbursement and the application of thresholds through our work to ensure there are no unintended consequences or customer detriment.

**c. No blame fund**

At present the Code refers to the application of the 'no-blame' fund in the following scenarios:

ALL2(3) Where neither firm involved in the relevant payment journey has breached any provision of SF, the customer's firm who has administered the reimbursement should apply to [the no-blame fund] to recoup the cost of reimbursement.

ALL2(4)(c) Where neither firm has breached any provision of SF and the customer is found to have been vulnerable, the customer will receive 100% reimbursement. The customer's firm who has administered the reimbursement should apply to [the no-blame fund] to recoup the cost of the reimbursement. That is, where neither party is liable for the success of the scam, or the customer is assessed to have been vulnerable.

While reference to the fund is included within the Code, responsibility for the governance and operation of the fund sits with UK Finance. In December 2020, the industry announced that it had agreed to extend the fund until 30 June 2021. Given the level of interest from regulators, media and the wider industry, feedback on these provisions focused on the ambiguity around the continued existence of the fund.

There was also a substantial number of respondents who supported a self-funding proposition to be reflected in the Code. This would mean that if the outcome of the firm's assessment of a CRM Code case was that it was a no blame scenario, the firm would reimburse the customer rather than applying to the central fund. Additionally, a number of other models of funding were also proposed including:

- Holding firms which receive the funds held liable for allowing the opening of a fraudulent account;
- Both sending and receiving firms contribute 50% of losses unless one firm can prove the other was solely at fault;
- Extending existing levies as well as funds from dormant accounts to fund a centralised no blame fund; and
- Convening a larger group of non-financial stakeholders to contribute to funding from non-banking sectors which enabled such scams to occur, including e-commerce sites, social media and telecoms for example.

We welcome the continued discussion and work within industry to develop a longer term sustainable mechanism for reimbursing customers in a no blame scenario. The LSB's position remains that regardless of the funding mechanism, the Code requires that customers in a no blame situation should be reimbursed. While work continues on a sustainable mechanism for such cases, we will amend the Code to recognise that firms can 'self-fund' no blame cases or can continue to use the central fund. We believe that this amendment is necessary to future proof the Code and ensure that the uncertainty around the continuation of the fund does not prohibit a wider range of PSPs from becoming signatories to the Code and that regardless of the funding mechanism, customers in a no blame scenario are reimbursed.

**Recommendation**

Provision ALL2(3) of the Code is updated to reflect that firms may fund 'no blame' cases from the central fund or self-fund the reimbursement of customers who are assessed to be in a 'no blame' scenario.

**How we will address this**

We will issue updated wording to the Code in due course.

### d. After Care

The Code requires that firms 'should have processes and procedures in place to help with customer aftercare' (GF (3)). This section received mixed feedback. It was positive to note that firms are referring cases to their specialist vulnerability teams, where it is identified as a factor, and furthermore many firms came forward to express ideas around more collaborative work with the consumer sector. For example, there were suggestions around using centralised monies to fund specialist organisations where firms can triage those customers who have been victims of APP scams and need further, specialised support.

However, feedback from organisations which currently work with consumers who have fallen victim to APP scams was less positive. This was due to a number of factors that have already been discussed, including how communications, particularly decisioning letters, were poorly outlined and often did not cite the Code or provide information about the customer's further rights, such as the recourse to FOS. It was reported that the impact of this can cause people to spiral into further debt, cause distress and fracture relationships, which firms were said to be unaware of.

Our review of R2(1)(c) also identified that further work was required to ensure that customers were aware of the basis on which the decision had been made to decline reimbursement and the support which is available to customers who have fallen victim to scams. We will continue to work with industry and stakeholders to drive improvements to the process and aftercare communications that firms have in place, but at this stage, we do not believe that further changes to the Code's wording are required.

## 5. Next steps

When we set out to review the CRM Code, we wanted to better understand how the Code had been implemented in its first year, how it was working and importantly, whether improvements were required to ensure it works more effectively. Our recommendations have been informed by consultation responses and the findings from our wider work. Our follow up review on provision R2(1)(c) is underway and is due to report in early summer 2021. The findings from which will further inform our understanding of how signatories are applying the Code's requirements and whether further work on the Code itself may be required.

Responses to the consultation identified that the Code represents a significant step forward to address what was a clear gap in consumer protection but that more needs to be done to ensure that is applicable to the wider range of firms, beyond current signatories, which provide payment services to consumers. Our recommendations have also identified where further work is required to ensure the Code is fully embedded within firms or to seek further input to inform our thinking on particular provisions. We have also looked beyond the Code requirements and have considered what the success measures for it look like and how we will work with industry to define these measures.

While we have identified a number of other issues which arose with regards to improvement of Code protections. These issues, discussed in the body of the report, remain agnostic to the legal or regulatory status of the Code and need to be addressed in order to strengthen the protections customers are afforded when using faster payments. This report sets out recommendations which will be driven by the LSB but, as we have identified through the course of this report, will require the input of stakeholders to inform our approach. We will begin work on the recommendations as a matter of priority and will publish a timeline of work by the end of February 2021 and a Call for Input by the end of Q1 2021.