Lending Standards Board

Call for Input: Findings Report

Contingent Reimbursement Model Code for Authorised Push Payment Scams

November 2021

Contents

1. Executive Summary

In January 2021, we published the findings from our consultation on the Contingent Reimbursement Model Code for Authorised Push Payment scams (the CRM Code or the Code). In addition to the recommendations outlined in our report, there were some topics which were identified as being potentially detrimental to customers, and which it was felt that the Code did not adequately cover. These formed the basis for a Call for Input which was issued in March this year. The Call for Input sought to home in on specific topics for which there was not sufficient evidence submitted in the full review to enable us to form policy and Code decisions.

The Call for Input ran from 31 March - 26 May 2021 and focused on the following areas:

- how the scope of the Code should more fully reflect the evolving nature and complexity of APP scams to ensure that it is able to remain relevant and in line with developments in the wider payments landscape;
- that the Code should recognise the wider range of participants within the payments industry whilst ensuring that it retains a consistent approach to the standards of protections provided; and
- that the Code should more fully reflect the roles and responsibilities of receiving firms in the customer payment journey.

a. Summary of findings and next steps

We received submissions from a range of stakeholders who identified that APP scams continue to evolve as scammers employ ever more sophisticated approaches to scam customers. The most commonly cited newer scams were those that employed a multigeneration model, these scams, sometimes referred to as 'friends and family scams', typically involve a customer being duped into increasing the number of transactions and/or payees involved in the scam. Firms also reported seeing an increase in scams involving cryptocurrency or forex.

The feedback provided identified a trend of APP scams moving from originating amongst CRM Code signatories, to non-signatory firms. This leads us to conclude that the preventative elements of the CRM Code are acting as a deterrent for scammers, whilst providing greater protection for customers of signatory firms. However, in order for the Code to remain effective, it has to take account of the fact that scams will, unfortunately, continue to evolve.

A common feature of the newer scams highlighted is that they challenge the three-party approach which forms the basis of the Code. We were told that the more elongated payment journeys, involving multiple movements of funds, slows down investigations and also makes funds harder to trace at the point the scam is reported. However, firms were seeking to investigate such scams under the Code but were unclear as to whether such scams were in scope.

Having considered the submissions to the Call for Input and current practice, we are of the view that the investigation of multi-generation scams are captured within the scope of the Code. We will therefore seek to update the Code, along with the practitioner guide, to reflect our expectations in this area.

Signatory firms also told us that they were seeing an increasing number of scams involving cryptocurrencies, particularly as a final destination for funds, but from the feedback received, we are unclear of the scale of the issue. Whilst the Code applies to Faster Payments made in GBP-denominated UK domiciled accounts, cases involving cryptocurrency would still involve an initial payment being made by a customer from their account held with a signatory firm prior to conversion to cryptocurrency. However, firms identified that these scams were not always being captured within relevant APP scam data and/or were unclear as to whether this data should be captured within CRM Code reporting. In addition, clarity was sought as to whether relevant cases should be assessed under the Code.

We will engage with industry with a view to understanding how available data can be used to provide a more detailed picture of the volume of APP scams involving cryptocurrency. This will be used to further inform where guidance for firms may be required to support firms in assessing such cases under the Code.

b. Increasing participation in the Code

Increasing participation in the Code continues to be a key area of focus for the LSB. Whilst take up from industry has been slower than we would have expected in that regard, we recognise the challenges that the requirements of the Code can place on some business models.

The responses received represented a wide range of business models, some of which cited perceived common barriers and adjustments that would be needed to the Code to enable participation. We are mindful of the need to ensure that the Code remains consistent in its approach to protecting customers while ensuring that a wider range of firms, beyond the largest banking groups, are able to become signatories to it. However, this has to be balanced against feedback which suggested that the Code may not be the appropriate vehicle for all participants within the payments sector.

We have outlined the high-level areas where amendments are required within this report and will look to initiate these changes to the Code as one of our next steps. As part of wider updates to the Code, we will also activate the Confirmation of Payee (CoP) provisions for those firms who are able to offer this functionality.

c. Roles and responsibilities

The majority of industry respondents told us that receiving firm accountability was lacking in the resolution of APP cases, and this was even more prominent where the receiving firm was a non-signatory to the Code.

The Code sets out a three-party liability model which captures the customer, sending and receiving firm. However, feedback suggested that the model, as it applies to sending and receiving firms, should be reviewed to ensure that receiving firms have greater accountability for their role in the payment journey. Accountability for the scam was described in terms of the acceptance of liability and subsequent allocation of reimbursement, as well as failure in upholding preventative elements as the recipient firm had allowed mule accounts to exist through which the funds could pass.

We will undertake work with industry to explore the issues outlined in this report which will be used to inform where updates may be required to the Code.

d. Customer experience

Customer awareness of APP scams also continued to remain a high priority across stakeholders, this included the need for both consumer awareness of APP scams as well as support for customers when they find that they have fallen victim. It was widely agreed that consumer organisations play a vital role in both of these situations, however some of the feedback received suggested that there was not always consistent information being provided to customers.

Whilst the LSB does not work directly with consumers, we are aware that they are directed to, or find themselves coming across, our information when they are researching matters relevant to our Standards and Codes. To that end, we have a customer information document which accompanies the CRM Code and sits on our website. Feedback suggested that whilst the information within it is accurate, it is not very engaging to customers. In our January report, published following our full review of the CRM Code, we committed to reviewing and updating this document.

e. Next steps

As set out in the main body of this report, we will:

1. Update the Code and practitioners guide to reflect that multi-generation type scams are within scope of the Code.
2. Engage with UK Finance to ensure that relevant supporting processes, such as those captured within the Best Practice Standards, are able to take account of the updates to the Code.
3. Engage with industry to further understand how APP scams data involving cryptocurrency is recorded and what data is available to support our understanding of the scale of the issue.
4. Engage with industry to build on information provided via the Call for Input with a view to developing guidance to support firms in assessing cases involving cryptocurrency under the Code.
5. Update the Code to enable a broader range of firms to participate in it while maintaining a consistent approach to consumer protection. We will publish further information regarding these updates shortly.

6. Continue to actively engage with industry with a view to increasing the number of signatories to the Code.
7. As part of wider updates to the Code, we will implement the relevant Code provisions on Confirmation of Payee.
8. Continue to engage with the PSR as its work on phase 2 of Confirmation of Payee progresses with a view to whether the Code should include provisions to capture Secondary Reference Data provisions.
9. We will undertake further work with Code signatories to ensure that the Code sets a fair balance between sending and receiving firms. This work will inform where updates are required to the Code.
10. Progress with our work to update the customer information document to improve its accessibility and useability.

2. Background

The CRM Code was launched in May 2019 and sets out good industry practice for preventing and responding to Authorised Push Payment (APP) scams.

Currently, there are nine signatory firms, comprising 20 brands, 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.

Since taking on responsibility for the governance and oversight of the Code in July 2019, we have undertaken two full thematic reviews, together with a follow up review of the customer's reasonable basis for belief, the summary report for which was published on 16 June 2021. Alongside our oversight work, we have also undertaken a full review of the CRM Code (the Code review) with the subsequent report published in January 2021.

As a result of the Code review, we updated the Code in April 2021 to include new governance and oversight provisions. These changes also addressed gaps we identified through our oversight work, to ensure that Code related policies and processes are formalised, and customer facing members of staff in firms have greater knowledge and awareness of the Code. In addition, we have also taken the opportunity to update relevant sections of the Practitioner Guide to provide further guidance to firms following our thematic and follow up reviews.

There was substantial feedback from respondents to the Code review who supported a self-funding proposition, for reimbursement of customers, to be reflected in the Code. Wording was adjusted to reflect this feedback and to make it clear that firms could self-fund no blame cases rather than being required to call on the no-blame fund. Earlier this year, UK Finance announced the end of funding arrangements for the central funding pot related to 'no blame' scenarios.[1]

However, there still remains more for us to achieve from the recommendations made in our January report. This includes a focus on assessing the effectiveness of the Code through the development of success measures, work on which has recently begun. This piece of work is inter-related to the work currently being scoped by the Payment Systems Regulator (PSR) which launched a Call for Views on APP scams as part of its activity around tackling payment fraud.

[1] https://www.ukfinance.org.uk/press/press-releases/uk-finance-calls-for-cross-sector-collaboration-to-stop-app-scams

The Code is currently the only regulatory tool in place which seeks to ensure that there is a consistency of approach when detecting and preventing APP scams, and where required, reimbursing customers who have fallen victim to APP scams through no fault of their own. As the themes covered within the PSR's Call for Views overlap with many of those covered within our Code review and associated activity, we continue to engage closely with the regulator as our respective workstreams progress, and we look forward to the outcome of its Call for Views.

We received 14 written submissions in addition to engagement with stakeholders around the topics highlighted above. We also conducted several bilateral meetings with organisations upon request to discuss the topics most pertinent to them. This report outlines the findings from the Call for Input as well as our proposals for further work across the key areas highlighted within it.

3. Key findings

a. The evolving nature and complexity of APP scams

Within the Call for Input we sought to gather further information on the issue of emergent scams to understand their nature and prevalence and to enable us to understand how these should be taken into account within the Code.

Overall, whilst prevalence figures were largely absent from the responses we received; we were provided with vital insight into the nature of such scams. In this section we have outlined some of the information we have garnered around multi-generation APP scams which, alongside scams involving cryptocurrencies, were the most frequently cited emergent scam type. We have set out our view on how these cases should be considered under the Code, recognising that we will need to engage further with industry where this impacts on existing processes.

The feedback provided demonstrated a trend of APP scams shifting from originating amongst CRM Code signatories to non-signatory firms and this was prevalent, for example, within multi-generation scams.[2] While this leads us to conclude that the preventative elements of the CRM Code act as a deterrent for scammers, and provide greater protection for customers of signatory firms, it underlines the point that in order for the Code to be as effective as possible, it requires greater participation from Payment Service Providers (PSPs). While we continue to actively engage with industry and have onboarded new firms since taking on responsibility for the oversight of the Code, ensuring a whole 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.

[2] For the purposes of this report, non-signatory firms are defined as those firms who could sign up to the Code, as drafted, but have not yet done so.

b. Multi-generation APP scams

The key features of multi-generation scams are the elongation of payment journeys and/or the involvement of multiple payment channels. These scams, sometimes referred to as 'friends and family scams', typically involve a customer being duped into increasing the number of transactions and/or payees involved in the scam (for example, being convinced to transfer funds to a family member who in turn is asked to further forward them, onto the scammer's account). While the funds have been moved to a trusted third party, in that they are a friend or family member, the payment has left the control of the payee. This approach seeks to evade the detection and preventative measures of the Code and creates challenges for the assessment of such cases under it, as the Code assumes that there will only be three parties involved in the payment journey: the customer; the sending firm; and the firm which receives the funds.

From the responses we received, it appears that there are a number of different scenarios being reported to firms for assessment under the Code. These scenarios may involve some of the following:

- where the person reporting the scam is the customer who has had direct contact with the fraudster and contacts their bank to raise a case under the CRM Code;
- the scam is reported by the person who has been asked to move funds onwards to the fraudster, e.g., a friend or family member;
- the friend or family member may move on just the funds they have been asked to or in some cases, they are drawn into the scam and also move their own funds; and
- both signatory and non-signatory firms may be involved at various points of the payment journey.

c. Multi-generation scams and the Code

Under the Code, a payment journey begins when a customer initiates a payment, adds a new payee, or amends an existing payee on their account followed by all the steps taken to authorise that payment. The scope of the Code is limited to the first movement of funds from the customer's account to another person, but it makes the assumption that the person who receives the funds is the scammer. It also assumes that the customer reporting the scam is the person who has fallen victim to it and has ultimately moved money to the fraudster. As such, the Code requires the customer's firm to carry out the investigation, but this is challenging where the original customer who has fallen victim to the scam may not be so readily identifiable, for example, where instead the family member or friend who passed funds through to the scammer raises a claim under the Code with their own firm.

This means that assessing the circumstances around the scam is more difficult and in circumstances where the friend or family member has only moved on the received funds, they have not suffered a monetary loss, but they have, arguably, been involved within the overall scam.

The situation can be further complicated where the friend or family member is subsequently drawn into the scam which results in them moving on both the received funds and their own. This can mean varying outcomes for customers, as the investigations will take account of the current Code requirements for payment journeys, with sometimes the added complexity of both non-signatory and signatory firms involved in the payment journey.

The investigation of a multi-generation scam requires engagement to take place between the originating firm and all of the subsequent payees' firms through whose accounts the funds may have passed. In some circumstances, this can result in the freezing of funds within the first-generation recipient account or the locking down of a customer's banking facilities which is not a malicious account. This has a number of consequences for the individuals who have been caught up in the scam, as well as causing delays to the ultimate receiving bank being put on notice of the scam, which provides additional time for the fraudster to move the funds away. While the communication between firms is underpinned by the Best Practice Standards (BPS),[3] elongating the payment journey can have implications on the timescales and processes for communications between firms regarding the resolution of APP scams.

d. Application of the Code to multi-generation scams

Responses to the Call for Input indicated that firms are seeking to assess such cases under the Code but as it is based on a three-party model, it may not always be clear to firms how such cases fit within the Code.

In the example where a customer receives funds from another customer with whom the scam originated, and then passes these funds to the scammer, the intermediatory customer's firm plays a role in both the receiving and sending of funds. As their firm communicates with other involved firms in the payment chain, it must identify itself both in relation to the reception or execution of the payment and its sequence in the scam. Not only do these cases present challenges for firms, but they can also lead to variable outcomes for customers. They may, for example, be directed back to the bank of the person on whose behalf they have forwarded on the funds, particularly where they have not moved any of their own funds on and therefore not suffered a loss.

We were told that firms also face challenges investigating these scams end-to-end, as depending on whether or not the scam originated with their customer, they were reliant on communications from earlier payees, which may not always be forthcoming. Feedback highlighted that the inter-bank communication issue affected not just the investigation itself, but also repatriation and general communications. While the Code may not have been drafted with multi-generation scams in mind, firms are attempting to investigate and include all parties within this process, ultimately with the aim of reimbursing the customer. However, we recognise that firms require clarity as to our expectations in this area and how such cases should be treated under the Code.

[3] The BPS 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 time on scam claims. Responsibility for the content, and any associated oversight of the BPS, sits with UK Finance but the requirements of the BPS are built into the Code.

Having considered the submissions to the Call for Input and current practice, we are of the view that the investigation of multi-generation scams is captured within the scope of the Code. In reaching this conclusion we have taken into account the current wording of the Code which states that:

DS1(2) … (a) APP Scam Authorised Push Payment scam, that is, a transfer of funds executed across Faster Payments, CHAPS or an internal book transfer, authorised by a customer in accordance with regulation 67 of the PSRs, where:

(ii) The customer transferred funds to another person for what they believed were legitimate purposes, but which were in fact fraudulent.

We have taken into account the circumstances surrounding the movement of the funds to, for example, individuals who are known to the originating customer, who in turn move the funds on. In these circumstances, the customer has moved funds to a friend or family member for what they believed were legitimate purposes.

The underlying assumption of the Code - that the funds will move from the customer directly to the scammer - is therefore challenged by multi-generation scams. While the customer has initiated a payment which ultimately ends up with the scammer, the payment journey has been intentionally elongated to involve more than one individual. We do not believe that the intention of the Code is to prevent cases involving customers who have fallen victim to an APP scam from being assessed under it simply because the scam has increased in complexity. We will therefore seek to make reference within the Code, supported by an update to the practitioner guide, to reflect our expectations. These amendments will be actioned in due course; however, we have set out some overarching principles below.

When assessing such cases under the Code, firms should take into account that:

- A firm's assessment of the case should fully explore the circumstances of the scam which looks beyond where the scam originated to enable the firm to fully consider the individual customer's case.
    - When a customer reports an APP scam, it should be considered in the round and that the scam may not be limited to a singular transaction or payee and may involve heavy manipulation of the customer.
    - Consideration should be given to the full circumstances of the scam and the point at which the funds moved out of the customer's control, i.e. because the funds were moved to a friend or family member does not, in our view, preclude it from being considered under the Code.
    - Whether the scam originates at a Code signatory or otherwise, when a customer of Code signatory reports the scam, we would expect signatory firms to be assessing the case under the Code. It is through the assessment of the claim that the firm will be able to establish the full circumstances of what has happened, which includes whether the customer reporting the scam has incurred any loss.

- Gaining a holistic picture of the scam and circumstances may require information to be shared which is held by other firms and their customers.
    - Firms should consider whether current processes can be adapted to allow for more effective communication between the firms involved in the payment journey.
- Aftercare provided to customers should take account of the circumstances which surrounded the scam.

e. Processes supporting the application of the Code

Key to the effective assessment of APP scams with elongated payment journeys is the need for efficient communications between firms involved in the scam. This is particularly important for signatory firms who are involved but are perhaps not the originating firm. Moreover, expedient tracing and securing funds intended for scam purposes also requires similar efficient processes between firms across payment journeys.

At present, communication about APP scams between firms happens via processes associated with the BPS. We will engage with UK Finance, as the owners of the BPS, to ensure that the proposals we are making around multi-generation scams and communications between firms are reflected within the processes referenced within the BPS.

Summary of next steps and actions

1. We will update the Code, and practitioners guide, to reflect that multi-generation type scams are within the scope of the Code.

2. We will engage with UK Finance to ensure that relevant supporting processes, such as those captured within the Best Practice Standards, are able to take account of any amendments made to the Code.

4. Cryptocurrency and APP scams

It is apparent from a number of responses, together with our own intelligence, that there has been a rise in scams involving cryptocurrency, particularly over the last 12 months. The two main scam types identified by firms were either where the scammer had taken over the customer's crypto-wallet and forwarded the relevant currency onto untraceable accounts or convinced the customer to pay directly into the fraudster's cryptocurrency account for goods or the promise of investments which did not exist. Given the fast-paced evolution of such scams, firms reported that these types of transactions can become harder to spot. We were told that firms may struggle to differentiate between transactions which need to be stopped and legitimate cryptocurrency transactions, the latter resulting in unnecessary friction to the payment journey. This can impact on customers who may see genuine payments blocked which results in inconvenience and potential complaints.

We were told that in CRM Code cases involving crypto exchange firms,[4] the wallet to which funds are moved will typically be in the customer's name. However, there may be circumstances where the account to which the funds are moved (the holding account) has been opened in the customer's name without their knowledge and which they do not control. The customer is then socially engineered into moving funds into the holding account which is under the control of the scammer.

a. Cryptocurrency scam volumes

Whilst nearly all signatory firms reported seeing an increase in cases which involved cryptocurrency, exact prevalence figures for the volume of such scams were rarely cited. The reasons for this are unclear, although some responses suggested that existing categories for CRM Code related data did not currently capture such scams or the scam typology was evolving at a rate whereby record-keeping in systems was lagging.[5] In addition, the scope of the Code is limited to GBP-denominated UK domiciled accounts. All of which means there is a lack of clarity as to whether scams involving cryptocurrency should be recorded within APP scam data.

We recognise that cryptocurrency currently sits outside of the Code, and therefore may not be captured under industry APP scam data. However, as this is an area which firms have reported an increase in scam volumes, we believe that it is vital for firms to be able to ascertain the volume and intelligence in this space. Taking into account feedback to the Call for Input, there appears to be a gap for firms to agree and record consistent categories which are flexible enough to accommodate evolving scam typologies.

At present, as required under the Code, data about APP scams is collated by UK Finance on behalf of its members. We believe that there would be a benefit in reviewing and analysing the data further, so as an industry, there is more accurate information to discern scam types and methods which may have been retrofitted into existing categories. We will seek to engage with industry with a view to understanding how available data can be used to provide a more detailed picture of the volume of APP scams involving cryptocurrency, However, we are mindful that the PSR, within its Call for Views published earlier this year, stated its intention to require firms to publish scam level data. We await the publication of the regulator's response, which we understand is due to be published shortly.

b. Cryptocurrency and regulation

There is a regulatory gap in relation to cryptocurrency, which is an issue that is broader than the LSB's remit. The PSR, in a thought piece published in July this year, acknowledged that cryptocurrency has the potential to introduce innovation and choice of payments for customers. However, any harms arising from its use need to be minimised and users need to understand the risks, including the lack of regulatory protection associated with cryptocurrency.

[4] A crypto exchange is **a** platform on which customers can buy and sell cryptocurrency.

[5] At present scam typology for the CRM Code includes: Invoice and Mandate, CEO Fraud, Impersonation (police/bank), Impersonation (other), Purchase, Investment, Romance, and Advance Fee, with all of these having an inherent assumption, as per the Code scope, that the scam payment was conducted in pounds sterling.

This reflects the findings of the Financial Conduct Authority's (FCA) consumer research on cryptoassets, issued in June 2021, which followed up on previous FCA consumer research and found that 78% of adults had heard of cryptocurrency but that overall understanding of cryptocurrency had declined.

UK authorities too remain mindful of this regulatory gap; a HM Treasury consultation on the UK approach to cryptocurrency and stablecoins closed earlier this year, and the FCA, alongside the PSR, is working with the Treasury and Bank of England as part of the Cryptoassets Taskforce to look at issues of appropriate regulatory intervention in cryptocurrency matters. Steps towards a more secure regulatory environment have already begun. The FCA has published a list of unregistered crypto exchanges that it suspects are operating in the UK, to help consumers avoid using them whilst at the same time exploring the benefits of stablecoins to promote a more competitive payments market.[6]

As set out above, there are a range of regulatory challenges posed by cryptocurrency which sit beyond the CRM Code. As consumers become increasingly aware of cryptocurrency, firms have seen an increase in the number of scams being reported, as scammers seek to exploit consumer interest and capitalise on the lack of regulation in this space. We are also mindful that the Code is limited in scope to GBP-denominated UK-domiciled accounts and importantly, of the work being undertaken by the regulators to address the regulatory gap in this area. However, as with multi-generation scams, we recognise that firms are seeking to assess cases involving customers who have fallen victim to cryptocurrency scams under the Code and therefore require clarity on our expectations of how relevant cases should be assessed within the confines of the Code.

As set out above, we will engage with industry with a view to understanding how available data can be used to provide a more detailed picture of the volume of APP scams involving cryptocurrency. This will be used to further inform where guidance for firms may be required to support firms in assessing such cases under the Code.

Summary of next steps and actions

3. We will engage with industry to further understand how APP scams data involving cryptocurrency is recorded and what is available to support our understanding of the scale of the issue.

4. We will engage with industry to build on information provided via the Call for Input with a view to developing guidance to support firms in assessing cases involving cryptocurrency under the Code.

[6] Digital tokens can be issued with the aim of being maintained at the value of an underlying sovereign currency and used to make payments outside the conventional payment systems. These are generally referred to as 'stablecoins'.

5. Wider participation of firms in the CRM Code

a. Consumer protection at sector level

As financial services and the payments ecosystem continue to evolve, business models outside of traditional banking structures have to be taken into account as they also serve customers' financial, and payment needs; be they newer structures such as cryptocurrency firms or building societies working within geographical localities. It is vital therefore that protections are afforded to as many customers as possible when sending money via Faster Payments.

Our report on the Code review identified that 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, Payment Initiation Service Providers (PISPs) and Electronic Money Issuers (EMIs).[7]

The Call for Input sought to further explore how the Code could more effectively take account of the range of firms operating within the payments system. This would have a number of advantages: a greater number of customers are protected; improved and greater levels of intelligence about APP scams; better communication between firms; and expedient remediation, to name but a few. We recognise that the voluntary nature of the Code means that we cannot compel firms to become signatories, however we believe that it is important that the Code can capture as wide a range of firms as possible while also ensuring that there is a consistent approach to consumer protection.

Increasing participation in the Code has been a key area of focus for the LSB. Whilst take up from industry has been slower than we would have expected in that regard, we recognise the challenges that the requirements of the Code can place on some business models. The findings from the Call for Input reiterated the need to include a wider array of participants, in particular to address the concerning shift we have seen towards APP scams increasingly originating from non-signatory firms, and further, to address the balance of liability between sending and receiving firms, particularly those firms which are not signatories.

We also recognise that being a signatory to the Code is a nuanced debate with a number of considerations firms must take into account including compliance costs, evaluation of existing controls and their exposure to APP scam risk. We have explored some of these issues with respect to some firm business models below.

[7] A Payment Initiation Service Provider (PISP) lets customers pay companies directly from their bank account rather than using your debit or credit card through a third-party such as Visa or MasterCard. PISPs utilise Open Banking technology and standards in their operations.
Electronic money (e-money) is broadly defined as an electronic store of monetary value on a technical device that may be widely used for making payments to entities other than the e-money issuer. The device acts as a prepaid bearer instrument which does not necessarily involve bank accounts in transactions.

b. Building societies

Respondents had an almost ubiquitous perception of the building society model being low risk to APP scams, this was because customers were only able to send funds to a nominated account.[8] It is, however, still possible that some customers are manipulated into moving their money from an account held with a building society into their nominated account, and then the funds are further moved onwards to the scammer. However, this is balanced against the timings involved in moving funds through to a nominated account, as often Faster Payments are not part of the building society offering, which may inadvertently act as a deterrent to APP scams, especially where these scams rely on speed of the transaction to move money and evade investigation.

Moreover, it was reported to us that by virtue of their relatively smaller size, building societies retained a culture of knowing their (usually local) customer base intimately, (which it was noted by some respondents is not always possible for larger or digital based firms). It was also suggested that this in turn allowed for greater opportunities for front line staff to intervene where known customers were transacting in a way which was out of character. However, there was some feedback which suggested that building societies faced challenges in being able to sign up to the Code as it was not drafted to take account of such firms' business models.

c. Electronic Money Issuers

Almost all Code signatories, as well as some other financial firms and consumer organisations, reported that while numbers were low, they were seeing a growing trend towards scammers targeting cryptocurrency firms (as discussed in section 4 above) and Electronic Money Issuers.

Responses from this area of industry stated that the Code was not perceived to be appropriate for their business models. The reason stated for this was mainly due to the compliance burden of the Code on such firms, which tend to be much smaller with regards to the volume and the value of payments processed, in comparison to retail banks. The compliance burden was perceived to be with regards to several factors which included:

- the cost of putting in new processes and training staff on the Code; one such area related to the identification and support for vulnerable customers which was said to be challenging as the relationship with the customer is purely transactional and can often be sporadic;
- the capacity for continuous oversight and monitoring required (internal to the firm and that by the LSB); and
- the opportunity cost of implementation, whereby it was perceived that the firm would need to direct resources away from other initiatives in order to implement the Code.

[8] A nominated account is a UK bank or building society account that a customer can transfer money from and send money to. The customer is required to be an account holder on the nominated account. This means that any withdrawals out of the building society account are only sent to the nominated account.

Stakeholders from across industry and consumer sectors recognised that customers are increasingly using a diverse range of payment methods and it is right that these choices exist. However, as tackling scams is a sector-wide issue, many firms reported concerns about perceived weak spots in the broader sector, with EMIs and cryptocurrency firms being seen as prime targets for scammers.

Code signatories and industry stakeholder respondents, as well as consumer sector organisations, reported that they would be open to working with newer entrants in the payment system with focus on the identification of customers vulnerable to APP scams. We welcome such discussions and will engage with stakeholders to understand whether there is a role for the LSB to play in facilitating such discussions.

d. Payment Initiation Service Providers

On the role of PISPs, a common view was that innovation and choice for the customer were welcome advancements. At the same time, there was a degree of caution expressed by some respondents who felt all firms operating in the payment ecosystem should undertake their fair share of consumer protections, and it was perhaps a little too early to fully grasp the risks posed by developments in the Open Banking environment.

We did, however, receive feedback that in order to comply with Code requirements, where the consumer initiates a payment via a PISP, some signatory firms will initiate a Confirmation of Payee check and, where deemed to be necessary, provide a warning within their own payment channels.[9] The added friction in this model can sit in opposition to the Open Banking offering of streamlined frictionless payment. However, those signatory firms who have implemented these steps stated that this is necessary for them to meet their obligations under the Code, and to manage their own level of risk.

Whilst the CRM Code is one example of consumer protections against APP scams, it was widely noted that the Open Banking Implementation Entity (OBIE) had taken a progressive approach to anticipating APP scam threats by launching a consultation in February 2021, on evolving the Open Banking standards with regards to Confirmation of Payee (CoP) and the CRM Code. Within the subsequent analysis of this work, the OBIE concluded that it has not yet demonstrated that there is a clear appetite on the part of PISPs to participate directly in CoP or the CRM Code. An alternative was suggested whereby some PISPs proposed that in order to secure friction-free journeys, they would be willing to underwrite liability for APP scams which they can control. It was suggested that this might be a preferable alternative to becoming a full participant to CoP or a signatory to the CRM Code.

We continue to engage with the OBIE and share our mutual findings from research and broader engagement activity where this is relevant. Whilst we recognise that the volume of APP scams taking place via the Open Banking platform is, at present, low. In order to mitigate the risk of this becoming the channel of choice for criminals seeking to exploit customers, we continue to work with the OBIE as it encourages PISPs to develop scam prevention strategies

[9] 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.

and to work with firms in order to develop data sharing solutions, with the ultimate aim of establishing an ecosystem that maximises protection for consumers.

6. Addressing the barriers to entry

The feedback to the Call for Input elicited a common view across the consumer sector and firms including banks and building societies that APP scams, especially those which were not necessarily being seen at the time the Code was drafted, were in part involving platforms beyond immediate banking services. The feeling was stronger amongst Code signatories in particular, who felt they were underwriting the risks for customers' security details which were being compromised (either through the scammer duping the customer to give out details or poor security systems being hacked) in other non-financial settings and on websites.

There is a drive for a cross-sector response, with the work of Stop Scams UK and Home Office cross-sector partnerships being highlighted by many respondents. At the same time, there was also a view that much more still needs to be done by mainstream social media and retail companies to play a greater role in tackling scams at the point of origination. Whilst the LSB's remit does not extend to include non-financial firms, we will continue our efforts to galvanize those firms who are eligible to sign up, to do so.

In our January report, we committed to revising the Code to address the perceived barriers to entry to ensure that the Code is capable of applying to a broader range of firms. In doing so, we need to ensure that any amendments maintain a consistency in the standard of protection provided to customers under the Code. We are also mindful of the OBIE's work in this area and therefore the amendments may still not go far enough to enable PISPs to become signatories to the Code. We will balance the focus on widening participation with ensuring that the existing protections of the Code are not inadvertently decreased and in doing so, inadvertently create a two-tier approach to protections under the Code.

We are also mindful of the PSR's work on APP scams and the measures it proposed in its call for views to require firms to either sign up to a PSR recognised industry Code or automatically reimburse customers who have fallen victim to an APP scam. In addition, the government's response to the Call for Evidence on the Payments Landscape Review states that it is the government's view that *the introduction of Faster Payments rules setting out reimbursement and liability requirements on all scheme participants, alongside preventative measures, is the best possible solution to the issue of APP scams. The PSR's call for views has now closed, and the government is engaging with the PSR and industry on next steps, including considering what further actions may be necessary to make urgent progress on this issue.*

In the interim, we will move forward with our work to ensure that a broader range of firms are able to sign up to the Code and will consult, where required, on any amendments to the Code by the end of the year. The amendments will seek to address the perceived barriers set out above, subject to ensuring there is no decrease in consumer protections. These will include amendments such as:

- in light of the PSR's proposed measure to require firms to publish APP related data, and our discussion on cryptocurrency scams above, we will consider whether amendments are required to the Code provision on the collection and reporting of data and reporting;
- ensuring that the Code requirements for transactional data used to assess risk profiles to APP scams, are relative to the size and model of the firm; and
- allowing for the Code to recognise that firms may not provide Faster Payments to their customers and, in turn, may not offer points of customer contact in a 24/7 fashion.

It should also be noted that this list indicates broad changes and does not constitute a comprehensive list of changes to the Code. We will outline the revised Code wording and undertake due process and consultation, where necessary, especially with existing signatories, before any changes are codified.

Summary of next steps and actions

5. The Code will be updated to enable a broader range of firms to participate, while maintaining a consistent approach to consumer protection. We will publish further information regarding these updates shortly.

6. We will continue to actively engage with industry with a view to increasing the number of signatories to the Code.

7. Wider amendments to the Code

Alongside the work above, we will also activate the Code provisions referencing Confirmation of Payee (CoP) in recognition of wider regulatory work on this issue. We committed in the Code review to review the provisions which reference CoP which, at present, have a holding date for implementation. Our consideration then was that not all firms considering sign up to the Code were subject to the PSR's direction,[10] and that by activating the provisions at that stage, we may have put some firms in breach of the Code, or the provisions would create a further barrier to entry for non-signatories.

However, since issuing our review report, there have been some key developments in the payments sector. Therefore, as part of wider updates to the Code, we intend to activate the CoP provisions for those firms who can offer this functionality. This will be done in tandem with the progress made by the PSR and Pay.UK in moving ahead with phase 2 of the CoP programme which will see a broader range of firms offering this functionality.

In June 2021, the PSR released a consultation outlining its analysis of CoP to date, and seeking views on its intention to move to phase 2 which would see a greater number of firms offering this functionality. In October, the regulator published the outcome of its consultation

[10] 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.

providing clarity of actions it expects industry to take and an overview of how it will support the industry for wider uptake of this service.

These actions, and the PSR's focus on increasing CoP within the industry, gives us greater confidence to move forward with the activation of the relevant provisions within the Code, which alleviates previous concerns about these provisions acting as a potential barrier for non-CoP participants.

We will also give further consideration in the future to the inclusion of Secondary Reference Data (SRD) provisions so that the Code remains relevant to any firms which are unable to undertake CoP.[11] This will be done in line with the work of the PSR on phase 2, and its assessment of progress next year.

Summary of next steps and actions

7. As part of wider updates to the Code, we will implement the relevant Code provisions on Confirmation of Payee.

8. We will continue to engage with the PSR as its work on phase 2 of Confirmation of Payee progresses with a view to deciding whether the Code should include provisions to capture Secondary Reference Data provisions.

8. Roles and responsibilities under the CRM Code

a. Sending and receiving firms

The Code works to the three-party model whereby it recognises the customer, the customer's firm (as the sending firm) and the receiving firm (the account to which the money is moved). The Code further sets out that the sending firm is responsible for assessment of claims made under the Code.

Feedback from existing signatories, as well as consumer representatives, suggested that responsibilities between sending and receiving firms, that are signatories to the Code, should be reviewed. The intention behind this is to increase the emphasis on the role of the receiving firms within the Code. There was a general view expressed that receiving firms had less responsibility under the Code and related to this, there were questions raised around the equitable balancing of responsibilities between sending and receiving firms. However, given the range of issues covered, we wanted to understand more about this issue through the Call for Input.

[11] Some firms, such as building societies, use secondary reference data to direct payments to their customers.

b. Receiving firm accountability

Under the Code, liability is allocated according to the roles each party played which may have enabled the APP scam to occur. For example, where the success of the scam is assessed to be due to neither firm meeting the required standards for firms, and there are no grounds on which to decline reimbursement, the firms share 50% of the reimbursement so that the customer receives 100% of the money they lost to the scam.

Responses stated that receiving firms, especially where such firms are not signatories to the Code, were perceived to not be accountable for their role in the payment journey. Accountability for the scam being attributed to receiving firms was described in terms of the acceptance of liability and subsequent allocation of reimbursement, as well as failure in upholding preventative elements, as the recipient firm had allowed mule accounts to exist through which the funds could pass.

Given that the success of an APP scam necessitates the presence of an account being accessed by a scammer and/or the funds passing through several intermediary accounts over which they have some degree of control, the issues of mule accounts is heavily interwoven into the narrative on receiving bank liability.

From the feedback received, we also saw that, at present, firms face two main issues in the prevention of mule accounts: firstly, firms face a challenge in identifying accounts which had been legitimately opened and operated, before being used for mule activity; and secondly, for multi-generation scams, firms are often caught between their duties to execute authorised payments in a timely fashion, whilst also adding in the necessary friction to freeze funds in order to conduct the appropriate investigations.

Signatory firms, in particular, highlighted the findings from our data report, which accompanied the full Code review, showing that recipient PSPs were recorded to be at sole blame across just 1% of all CRM cases. Signatories questioned why receiving firms were not holding themselves accountable more often, as accounts which should have been subject to stringent regulations and customer checks were being operated by scammers. The issue of receiving firms' failure to uphold responsibility for their part in the success of an APP scam was perceived to be exacerbated in instances where those receiving firms were also not signatories to the Code and/or were newer business models.

c. Application of the Code

In light of the feedback about the imbalance in the allocation of liability, we reviewed the underlying liability model of the Code and in particular the 'Allocation' provisions. It was not entirely clear from the feedback, the exact reasons for this unbalanced acceptance of responsibility, given that the Code allows for fair distribution of liability, and that the requirements of the Code account for receiving firms.

The most prevalent hindrances cited were issues around the voluntary nature of the Code. This fact, combined with the earlier observed trend of APP scams increasingly originating from non-signatory firms means the issue of unbalanced liability between signatory and non-signatory firms, it was suggested, may continue to exacerbate.

The Code cannot bind non-signatories to participate in this model, and the decision to become a signatory is on a voluntary basis. For this reason, feedback reiterated overwhelming support for a form of mandatory avenue for the provisions within the Code. This included 'recognition by a regulator' of the Code in its entirety, changing payment scheme rules to include Code provisions, or leveraging other proposed legislation to include protective elements of the Code.

To that end, a number of avenues were proposed in the feedback for placing more responsibility on receiving firms, including:

- Assigning liability so that where a customer has been scammed, the receiving firm automatically holds a degree of responsibility as it has allowed an account operated by a scammer to remain open. This would capture firms outside of the Code (which already stipulates liability according to the roles each party played in the success of a scam).

- Creating standards for receiving firms with regards to investigation, and communications of the outcomes, as well as improved clarity for the customer regarding receiving firm processes. As well as tracing the funds, this was with a view to improving the experience a customer has in making a claim and incentivising receiving firms to co-operate in order to reduce any delays.

Options beyond the scope of the Code were also proposed including:

- Compelling receiving firms to share information with all parties, to help trace the fraudulently obtained funds if they have been further forwarded on. This related to a broader point about how the payments industry as a whole needs to co-operate to help trace fraudulent funds and to locate and freeze such accounts to help reduce their usage.
- Engaging payment schemes to consider how consumer protection can be improved, by for example, enforcing scheme conditions so that those firms offering a given payment option, such as Faster Payments, agree to offer protections by virtue of the conditions of the scheme.

Taking into account the feedback provided, it appears that the issues identified are being driven by a number of factors including: expectations around receiving firms and how such firms assess the part they have played in the success of the scam; the move towards non-signatory firms being targeted by fraudsters; the wider issue of the identification and closing down of mule accounts; and how the Code can ensure that receiving firms take greater accountability for their acts and omissions which enabled the success of the scam.

It is important to note that while the Code can create additional obligations on receiving firms, it cannot bind non-signatory firms and, in turn, we have no oversight of how the receiving firm is applying the provisions of the Code where they are not a signatory to it. It is our oversight which drives consistency of application of the Code's provisions and in order for it to be as effective as possible, it requires a wider industry commitment to being a signatory to the Code.

Having considered the feedback provided, in order to ensure that the Code is able to work as effectively as possible, we will undertake further work with industry to explore the issues outlined in this report and test the viability of the models suggested, where they fit within the scope of the Code. This work will inform where updates may be required to the Code. We will also seek to share feedback, as appropriate, with relevant stakeholders where we believe they may be better placed to take forward some elements of this work.

Further information on this will be provided in due course but we propose to begin our work on these areas of the Code before the end of the year.

Summary of next steps and actions

9. We will undertake further work with Code signatories to explore the issues raised in this section of the report to ensure that the Code sets a fair balance between sending and receiving firms. This work will inform where updates are required to the Code.

9. The CRM Code and customers

a. The role of the consumer organisations

Within the Call for Input we sought further views on the feedback we had received in January, with regards to the role's consumer organisations could play in the customer payment journey. Initially we were told that such organisations had the potential to undertake the following roles:

- provide awareness about APP scams and advice on steps the customer could take to protect themselves from being exploited;
- provide a source of support within the payment journey itself, by for example being signposted to advice or guidance whilst the customer conducts a payment; and
- provide follow up advice and support where the customer has been scammed.

We tested these propositions within the Call for Input, as well as our other engagement activity such as bi-lateral meetings and wider engagement with consumer stakeholders. We found that the role that such organisations play with regards to being trusted sources of information for consumers and as a source of support after being scammed was greatly valued and these roles should be enhanced and continue. It was also broadly agreed that the customer payment journey should not include anything which causes confusion, alarm, or extra friction, and this should remain as secure, seamless, and clear as possible.

b. Information provision for customers

Customer awareness of APP scams continues to remain a high priority across stakeholders. There is the need for both customer awareness of APP scams prior to any scam occurring and support for those customers who find that they have fallen victim. It was widely agreed that consumer organisations play a vital role in both of these situations.

Whilst the LSB does not work directly with customers, we are aware they are directed to sources of information or find themselves coming across our information when they are researching matters relevant to our Standards and Codes. To that end, we have a customer information document which accompanies the CRM Code and sits on our website. In our January report, we committed to reviewing and updating this document and as part of the Call for Input we received feedback on the current content which suggested that, whilst the information within it is accurate, it is not very engaging to customers.

At the same time, there was also feedback which suggested that other customer facing information beyond the LSB can appear inconsistent depending on which consumer organisation the customer approached. We were provided with examples of two consumer organisations which prompted consumers to take different actions by contacting different parties. For example, one website advised customers to call the police first, whilst the other signposted to a further consumer organisation and advised consumers to speak to their bank. Firms were concerned that customers were not being advised to immediately contact their own bank first and foremost, as time is of the essence in being able to secure funds.[12]

We also saw that some consumer organisations produced materials tailored to their audience. The material submitted to us was engaging, used accessible language, and designed to a high standard.

We would not want to replace the awareness raising work that is being carried out by consumer organisations who can use their experience and expertise to tailor their messages to their target populations. However, given our findings that customer information provision in the wider public realm can at times be inconsistent, we will progress work to update the customer facing document to make it more accessible to consumers, recognising that it serves as an authoritative and consistent point of information provision in relation to the Code which other organisations can draw upon.

Summary of next steps and actions

10. We will progress with our work to update the customer information document to improve its accessibility and useability.

[12] However, we do acknowledge that it is possible that such advice on consumer websites assumes that customers have already informed their banks and are seeking further help when other avenues have been exhausted.

10. The CRM Code and public narrative

As noted in our January report, respondents advised that the Code was regularly being framed as a 'refund scheme' by some groups of stakeholders. It was felt that this was often linked to the heavy focus on reimbursement levels under the Code. We also discussed the detrimental impacts of defining the Code in such narrow terms, and the need to take account of the preventative and aftercare measures of the Code. Our report set out a series of recommendations to be taken forward to ensure that the Code, and the consumer protections which sit at the heart of it, continue to work as effectively as possible. One key recommendation was that further work was required to define the success measures for the Code. While the Code's objectives, which were developed by the APP Steering Group, are clear, there has been no consensus on how to determine whether these objectives have been met.

We believe that it is vital that success measures are accurately defined and introduced to properly assess the effectiveness of the Code, ensuring that the understanding of its impact goes beyond solely focusing on its reimbursement provisions. Success measures may include but not be limited to the impact of its prevention and detection measures to reduce the occurrence of scams; increased awareness of the Code through consumer education; and consistency in application of the Code and wider adoption across industry.

Code signatories, and other firms, within the feedback provided to Call for Input, overwhelmingly stated that the messaging around the Code needed to be more balanced so that consumer responsibilities are visible in the public narrative. However, this was countered by alternative views from consumer stakeholders asserting that it is not reasonable for customers to be aware of liabilities as they are transacting, and customer education is only a small part of narrowing the information asymmetries between banks and their customers. They went on to assert that the greater onus should be on banks to design protective products and services and have in place expedient remediation processes.

The Code is based upon a contingent model which requires the assessment of individual cases and the circumstances which led to the customer making the payment. The Code does not bind customers; therefore, we are unable to support the development of customer facing communications which seek to set out responsibilities for customers under the Code. We are concerned that in seeking to set out responsibilities for customers under the Code, they would be held to standards they have had no role in developing, may have no awareness of and depending on their circumstances, may not be able to meet.

However, the preventative and educational elements of the Code cannot be underplayed, and we have begun work which seeks to re-set some of the narrative around the Code through the development of success measures which look beyond just reimbursement levels. We will engage with stakeholders over the coming months to seek input and views on how we should look to measure the success of the CRM Code. We will provide further updates on this work in due course.

11. Conclusion and next steps

Our full review of the CRM Code concluded in January 2021 and resulted in a number of recommendations for the LSB to take forward. These recommendations identified the need for a Call for Input to obtain additional insights to enable the areas, identified within our report, as having potential customer detriment to be addressed.

The Call for Input has enabled us to further our understanding of what these areas of concern are, how we can seek to resolve them and ensure that customers retain the maximum protections offered by the Code.

We would like to thank all respondents for the time taken to engage with the Call for Input. We would be unable to move forward with our recommendations and proposals without the engagement of key stakeholders, firms and the wider industry.

As detailed within this report we have focussed this Call for Input on three key areas; expanding the scope to take account of emerging scams; increasing participation; and ensuring responsibilities are shared equitably between sending and receiving firms. We are now in a position of being able to take forward a number of actions over the coming months either through amendments to the CRM Code and accompanying practitioners guide or through further engagement with industry. Any action we undertake is cognisant of the PSR's work on APP scams and particularly, the output from its Call for Views. We will continue to engage with the regulator to ensure that customers are protected from APP scams and, in the unfortunate event of falling victim to a scam, customers receive a fair outcome when resolving any claims for reimbursement.