September 2018

APP Scams Steering Group

Draft Contingent Reimbursement Model Code

CONSULTATION PAPER

Non confidential responses

Part 1

IMPORTANT NOTICE

This document includes consultation responses to the Draft Contingent Reimbursement Model Code (published in September 2018) of the APP Scams Steering Group. The Steering Group provided a non-exhaustive list of consultation questions and invited feedback to the further development of the code. Respondents were asked to clearly mark any confidential information contained in the response which should not be published. Only the group's Chair and the group's independent adviser will see this confidential information. The Chair, independent adviser and independent economic consultancy (Cambridge Economic Policy Associates, see www.cepa.co.uk) will provide the information to the rest of the steering group on an appropriately anonymised basis.

The responses published in this document have been submitted via the PSR and have been confirmed by the respondents as being non-confidential. Checks have been carried out to ensure no confidential information has been inadvertently released. Responses are included in alphabetical order within the respective sub-categories.

CONTENTS

Atom Bank Consultation Paper Response

APP Scams Draft Contingent Reimbursement Model Code

Atom Bank welcomes the opportunity to comment on the Draft Contingent Reimbursement Model Code; published by the APP Scams Steering Group in September 2018, particularly as we feel challenger bank opinions were not adequately represented in the drafting of the Code. As a digital bank one of our priorities is to ensure that we are a leading business when it comes to the security and protection of our customer's data and money. Atom are fully supportive of the FCA's operational objectives designed to protect customers, protect financial markets and promote competition so we can see the welcome benefits of this forthcoming additional customer protection. At the same time, however, we are mindful that the established banks will have significant advantages in implementing the Code, versus those that the challenger banks/ new entrants may enjoy. We have outlined these challenges in our responses below.

Atom currently offers Fixed Term Saver accounts. APP scams are not currently a risk with this product as there are limitations on where funds are paid out at maturity i.e. to an account in the customer's name or a nominated account that has been validated. Implementation of the Code will likely coincide with the expected launch of our first 'payment account' in 2019; which will introduce the risk of APP scams when we allow our customers to authorise faster payments to third parties.

Atom undertakes all financial crime, fraud detection and complaints handling in-house. Additional recruitment; particularly in relation to fraud data and analytics roles to enable compliance with the Code's 'Detection Standards' will be necessary before we can subscribe to the Code.

Standards

Q: Do you agree with the standards set out in the Standards for Firms?

We agree with the standards however we believe it will be difficult to measure compliance with the 'Standards for Firms' as the requirements of the Code are not prescriptive. App scam prevention measures will need to be implemented via a legal or regulatory framework if they are to be applied consistently and fairly. In the absence of legal and regulatory backing, all firms will take a different approach to compliance, depending on their risk appetite and product base.

The FCA has already indicated that they have an expectation that firms will show commitment to the Code, albeit the Code will be voluntary. The level of that commitment has not been communicated, which will impact Senior Manager Function holders who will need to apportion both resource and budget to implement new systems and controls to show compliance with the Code. Treating Customers Fairly (TCF) considerations will also need to be considered in relation to the potential decision not to reimburse victims of APP scams.

Detection

Unusual transactional activity

In relation to the 'Detection Standards', it is proposed that firms will undertake better analysis of transactional data for unusual transaction activity. Atom is growing its fraud monitoring capabilities in line with the expansion of our products, and as such, our data profiling, versus the established banks will be less mature. Whilst our intention is to always build capability to a 'best in class' position, as a new player it will take time for us to do this. The result of this could be a higher proportionate cost as we build these capabilities and get ourselves on an equal footing with the established banks.

Customer interactions

Fraud prevention is critical to Atom's success as a digital bank, and fraud detection, in the absence of a face to face customer interaction, presents unique challenges. Our intention is to drive awareness and engagement with our customers to help them protect themselves, but as their bank we also have a responsibility to 'look out' for them. Our security model takes into consideration the additional challenges of being a 'digital only' bank, but again this does put us at a disadvantage against the mainstream banking model where face to face or voice interactions can be more easily identified as fraudulent.

Faster Payment limits between the banks should also be considered, as these are set at individual bank level, according to their risk appetite, and vary according to the delivery channel i.e. branch, online, telephone or app. Again, this sets an uneven playing field where the receiving bank could be paying out a higher level of compensation than their own Faster Payment limit, in the event of an APP scam. This needs further consideration to ensure fairness and transparency for the Code.

Prevention

The Confirmation of Payee (CoP)

The CoP scheme is co-dependent with the CRM as it will be one of the features by which a consumer can validate a payee's bank account prior to authorising a payment. Implementation of the new system will be a cost that firms will pay in order to become a subscriber to the Code. However, we do see the benefit to our customers and provide some reassurance when they authorise payments. Given the implementation cost involved, the solution must be reliable and effective before being made accessible to customers as a fraud prevention tool and we understand that work is underway at industry level forums to ensure this reliability.

Response

Reimbursement of customers following an APP scam

The standard of care expected for consumers, and how this will be evidenced needs to be clearly defined, only then can the requirements be applied consistently across the industry. The Code currently sets a very low threshold for customer standards, with no need to evidence compliance with those standards. This may unintentionally lead to a general view amongst consumers that their transactions are being 'insured' by the banks.

There is a risk that the CRM will be attractive to criminal gangs, making claims that they have been defrauded once they understand the extent to which the CRM has been implemented within each bank.

Vulnerable Customers

Q: Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

Recognising that a customer is vulnerable relies to some extent on having regular and ongoing interaction with customers. Atom bank has a customer self - serve app model which inevitably means we have limited human conversations with customers, so we continuously work on new methods of identifying customer vulnerability using data and technology and will strive to do this in the future to ensure compliance with the Code.

Given some of the sensitive circumstances that lead to vulnerability, and the reluctance of customers to discuss these private issues firms may not always be able to flag a customer as vulnerable. There are existing FCA requirements on firms to obtain consent from customers before flagging them as vulnerable. GDPR also brings a requirement that any consent can later be withdrawn. Firms will need to decide how best to manage these requirements in line with the Code's vulnerable customer requirements. Discussions on vulnerability between sending and receiving banks following an APP scam will need to be managed within these legal and regulatory requirements.

Where a customer has been assessed under the Code as vulnerable to APP scams, and firms have met all their standards, then it is proposed that the cost of reimbursement should be funded by the customer's firm. One of the unintended consequences of this additional protection afforded to vulnerable customers will be that non-vulnerable consumers who have acted recklessly may claim they were vulnerable at the time to receive reimbursement.

Timescales

Q6: Do you agree with the timeframe for notifying customers on the reimbursement decision?

The timescales in the draft code are aligned with timescales defined in PSD2 and complaint handling requirements in DISP; which is sensible. However, given the resource constraints in smaller firms such as Atom, this may be onerous given that some investigations may be complex.

Covering the cost of reimbursement

Q: Do you agree that all customers meeting their requisite level of care should be reimbursed,

regardless of the actions of the firms involved?

Q: Do you agree that the sending firm should administer any such reimbursement, but should

not be directly liable for the cost of the refund if it has met its own standard of care?

The requirement to reimburse APP fraud victims is an unknown cost to some firms that aren't currently exposed to APP scam risk, and they may either choose not to introduce certain new products and services which will introduce that risk, or they will need to factor in the potential costs in their product pricing. This means that ultimately the cost will be passed to all customers.

In the case of no-blame situations we do not agree that firms should be expected to cover the cost of APP fraud when the firm is not at fault, when they have met the required standard of care required under the Code. It is unrealistic to expect that receiving firms will be able to identify all money mule transactions on accounts but may still be liable for reimbursing victims. According to Vocalink two thirds of mule accounts are undetected. There is currently an industry led initiative to reduce mule activity i.e. Vocalink's Mule Insights Tactical Solution which commenced live proving in September, with participation from ten large financial institutions in the UK. This scheme is available to members of the Faster Payments Scheme (of which Atom is a direct member). Whilst this tool is recognised as invaluable in assisting in the re-patriation of funds to customers it is another cost to firms which may ultimately have to be passed on to customers. As the Confirmation of Payee system is considered co-dependent on the CRM then some thought should be given to making the Mule Insights solution equally dependent. Both solutions will assist banks in the prevention and detection standards in the Code.

Evidential approach

Q: How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

Q: How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

Prescriptive requirements will be required on what is to be considered 'acceptable evidence' in complying with the requirements of the Code. The Financial Ombudsman Service will need to be seen to be consistent in making decisions on whether a firm should repay the customer. Such consistency will only happen if there are prescriptive requirements.

The intent of the Code must be for banks to be fully accountable for reimbursing customers, and for the FOS to only conclude on cases where no agreement between the banks can be reached. We need to ensure that escalations to FOS do not increase simply because the standards are not prescriptive enough to be clear.

In relation to evidencing vulnerability, the nature of their vulnerability may be very sensitive and there will be data privacy implications when firms need to request evidence to prove their vulnerable status. (See Vulnerable Customer section above). This may result in increased customer complaints or breaches of GDPR. Clear guidance within the Code, on what constitutes acceptable evidence of vulnerability will help mitigate this.

Inter–firm allocation and dispute resolution

Q: Is a simple 50:50 apportionment for shared blame between firms appropriate?

The suggestion that a 50:50 split between sending and receiving banks in a shared blame scenario may seem the most straight-forward approach but it may be extremely onerous on smaller firms that do not have corresponding loss provisions that the larger firms will be able to hold. Clarity is also required to determine what action will be taken in a transaction where only one of the PSP's has subscribed to the Code.

Positive and negative effects on victims of APP scams

Q: What positive and/or negative impacts do you see for victims of APP scams as a result of the implementation of the code?

Positive

- A reduction in APP scam victims as banks begin to subscribe to the Code and consumers become better educated about protecting themselves against fraud.
- An increased sense of security, particularly when using digital services; which in turn helps give consumers confidence to move to new services and brands.
- Introduction of a CoP solution will provide real-time feedback to consumers before they authorise third party payments. (On the assumption that the CoP solution is proven to be reliable and straight-forward for firms to implement.)
- Increased protections for vulnerable customers.
- FOS protection for customers seeking redress.

Negative

- An expectation from consumers that they will always be reimbursed for APP scams and the potential for negative publicity for any firms that decline reimbursement requests, having proven they had the requisite standard of care.
- Sensitive nature, and data privacy implications for vulnerable customers who will need to prove their vulnerable status.
- Vulnerable customer status may only be categorised by one bank in a transaction, and there will be data privacy implications of sharing sensitive data.

Positive and negative effects on firms

Q: What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

Positive

- The Code will implement a consistent consumer protection standard for all firms to adhere to.
- Firms will be more focussed on educating their customers about APP scams.
- Increased protection against scams means that more consumers will be encouraged to bank digitally driving down costs as consumers to change their banking from their traditional bank to the challengers.

Negative

- The scheme is anti-competitive to the challenger banks/new entrants as the costs in implementing the scheme and increasing dedicated fraud head count may lead to a reluctance to launch new products and services or to implement payment restrictions within new products.
- The Code is voluntary and requires legal or regulatory backing for it to be applied consistently.
- Fraudsters and criminal gangs may manipulate the scheme, particularly when they get to understand to what extent each firm has implemented the 'prevent' and 'detect' elements of the Code.
- The timeline to implementation is too restrictive. Legal and regulatory changes generally allow a lead in period, allowing firms to implement policies, procedures, and staff training. The bigger banks that have been involved in the Steering Group responsible for drafting the Code have an advantage that they are likely to have already commenced building procedures to comply with the requirements of the Code.
- Inconsistent application across the industry given that the larger banks will have mature transaction analytics and behavioural profiling systems and the corresponding resource available to handle investigations and complaints.

Atom Bank

15th November 2018

Barclays

1 Churchill Place
London
E14 5HP

home.barclays

15 November 2018

C/O Payment Systems Regulator
APP Scams Steering Group
12 Endeavour Square
Stratford
E20 1JN

Barclays' response to the Steering Group Consultation on the Contingent Reimbursement Model Code

Dear Steering Group,

Executive Summary

Barclays welcomes the opportunity to provide a response to the Steering Group's Contingent Reimbursement Model (CRM) Draft Code ("the Code") Consultation.

Barclays understands the importance of there being a comprehensive approach to tackling the increasingly common and sophisticated scams which can cause significant financial and non-financial detriment to consumers. For this reason, we are supportive of the PSR's aim of developing a comprehensive solution and have been an active participant in the Steering Group which was tasked with developing the Code.

We believe that the Code represents a vital step forward in providing support and clarity to consumers regarding their rights and responsibilities in the event that they are a victim of an Authorised Push Payment (APP) scam. Barclays are therefore supportive of the general approach being undertaken with respect to the CRM.

However, when considering how to challenge the fundamental prevalence of APP scams, there are a number of critical issues that - as we explained in our response to the Draft Consultation and through our participation on the Steering Group – are yet to be adequately addressed.

Importantly, as currently designed the Code's potential benefits are focused on putting consumers back in the financial position they would have been in, had the scam not occurred in the first place. Whilst this is an important and necessary development, Barclays strongly believe that a primary focus of any policy effort should be preventing scams from occurring in the first place. Taking the profit out of crime for fraudsters will in turn reduce attempts, undermining a source of funds for organised crime, and therefore weakening their wider negative impacts on the UK.

The Code rightly includes measures to ensure that in-scope Payment Service Providers (PSPs) undertake all reasonable efforts to deter and prevent scams from occurring through either their accounts or their payment 'rails'. However, as currently drafted, its efficacy is necessarily limited due to two exclusions:

1. The first is the exclusion of out-of-scope PSPs; Barclays are therefore firmly of the opinion that the Code needs to be mandatory and have a regulatory or legislative basis, with all PSPs subject to its provisions.
2. The second is the exclusion of the non-PSP organisations which facilitate scams – including but not limited to: platforms, technology firms, telecom firms, and pension funds. Barclays is similarly strongly of the belief that these organisations must be brought into the scope of the CRM and related activities if policy makers hope to have any impact on combating scams at their source, and therefore sparing consumers from the financial and emotional hardship that accompanies being victim of a scam. This would additionally support the principle of a regulatory level playing field (same risk, same regulation), an important principle of the UK's regulatory environment.

a. For example, many scams are enabled via fraudulent adverts on social media platforms, through which they the scammer engages with a customer via a messaging application – establishing trust which then leads to a request for a payment which the customer believes to be genuine.

Barclays agree with the concept that in circumstances where consumers have met their requisite level of care, and the associated evidential standards have been met, that consumers should be reimbursed. However, there are a number of associated issues that require clarification to ensure that the CRM works as intended and consumers receive fair, consistent and appropriate treatment. Importantly, if a PSP has also met their requisite levels of care, then – whilst consumers who have also met their requisite level of care should not be disadvantaged, and should be reimbursed – funding for any reimbursement must not come from the associated PSP. To do otherwise may lead to unintended consequences as it may be necessary for PSPs to limit a potentially open ended liability that they would otherwise hold.

With respect to governance, Barclays believe that the Payments Systems Regulator (PSR) is best equipped to take on governance of the Code and to give it the regulatory backing it requires to be a success for both consumers and the industry. Having proposed the initial Code to the industry, formed the Steering Group, and steered the progress made throughout, the PSR have the expertise required to support the industry in implementing and governing the Code to ensure it is a success. If the PSR believe they are not able to govern the Code, then this may delay implementation, and prevent it from having the regulatory underpinning required for it to be a success.

More generally, we note that any specific measures contained within the Code will quickly become out of date, and as such will need to be continually reviewed and updated.

Finally, if the Code is to be effective, its status is important. Following the consultation period, in the event that changes are made to the proposed Code, we believe that these should be widely and fully consulted on. It remains our strong belief that the PSR would be best placed to do this in line with its earlier work in this space, with input from working groups.

Outlined below are the principle areas where we believe the Steering Group should give further and serious consideration to, as they finalise their approach.

I. Ecosystem approach

Barclays believes that policy makers – including both Government and Regulators – should take the opportunity that has been presented by the analysis undertaken under the CRM Code's drafting process to take a long-term, strategic and encompassing view of the steps that are required from all the players in the APP scams ecosystem to stop scams before they have an impact on any consumers.

Importantly, we are concerned that the Code is limited to a focus on the largest PSPs. We believe that solving this problem requires full participation from all PSPs and from all those who feature in the "scams ecosystem", including the platforms and technology firms who often host or enable the nefarious elements that undertake these criminal activities, along with organisations that allow their security to be breached, therefore placing consumers' data at risk of being used by criminals to enable either fraud or scams.

Extending regulation so that these actors ensure that their systems and services cannot be used by fraudsters should be a greater priority. Making PSPs solely responsible for compensating victims would distort incentives in what is becoming a complex, integrated market involving multiple entities. The Code does not address this fundamental point, and we would strongly urge Government, the PSR and the FCA to consider what further action needs to be taken to ensure that scams are prevented at source. Dealing only with the consequences will only have limited effect and it will be very difficult to measure any success and the effectiveness of the Code. Scams are criminal activity and, as with any other criminal activity, prevention ought to be the prime focus of

any policy efforts. Barclays stands ready to act in concert with other members of the ecosystem to make this a reality. Without this explicit inclusion, there will be gaps in both consumer protections and outcomes.

Consideration should also be given to the role of third party Payment Initiation Service Providers (PISPs) under the Code. Under Open Banking, PISPs will be able to make payments at customers' requests directly from the accounts they hold, using Faster Payments. PISPs must be covered by the Code, as otherwise there is a risk that a gap in consumer protections is created, which may undermine the success of Open Banking in driving competition in the current account and payments markets. Not having these in scope could create an unintended complex experience for the consumer, who would not have the same protection levels if they were to fall victim to a scam.

The role of data breaches in seeding such scams must be acknowledged, and those responsible made appropriately liable for their role in enabling such scams, by providing scammers with information on their victims that allows them to socially engineer their interactions with the victim.

II. Establishing when a customer is eligible for reimbursement

The issue of liability is at the heart of the development of a CRM. We support PSPs taking responsibility for their actions where they have been substandard and have contributed to a customer losing their money. However, we disagree with the notion that PSPs should accept all liability for a scam in the instance that 'no blame' can be attributed to either party. If this were to happen, consumers may see very little benefit in protecting themselves online (leading to greater volumes of fraud and scams), with PSPs effectively taking responsibility for the criminal behaviour of fraudsters and, at times, customer behaviour.

This would set a dangerous new precedent, by creating tangible liability which should only be within the remit of the courts, or Parliament. Without careful consideration, the unintended consequences of this approach could have severe cost implications for PSPs (which, at best, will cause friction to payment journeys, and, at worst, create prudential risk) and be detrimental to competition - driving consumers to larger PSPs who are signed up to the Code for a more favourable reimbursement option than challenger banks and smaller PSPs.

With respect to liability, Barclays is supportive of the Code as currently positioned. However, we are clear that should policy makers determine that PSPs should bear the full liability for consumers' losses when they fall victim to scams – in situations where it is accepted that the PSP had undertaken appropriate steps to prevent/deter the scam from occurring – it will be necessary for PSPs to take steps to limit this open ended liability. These steps would be undesirable for both PSPs and consumers, and could include actions such as: slowing Faster Payments (FPS) services for consumers or, materially increasing the number of genuine consumers whose payments are interrupted. We are categorically clear that these are not steps that we would wish to take, since they would materially negatively impact our consumers' experience of making a payment.

Barclays have made a commitment to work towards the principles of the Code, but without an appropriate solution to no blame and shared blame scenarios, we do not believe that the reimbursement elements impacting these areas of the Code can be implemented and PSPs will not be able to reimburse in these cases.

In addition to this, Barclays feel that 'shared-blame' scenarios between the PSP and customer require further consideration before the final Code is issued. We do not think it is the right outcome if PSPs are required to reimburse (even partial) victims when they have not followed the requisite level of care as this could encourage inconsistency in who would be reimbursed. Doing so would likely lead to an increased risk of the UK being specifically targeted by criminals as an easy-target for scams. We recommend that this is given time for consideration, and that case studies are put through to support decisions.

III. Governance

Barclays notes that important questions remain with respect to the governance of the Code. We are clear that – in order to achieve the original objectives of the Code, and to have a meaningful chance to offer real and substantive protections for consumers against being a victim of APP scams in the first place – regulatory

oversight of the Code and associated activity is a necessity. As such, our clear position is that the PSR are made the accountable organisation for oversight of the Code.

With respect to taking forward the next steps in designing and driving forward an eco-system led approach to combatting APP scams, we believe that this role could be undertaken by the PSR. There may also be merit in this being undertaken in conjunction with the Home Office, given their eco-system wide perspective and broader responsibility for combatting economic crime.

IV. Evidential standards

Barclays recognises the importance of ensuring that an appropriate tangible evidence framework is implemented so there is consistency throughout all APP scam investigations across all PSPs. Additionally, due to PSPs reimbursing based on the principles from a public Code, the risk of first party fraud becoming more prevalent in the scams eco system becomes greater.

Throughout the Code it is appropriate that to investigate every case on its own merit and that evidence is required from the sending PSP, the receiving PSP, and the customer. We are currently co-chairing the Evidential Standards Working Group, where we hope to create an appropriate solution that all PSPs who sign up to the Code can implement. During the conversations at the Working Group thus far, we feel that some of the evidence, including general principles such as education and aftercare, may need to be monitored by the governing body to ensure a smooth investigation process.

We also suggest that the Steering Group should note concerns about how some of the principles should be shared. There are aspects of the Code which we feel would be inappropriate to share due to commercial and sensitivity concerns. This includes business analytics that underpin when effective warnings appear. The Steering Group should note that the framework may require regulatory underpinning for it to be fully transparent for consumers, consistent, and help mitigate first party fraud. This regulatory underpinning will need to ensure that the approval process for sharing confidential evidence is built in.

V. Timing

Whilst we recognise the importance in bringing in protections and reimbursement for consumers with respect to APP scams, it is of critical importance that the improvements being considered within the Code are implemented properly and thoroughly.

As such, it is imperative that appropriate and sufficient timelines are allowed with respect to the implementation of the Code and it is acknowledged that different PSPs may take different lengths of time to be compliant. This could potentially include a phased approach, as appropriate, to bring in protections as and when they are sufficiently developed, followed by the reimbursement principles with no issues remaining. This would then finally be followed by the reimbursement principles that have then subsequently been worked through during that period.

It is imperative that the Financial Ombudsman Service reflects these timelines in consideration of the Code in its adjudications. We believe that a robust holistic model will have a much greater impact than one being put out early when there are still outstanding issues that need to be considered.

Summary

In summary, we welcome the Code and believe that it represents an important step forward for industry and consumers. However, there remain a number of fundamental issues that require urgent attention from Government and Regulators if consumers are to be truly protected from the menace of APP scams. Barclays stand ready to be an active participant in these discussions, but believe that the challenge can only be surmounted with clear direction from policy makers, and via regulation.

Q1: Do you agree with the standards set out in the Standards for Firms?

Barclays are generally comfortable with the proposed Standards for Firms, which we believe will provide PSPs with additional clarity with respect to what further action they could undertake to provide further protections for consumers.

However, we would suggest that the following improvements and considerations are considered before the language is finalised and the Code is issued:

- The Code still contains some subjective language; we would suggest that this is amended in order to ensure a consistent interpretation is made by each organisation when implementing the Code, to ensure that consumers receive a consistent outcome. For example, SF1(2)(e)
    - (i): this principle describes the prevention messages before the customer makes the payment as: Understandable – in plain language, **intelligible and meaningful** to the Customer
    - (ii) Impactful – to **positively** affect Customer decision-making in a manner whereby the likelihood of an APP fraud succeeding is reduced
        - We would suggest that this section is inherently subjective, given that if the customer makes the payment, it is not positive. To resolve this, we would suggest that in (i) 'intelligible' and 'meaningful' are removed. For (ii), we would suggest that the entire clause is removed.
- As currently drafted, the Standards could result in a situation where a vulnerable customer has their ability to bank reduced or limited due to additional frictions (with the Code explicitly requiring that organisations undertake additional steps for the protection of those in vulnerable situations). Whilst we appreciate that some vulnerable consumers may require additional protection, it should be noted that this may result in a sub-optimal outcome in some consumers' minds. Regulatory underpinning could potentially help mitigate this from adding controls as to what the extra layer of protection looks like.
- We continue to be concerned by the positioning of Confirmation of Payee (CoP) with respect to the CRM. These concerns include:
    - The specification of a compliance date for CoP, as opposed to when the technology has been proven to be both 'live and stable'. A rush for compliance for what is new and far-reaching technology poses substantive resilience risks for firms and consumers, with potential consequences ranging far beyond the remit of the CRM.
    - CoP is currently positioned as being one of the core strands of the CRM approach. However, in terms of the volumes of potential scams that will be impacted, we do not believe the impact will be large. Inaccurate expectations on the efficacy of CoP in combatting APP scams should therefore not be included in the Code.
    - The Code explicitly states that CoP should not be implemented in a way where PSPs' priority is to de-risk their potential liability. We believe that this statement should be removed; it will be up to each PSP as to the level of friction that they introduce into their payment journeys as a component of the implementation of CoP.
- The standards should include a general statement to clarify that, in specific circumstances where the Code conflicts with the law, the PSP must follow the law. Without the Code being implemented through regulation, the legal basis for compliance with the code is uncertain and as a consequence actions taken by a PSP may potentially be subject to a legal challenge. This situation would not arise if the code has a regulatory underpinning.

- Further detail should be included to clarify the situations in which a Payment Initiation Service Providers (PISPs) or agency bank would be expected to display warnings on behalf of the sending firm, as it is acting as an intermediary.

- Finally, we believe that SF2(1) - covering how receiving banks open accounts - should be redrafted. As currently written, it suggests that documentary evidence of identity must be subject to independent verification; however, this is not accurate - it is the customer's identity that must be subject to independent verification. Additionally, there are exceptions to this requirement – for example, e-money products under the CDD threshold. As such, we recommend that this section is reworded to align with the Money Laundering Regulations 2017: '*Firms must open accounts in line with legal and regulatory requirements on Customer Due Diligence (CDD), taking into account industry guidance'*.

Q2: We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences - for example, whether this may enable firms to avoid reimbursing eligible victims.

Barclays notes that the tightening of this provision may inadvertently lead to some PSPs viewing compliance with the Code as being little more than a 'tick-box' exercise, and therefore will not lead to an improvement in customer outcomes. For example, 'effective warnings' may be unnecessarily displayed to consumers which would cause a higher friction and inconvenience for genuine payments and not have the right impact for APP scams.

Should this provision be tightened, it could also conflict with the 'shared-blame' scenario. Whilst this is still under discussion, we suggest that this section is not amended. More generally, customers' actions should always be taken into account

More generally, Barclays remain strongly of the view that, in order to provide the best foundations for consumers to be provided with security from APP scams, and reimbursement as appropriate in the event that they do fall victim, regulatory underpinning to any Code is a necessity.

Failing this, any Code will lack the universal application and legal backing required for real efficacy. Whether compliance with the Code would have helped prevent the APP scam from happening is important. Without this provision the Code attaches strict liability which discourage PSPs from subscribing to the Code. Strict liability as a legal concept is not appropriate for scams and places a disproportionate level of responsibility on PSPs.

More generally, we note that much of the activity undertaken today by PSPs with respect to protecting consumers who have been victim to a scam rests on voluntary cooperation and goodwill. The shift to a 'liability' model risks undermining this, and therefore we believe regulatory underpinnings are required to ensure that all PSPs play their role in supporting and protecting consumers, and are not inadvertently disincentivised from doing so.

Q3: We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

Barclays agree with the concept that in circumstances where consumers have met their requisite level of care, and the associated evidential standards have been met, that consumers should be reimbursed. However, there are a number of associated issues that require clarification to ensure that the CRM works as intended and consumers receive fair, consistent and appropriate treatment. We set out these issues elsewhere in our response.

In circumstances where it is accepted and evidenced that the customer has not met the requisite level of care expected of them, we do not believe that reimbursement from PSPs would be appropriate. To do so would not be consistent with the aim of the Code, would not be transparent, and would not be fair on those customers who have undertaken the appropriate levels of care expected of them. Importantly, it would also likely diminish the incentive for customers to act to protect themselves, increasing the prevalence of scams, and therefore the financial and non-financial detriment suffered by other victims, increasing the damage to the wider economy, and fueling organised crime. We note that PSPs would, in such cases, retain the right to consider a gesture of good will, dependent on the customer's circumstances.

To help understand this important issue in more detail, we believe that there is merit in the formation of a dedicated Working Group to test and review case studies, in order to more deeply understand the categorisation and recommended approach to different types of APP scams. For example, this work could be undertaken by the 'Reimbursement Process Flow Working Group', run by UK Finance.

We note, that - if such provisions were to be amended - PSPs are held financially liable for the vast majority of low-value scams, and that they may therefore be necessitated to apply friction to all payment transactions, resulting in an overall detriment to consumers - worsening the overall customer experience for all consumers across the country.

Q4: Do you agree with the steps customers should take to protect themselves?

Barclays welcomes the progress that has been made on the Customer Standards, of which we are generally supportive. By helping customers be equipped and incentivised to protect themselves, this will discourage criminals from attempting attacks, which in turn will reduce the overall prevalence of scams.

However, we believe that there are a number of important issues which require consideration before Code can be finalised. First, as with the PSP Standards, the Customer Standards contain numerous instances of subjective language, which could result in different interpretations by PSPs, and therefore inconsistent customer outcomes. For example, "recklessly" sharing computer access – where we would suggest that "recklessly" is removed, in an attempt to remove any subjective language and ensure a consistent understanding.

Secondly, Barclays continues to disagree with the inclusion of R2(1)(e) in the Customer Standards. We believe this will discourage business consumers from taking steps to protect themselves from scams. This is because, if an organisation does implement preventive steps, but doesn't follow them, then they will have a reduced likelihood of being reimbursed. However, should the organisation not have taken preventative steps, the principle of reduced likelihood of reimbursement would not hold, and the organisation will therefore have a greater chance of receiving reimbursement. Therefore, this principle would act to dissuade organisations from taking reasonable preventive steps, increasing the prevalence of scams, and should be removed.

Separately, given that it has been agreed at Steering Group that gross negligence can only be applied to unauthorised payments, Barclays believe that R2(1)(g) should be removed accordingly.

Q5: Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

Barclays agree with the proposal that vulnerable consumers should be reimbursed on a case-by-case basis and that, where possible, higher protection measures should be put in place to prevent these consumers from falling victim to scams in the first place. However, we note that vulnerability is a broad characteristic and PSPs cannot be expected to always accurately identify a customer as being in a vulnerable circumstance. As such, we believe

that this should not necessarily be held against a PSP when investigating whether the customer is eligible for reimbursement.

More generally, we would suggest that consideration should be given to the following points before finalising the Code:

- What further principles could be implemented regarding vulnerable consumers who repeatedly fall victim to scams, despite PSPs best efforts. We note that, in the absence of clear guidance in these instances, consumers could experience inconsistent reimbursement decisions across the industry. This could potentially include some extreme measures such as PSPs potentially reducing access to the account.

- The application of a vulnerability characteristics to larger businesses; including factors such as some businesses being at a higher risk due to the nature of trade. In addition to the tangible evidential framework, we suggest that further consideration be given as to what we believe will likely be an inevitable rise in first party fraud, that PSPs will experience.

Q6: Do you agree with the timeframe for notifying customers on the reimbursement decision?

Barclays are generally comfortable with the proposed timelines to investigate and reimburse consumers. However, we believe that further guidance on the following issues would provide welcome clarity to implementing firms: Firms must be entitled to fully investigate a complaint and reach a resolution prior to the complaint going to FOS. The consultation paragraph 3.81 suggests existing complaints processes should be followed, but this is inconsistent with the wording in R4 and could impact timelines for the customer receiving a final decision. We agree with the process whereby, if a customer is dissatisfied with a PSP('s) assessment, the customer should allow the PSPs to investigate the case fully before FOS rights are triggered. This is not currently included within the Code, but should be explicitly stated.

The Steering Group has agreed that if the PSP is awaiting evidence from the customer, and that this has not been provided within the 35-day timeline, then the customer becomes ineligible for reimbursement. This is not currently included within the Code, but should be explicitly stated. Not including this could result in a lack of transparency in what to expect from the investigation for the customer, and the potential risk in cases not being concluded within the timeframes agreed.

In addition to this, we do have concerns around the length of time that FOS will take to reach a determination on escalated cases and how this could impact the customer given the review they are currently undertaking regarding fraud and scams. Whilst we appreciate the need for this review, we suggest that they are given sufficient time to complete the backlog of cases they're currently holding, and upskill colleagues on the CRM before they start making decisions on reimbursement. Doing so will ensure that consistent decisions are made for the customer, and that colleagues at the FOS will only need to work one case a time.

For full transparency and customer experience, we also think it'd be beneficial if the FOS continue to commit to working to their ADR principles of 90 days under the Code. The Code should specify that the time limits do not apply where there are ongoing legal proceedings or where, for example, a PSP is awaiting approval from a body such as the National Crime Agency (NCA). For example, in cases where an alleged fraudster is identified and charged, but denies culpability, the Code should provide that the PSP can await the outcome of the legal proceedings before determining whether to pay compensation to the customer. This would be to avoid scenarios such as a PSP determining that the customer was defrauded and paying compensation, followed by a criminal jury acquitting the defendant because they do not believe the claimant's claims of having been defrauded. We note that the term "exceptional circumstance" is not clear, and believe that this should be clarified, to provide consistency in consumers' experience across PSPs. Furthermore, PSPs should have the ability to extend the timeframe, if doing so would enable a more thorough and accurate investigation to be completed.

Q7: Please provide feedback on the measures and tools in the Annex to the Code, and whether there any other measures or tools that should be included?

Barclays are generally comfortable with the measures and tools contained within the Code's Annex, and think this is a helpful tool. We would suggest that the Annex is updated on a regular basis, to ensure that it contains the latest and most effective measures and tools. However, we would make two recommendations:

- BSI PAS 17271: We note that this is not a kite-marked 'BSI' at the present time, and that we understand its future is unclear. As such, it will require updating given that the Code requires changes to the way in which vulnerable consumers are reimbursed. We note that there are a number of useful vulnerability documents in existence which could provide positive guidance to PSPs, including the 'UK Vulnerability Taskforce'.

- Confirmation of Payee: We note that CoP does not provide exhaustive and conclusive proof that the payee is the individual that the payer intended to pay. As such, the Annex should update its description, and remove the claim that CoP allows consumers to *"verify that they are paying the person they intend before transferring money."*

Consideration should be given to the appropriate approach to consultation for such updates in future.

Q8: Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

Barclays agree with the concept that in circumstances where consumers have met their requisite level of care, and the associated evidential standards have been met, that consumers should be reimbursed. However, there are a number of associated issues that require clarification to ensure that the CRM works as intended and consumers receive fair, consistent and appropriate treatment.

First, if a PSP has met their requisite levels of care, then – whilst consumers who have also met their requisite level of care should not be disadvantaged, and should be reimbursed – funding for any reimbursement must not come from the associated PSP. To determine otherwise would be to place an unjust and unprecedented liability on a non-responsible party. Furthermore, this would act as a clear disincentive for any smaller PSPs to sign-up to the Code, reducing the Code's efficacy and coverage, and therefore undermining the goal of preventing consumers from suffering harm as a result of APP scams. It also creates an expectation in consumers that their PSP will always reimburse their loss making all their payments effectively insured by their PSP. Barclays do not believe that it is possible, nor appropriate, for consumers in no blame scenarios to be reimbursed until a robust solution for this is in place. In addition to this, if it were determined that PSPs should fund all APP scams, even when they've followed the right level of care, this could lead to unintended negative consequences. These could include PSPs being forced to materially deteriorate the current payments experience. We fundamentally do not believe this is the right outcome for consumers, but doing so may leave PSPs with no choice but to explore different options in order to limit the potentially open-ended liability such a proposal would entail.

Second, as currently drafted the Code is unclear as to what the appropriate outcome is in the situation where a customer has been subject to an APP scam that results in a financial loss, but where only one of the parties involved is subscribed to the Code. In such a situation, assuming that blame is shared between two or more organisations, financial responsibility should be similarly shared. It is correct that the customer should not be negatively impacted as a result, but nor should a PSP be unfairly held responsible for liability unrelated to them, simply because they have undertaken to sign up to the Code and the other party has not. More generally, this issue raises the broader thematic problem associated with a voluntary Code, which impacts only a subset of market participants, as opposed to a regulator-mandated universal approach.

Third, PSPs should not be liable to meet the cost of reimbursement in situations where there has been no breach of either law or duty. In order to ensure a consistent outcome for consumers, we therefore recommend that

the Code be mandated. This is because in the instance of a customer losing greater than £150k as a result of an APP scam and not in FOS jurisdiction would not be in scope; resulting in an inconsistent and unfair outcome for consumers who lose larger sums of money.

Subject to these three issues being resolved within the final Code, Barclays are supportive of the approach suggested in the question. If the Steering Group are unable to implement a solution to resolve no blame scenarios, we feel that we may be unable to implement the related reimbursement aspects of the Code.

Q9: Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

Barclays agree with the principle, subject to the agreement to liability principles that make clear that PSPs which have met their requisite levels of care are not held liable for the reimbursement of the customer.

In addition, clarity is required with respect to cases where either of the PSPs are out of scope of the Code (including Corporates as the receiving PSP, if they are not signed up to the Code). If the receiving PSP is out of scope, it isn't right to expect the sending PSP to cover the cost of this loss, or for the customer to have no choice but to escalate it to the FOS to get it resolved. On the other hand, if the sending PSP isn't signed up to the Code, we feel that it is unfair for the receiving PSP to have to potentially be unnecessarily escalated to the FOS in order for them to be able to administer any potential reimbursements. Because of this, a timeline should be put in place to provide clarity and consistency for the transfer of any funds (including relevant indemnities).

In no blame scenarios, funds should be directly sent to the sending PSP so they can reimburse the customer without occurring an unnecessary loss first. However, to do this, where the funding comes from for no blame scenarios needs to be established, and we feel that PSPs wouldn't be unable to reimburse consumers until this model is in place. If it's determined that PSPs should reimburse until the funding's established, PSPs would run the potential risk in smaller PSPs may not be able to afford to sign up to the Code, and PSPs having to explore other ways to fund the open ended liability; this would include areas such as materially slowing down the current payments experience for consumers. Understandably, we don't think this is the right outcome for anyone, but feel that this may be something that has to be explored as a result.

Finally, we suggest that a mechanism for dealing with inter-PSP disputes is enacted.

Q10: What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?

We note that working group is currently reviewing the different approaches to funding. Barclays' principle position on funding matters is that a primary focus of policy, regulatory and industry efforts should be on preventing scams from occurring at source (i.e. through an approach that engages the entire ecosystem, and places responsibility on all of those who enable this criminal activity to take place), and immediately after they have been initiated (i.e. through repatriation). Further focus and effort on both of these are still required.

More broadly, any funding solution with respect to reimbursement must be based upon either regulatory or legislative underpinnings. This will enable the proper assessment of liability within the whole ecosystem, ensuring that those who are responsible contribute proportionally to the reimbursement of consumers.

For those cases where – due to the lack of all stakeholders in the ecosystem participating initially, or in cases of 'no-blame' on either party – liability cannot be placed on an individual or organisation, we remain of the belief that Government should strongly consider the potential for reimbursement to be funded through dormant assets. To place financial liability in such cases upon PSPs would be manifestly unjust, and set out a dangerous precedent which PSPs would likely be forced to challenge through all available routes. In addition, we believe

there is merit in the Government considering the potential for such reimbursement to be funded through the use of funds held by a bank, which have been removed from customers' accounts on the basis that they are suspected to constitute the proceeds of crime. A significant proportion of such funds are likely to originate from scam-related activity.

We are fully supportive in having a sustainable model in place so consumers who have followed the right level of care are reimbursed. However, Barclays can't see how it's feasible for consumers in no blame scenarios to be reimbursed at all until a robust solution for this is in place to fund this.

As the Code develops, if it becomes expected for PSPs to bear the loss in these situations- even when they've followed the level of care expected from them from the Code- as positioned in previous answers, they would need to explore how to fund this open ended liability. Whilst we fundamentally disagree with this concept, it may leave us with no choice but to explore different options such as additional friction within the payments system.

Q11: How can firms and customers both demonstrate they have met the expectations and followed the standards in the Code?

In order for consistency, transparency, and the right customer outcome, it is important that all three parties involved in the APP scam produce tangible evidence. There are some aspects that should build part of the investigation:

- The sending PSP should be responsible for collation of the evidence if they're also administrating the reimbursement.

- Where possible, firms should try and build as much of the evidence as possible into their systems. These could include attestation boxes consumers can select to say they understand the warning that's been shown to them. However, we feel that this should be something that all PSPs who sign up to the Code are comfortable with agreeing to and have the capabilities to implement it.

- It is not only paramount for the customer that they produce evidence for a transparent and consistent experience, but also because of the first party fraud risks associated with the Code. It should be expected that the customer should provide evidence as to how they were contacted by the fraudster. This could include emails, SMS', and phone records. Doing this will allow PSPs to analyse how the customer could've satisfied themselves as the payee.

- In order to maintain consistent decisions and transparency, consumers in vulnerable situations should be expected to demonstrate some evidence. Some cases will involve the PSP already having it on record, but others will require something. This should be assessed on a case by case basis but some guidance should be given to PSPs within the Code.

There also needs to be some form of consideration to the more general principles and how these would be evidenced. These include customer education, colleague training, and victim aftercare. Evidence which shouldn't be shared publically, such as risk based decisions for effective warnings, require a process so PSPs can share it confidentially with the FOS to aid the investigation. In addition to this, consideration needs to be given as to what evidence can be shared between PSPs to close investigations. As the regulator, the PSR should support the evidential working group to come up with feasible solutions.

Q12: Do you agree with the issues the evidential approach working group will consider?

Barclays support the issues proposed for consideration by the evidential approach working group. In particular, we believe that the requirement on all three parties to provide some form of tangible evidence is of paramount importance, including situations where consumers display vulnerability characteristics. This is necessary in order to ensure that a fair apportionment of responsibility can be made.

We appreciate the importance that the evidential standards are not just based on each individual case, and that some aspects will need a strong governance framework to ensure PSP compliance. These include systemic factors such as evidence of aftercare, and colleague education.

It is worth noting that there are aspects of the Code which we feel would be inappropriate to share as evidence due to data protection, and the risk it would have by exposing business decisions. This includes business analytics that underpin when effective warnings appear. The evidential working group will need to consider what the approval process for sharing information with the FOS and across the sending and receiving PSP on these cases are, and potentially seek support on this from the PSR. Regulation underpinning would help as the PSR will be able to review and approve aspects such as risk based decisions, and training plans.

As a general point, should a consensus not be reached on this issue, we believe that formal regulatory direction will be necessary.

Q13: Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

Barclays are comfortable that the evidential approach working group have taken the appropriate approach to delivering an effective and evidence-based framework. However, as highlighted in previous answers, there is one core issue that should be considered before implementation of the Code. There are aspects of the Code which we feel would be inappropriate to share as evidence due to data protection, and the risk it would have by exposing business decisions. This includes business analytics that underpin when effective warnings appear. The evidential working group will need to consider what the approval process for these cases are, and potentially seek support on this from the PSR, due to the fact that this information won't be able to be shared publically or with the FOS. Regulation underpinning would help as the PSR will be able to review and approve aspects such as risk based decisions, and training plans.

As a more general observation for consideration by the Steering Group, we believe that further thought needs to be given to the scenario in which one or more parties are unable to supply evidence that meets the framework.

Q14: How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

To ensure that there is a consistent investigation process and outcome across the industry for vulnerable consumers across PSPs, and to mitigate the risk of first party fraud, we believe that vulnerability should be evidenced when investigating the case.

PSPs may already hold some evidence to demonstrate vulnerability. Evidence like this could be used to reflect the customer's vulnerability and how this could've contributed to the APP scam during the investigation process. However, given how broad it can be, it is not right to expect PSPs to always know if their customer is in a vulnerable circumstance.

When the victim informs the PSP that they're in a vulnerable situation during the investigation process, the evidential framework should consider building in evidence the customer could provide. We believe that each case needs to be assessed on its own merit, and that requirements to demonstrate vulnerability should be built

into the framework; examples in this scope that could be considered could include medical letters, or family testimonies. Given the nature, this will need to be agreed by all of those signing up. Doing so will not only help mitigate the risk of first party fraud, but more importantly, ensures full transparency for consumers so they know what the investigation will look like if they fall victim.

Q15: Please provide views on which body would be appropriate to govern the Code.

Barclays notes that important questions remain with respect to the governance of the Code. We are clear that – in order to achieve the original objectives of the Code, and to have a meaningful chance to offer real and substantive protections for consumers against being a victim of APP scams in the first place – regulatory oversight of the Code and associated activity is a necessity.

As such, our clear position is that the PSR should be made the accountable organisation for oversight of the Code. With experience in this area, forming the initial proposal, creating the Steering Group, and having a firm oversight of progress throughout, we believe that there is no other body who could be more qualified to govern the Code. If the PSR choose not to take this role, then it could cause a delay in implementation in finding a body who could do it, and not hold the same weight as a body with regulatory backing. This decision would ultimately have a direct impact on our consumers.

With respect to taking forward the next steps in designing and driving forward an eco-system led approach to combatting APP scams, we believe that this role could be undertaken by the PSR, but that there may also be merit in this being undertaken in conjunction with the Home Office, given their eco-system wide perspective and broader responsibility for combatting economic crime.

Q16: Do you have any feedback on how changes to the Code should be made?

Barclays believe that the Code should be underpinned by regulation, with our clear position being that the PSR should be made the accountable organisation for oversight of the Code. Any changes that are made to the Code should be in line with the current procedures in place to support it.

Q17: Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

Barclays recognise that in situations where both the sending and receiving PSP bear responsibility for the customer's loss, in accordance with the standards set out in the Code, both PSPs should share responsibility for reimbursing the customer. Whilst we appreciate the efficiency of a 'simple-split', we believe that a more appropriate approach would be one that recognised greater- and lesser-degrees of responsibility between the PSPs, i.e. where one is more responsible than the other, and therefore bears more financial responsibility.

In order to establish what the most appropriate split ratio would be, Barclays suggest that a number of cases should be run through a 'test methodology' in order to thoroughly understand the different approaches that are available, and to determine which is most appropriate.

Finally, we would suggest that further consideration should be given to the following situations:

i. The ratio split in the event where a customer and both PSPs are 'at fault';

ii. The outcome where a PSP is 'at fault' but is not subject to or in-scope of the Code (and the customer is unaware/unwilling to escalate to the FOS); and

iii. The outcome where an agency PSP or PISP has initiated a scam payment, and the extent to which this action should imply that they bear some (or potentially all, depending on the case) of the cost to reimburse the victim (and the means by which this would be implemented).

A robust solution must be implemented before PSPs are able to bear the loss and implement the reimbursement principles highlighted in the Code.

Q18: Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the Code?

The industry anticipates an increase in complex APP scam cases to be reported once the Code has been issued. Because of this, we feel that further granular work is required to establish how quickly decisions could be made before determining whether this model would be appropriate to use for the Code. Implementing something that hasn't been properly tested for efficiency could create a backlog of outstanding decisions for consumers.

Barclays believe that the most appropriate call to action is to run cases through a simple apportionment process to establish what the ratio split would be depending on the scam type.

Q19: What issues or risks do we need to consider when designing a dispute mechanism?

Barclays agrees in the need to establish a dispute mechanism. In designing this, we are strongly of the opinion that - in order for it to be effective and achieve the aims stated - it requires either regulatory or legislative underpinnings. This will ensure consistent and impartial outcomes, and the involvement of all PSPs (along with associated consequences for not complying with procedures). Furthermore, it should be 'owned' by an impartial body that provides PSPs and consumers with the reassurance that they will be treated fairly and their case judged on its merits (with neither the Steering Group, nor the FOS, being appropriate for this purpose).

In designing the mechanism, an important risk that should be carefully considered is that – without careful thought – the process could become overly complex, undermining its ability to resolve disputes. Fundamentally, the process should be built around an ability to digest each case on its merit and ensure that each PSP and/or customer at fault has the proportion of losses correct. However, it must also be simple enough that consumers can understand the rationale for why they received their reimbursement (and its level).

We also note that such a mechanism could take a considerable amount of time to design and implement. Its designers will need to consider how to build a tool that utilises the latest advances in algorithmic/big data analysis, appropriate governance procedures, and storage capabilities that are GDPR compliant. Given the mechanism's importance to the broader credibility of the Code, we strongly advise that it is built 'right', not 'quick', and that a rush to establish this for early-2019 should not undermine the mechanism (and therefore the Code) before it even has chance to become effective. Understandably, PSPs would not be in a position to reimburse consumers until this mechanism has been implemented.

Q20: What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the Code? How might the negative impacts be addressed?

Overall, the Code should have the impact of reducing the eventual financial detriment to consumers who are fall victim to scams (subject to their having taken reasonable steps), greater consistency in the treatment of victims across industry, and greater preventive controls from those who participate with the Code.

However, as currently designed the Code's potential benefits are focused on putting consumers back in the financial position they would have been in, had the scam not occurred in the first place. Whilst this is an important and necessary development, Barclays strongly believe that a primary focus of any policy effort should be preventing scams from occurring in the first place and where this is not possible, ensuring that those responsible do not profit from their criminal efforts. This will require greater focus on proactive initiatives and the improved recovery of funds via repatriation. Taking the profit out of crime for fraudsters will in turn reduce attempts.

The Code rightly includes measures to ensure that in-scope Payment Service Providers (PSPs) undertake all reasonable efforts to deter and prevent scams from occurring through either their accounts or their payment 'rails'. However, as currently drafted, its efficacy is necessarily limited due to two exclusions:

1. The first is the exclusion of out-of-scope PSPs; Barclays are therefore firmly of the opinion that the Code needs to be mandatory and have a regulatory or legislative basis, with all PSPs subject to its provisions.
2. The second is the exclusion of the non-PSP organisations which facilitate scams – including but not limited to: platforms, technology firms, telecom firms, and pension funds. Barclays is similarly strongly of the belief that these organisations must be brought into the scope of the CRM and related activities if policy makers hope to have any impact on combating scams at their source, and therefore sparing consumers from the financial and emotional hardship that accompanies being victim of a scam. This would additionally support the principle of a regulatory level playing field (same risk, same regulation), an important principle of the UK's regulatory environment.

Barclays believes that policy makers – including both Government and Regulators – should take the opportunity that has been presented by the analysis undertaken under the CRM Code's drafting process to take a long-term, strategic and encompassing view of the steps that are required from all the players in the APP scams ecosystem to stop scams before they have an impact on any consumers.

Importantly, we are concerned that the Code is limited to a focus on the largest PSPs. We believe that solving this problem requires full participation from all PSPs and from all those who feature in the "scams ecosystem", including the platforms and technology firms who often host or enable the nefarious elements that undertake these criminal activities, along with organisations that allow their security to be breached, therefore placing consumers' data at risk of being used by criminals to enable either fraud or scams.

Extending regulation so that these actors ensure that their systems and services cannot be used by fraudsters should be a greater priority. Making PSPs solely responsible for compensating victims would distort incentives in what is becoming a complex, integrated market involving multiple entities. The Code does not address this fundamental point, and we would strongly urge Government, the PSR and the FCA to consider what further action needs to be taken to ensure that scams are prevented at source. Dealing only with the consequences will only have limited effect and it will be very difficult to measure any success and the effectiveness of the Code. Scams are criminal activity and, as with any other criminal activity, prevention ought to be the prime focus of any policy efforts. Barclays stands ready to act in concert with other members of the ecosystem to make this a reality. Without this explicit inclusion, there will be gaps in both consumer protections and outcomes.

Consideration should also be given to the role of third party Payment Initiation Service Providers (PISPs) under the Code. Under Open Banking, PISPs will be able to make payments at customers' requests directly from the accounts they hold, using Faster Payments. PISPs must be covered by the Code, as otherwise there is a risk that a gap in consumer protections is created, which may undermine the success of Open Banking in driving

competition in the current account and payments markets. Not having these in scope could create an unintended complex experience for the consumer, who would not have the same protection levels if they were to fall victim to a scam.

In addition, there are a number of specific risks to consumers and industry that stem from the Code as currently drafted, which require serious consideration. These are:

i. Through the increased reimbursement of consumers, there is a risk that – without a parallel focus on ensuring consumers (and enabling platforms and others in the ecosystem) take reasonable steps to deter and prevent scams from occurring in the first place – the UK could become the 'scam capital of the world'. This is due to reduced incentives for consumers to protect themselves and less of a focus on targeting the criminals who undertake the scams. Indeed, we think it likely that fraudsters could place a greater focus on firms in the wider ecosystem to obtain customer details, and use this as the mechanism for even more sophisticated APP scams.

ii. In an effort to deter the prevalence of scams, PSPs will be forced to introduce ever greater levels of friction in all consumers' payment journeys. Although PSPs signing up to the Code will aim to implement effective warnings, the amount of consequent friction may result in genuine consumers becoming increasingly frustrated. In addition to this, Fraudsters quickly innovate and will quickly by-pass whatever prevention controls are put into place.

iii. The Code's lack of a mandatory (underpinned by regulation or legislation) basis will limit the potential protections (and therefore benefits) for consumers.

iv. There is currently a lack of consistency in the proposed treatment of consumers; consumers who lose over £150k and are not reimbursed will not necessarily have the same escalation support than those who lose under £150k receive. With the FOS jurisdiction escalation being limited to £150k, those who lose greater than this will be forced to resort to litigation. Without a legislative or regulatory basis, the courts will not have the tools to be able to reach the same conclusion as the FOS, meaning that those who have lost the most will not be able to benefit from the protections and support enjoyed by those who have lost smaller amounts.

v. The absence of a focus within the Code on strengthening the repatriation process will likely result in a greater amount of customer financial detriment. For example, in cases where a customer has not undertaken the requisite level of care expected, and the PSP did, the customer will not be entitled to reimbursement. However, the customer still has the potential to have their funds returned to them if these can be traced and returned through repatriation (with the consequent benefit of hampering the flow of funds to criminals).

vi. We believe that there is a key danger that some consumers – and especially those in vulnerable circumstances – will not escalate their case to the FOS if their PSP is not in scope of the Code and they are a fault. Without full participation, the greatest financial detriment and emotional distress will therefore fall on those most vulnerable. Given the broader regulatory and industry focus on protecting this subset of consumers, we feel that this is an issue which requires careful further consideration.

Q21: What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the Code? How might the negative impacts be addressed?

As we outline in our response to Q20, as currently designed, the Code's potential benefits are focused on putting consumers back in the financial position they would have been in, had the scam not occurred in the first place. Whilst this is an important and necessary improvement, Barclays strongly believe that a primary focus of any

policy efforts should be on preventing scams from occurring in the first place. This includes both the prevention of scams and the immediate recovery of funds from the criminals ('repatriation').

Furthermore, in order to achieve the stated aim of the Consultation (i.e. of providing a mechanism for consumers to be reimbursed when they are the victim of a scam), it is necessary to ensure that all the participants required to enable this reimbursement are subject to the Code. For this reason, Barclays are strongly of the view that the Code should be mandatory (for relevant firms) and have a regulatory basis. Should this not be the case, smaller and newer PSPs will not have an incentive to offer consumers the protections afforded in the Code, hampering efforts to combat scams and leaving consumers in an unclear state as to who offers them what protection. Furthermore, this would support the principle of a regulatory level playing field (same risk, same regulation), an important underpinning to the UK's regulatory environment.

More broadly, Barclays believes that policy makers – including both Government and Regulators – take the opportunity that has been presented by the analysis undertaken thus far under the CRM Code drafting process to take a long-term, strategic and encompassing view over the steps that are required from all the players in the APP scams ecosystem to stop scams before they have an impact on any consumers.

Importantly, we are concerned that the Code is limited to a focus on the largest Payment Service Providers (PSPs). We believe that solving this problem requires full participation from all PSPs, and further participation from all those who feature in the "scams ecosystem", including the platforms and technology firms who often host the nefarious elements that undertake these criminal activities, and organisations that allow their security to be breached, therefore placing consumers' data at risk of being used by criminals to enable either fraud or scams. Without the breadth of participation across the industry, consumers will not have the confidence of protection irrespective of how and with whom they choose to make payments.

Extending regulation so that these actors ensure that their systems and services cannot be used by fraudsters should be a greater priority. Making the PSPs solely responsible for compensating victims would distort incentives in what is becoming a complex, integrated market involving multiple entities. The Code does not address this fundamental point, and we would strongly urge Government, the PSR and the FCA to consider what further action needs to be taken to ensure that scams are prevented at source. Dealing only with the consequences will only have limited effect and it will be very difficult to measure any success and the effectiveness of the Code. Scams are criminal activity, as such, as with any other criminal activity, prevention ought to be the prime focus of any policy efforts. Barclays stands ready to act in concert with other members of the ecosystem to make this a reality. Without this explicit inclusion, there could be gaps in both consumer protections and outcomes, which is not the best consumer focused approach and could cause market distortions.

Whilst there are a number of positive impacts for PSPs that will likely result from the implementation of the Code, the following further issues should be carefully considered before the Code is finalised:

i. There is currently a lack of clarity with respect to expectation and responsibilities on PISPs, agency PSPs and Member Banking Systems (MSBs). Without this clarity of scope, there could potentially be cases where prevention could have occurred, but these organisations are not enabled to consider whether they should reimburse the customer. Given the rapid developments taking place within financial services with respect to the proliferation of new forms and types of payments, to ensure that consumers who choose to take advantage of new ways to pay are properly protected (and that these innovative new mechanisms are not therefore undermined and lose trust), we believe that the Steering Group must provide clarity that these organisations are within scope.

ii. There is a lack of requirement on smaller PSPs and non-PSPs to take steps to prevent scams from occurring. Not only does this necessarily increase the occurrence (and impact) of scams, and therefore increase customer detriment, but it undermines the work of PSPs to tackle this criminal activity.

iii. Without an alignment of the complaints process with current fraud procedures, consumers will likely lack clarity as to who they should complain to and what protections they are afforded, but this could also unnecessarily reflect poorly on PSPs who are signed up to the Code.

Q22: Are there any unintended consequences of the Code, particularly those which may impact on customers, which we should be aware of?

As set out in our responses to Q20 and Q21, as currently designed there are a number of potential negative impacts (or missed opportunities) within the Code which will impact on both consumers and PSPs (but which there is opportunity to redress, should policy makers choose to do so).

Q23: How should the effectiveness of the Code be measured?

The Code's effectiveness should be assessed against the extent to which it contributes positively to a reduction in the occurrence of scams. When scams do still occur, the Code's effectiveness must be measured against the extent which it enables consumers who have taken the appropriate steps to protect themselves to be reimbursed, with liability for that reimbursement sitting with the firms who have enabled the scam to take place.

Such measurement cannot be undertaken through a single means, and therefore a multi-faceted, data-driven approach must be designed. This should take account of the following considerations:

i. The Code cannot be expected to meaningfully reduce the preponderance of scams (and therefore customer impact) without having all PSPs in-scope. Without all PSPs being in scope, the measurement of metrics such as: complaints, losses, preventions and reimbursements cannot be viewed as comprehensive, and conclusions cannot necessarily be drawn from the data.

ii. Without all participants in the ecosystem being in scope, it is necessarily difficult to measure prevention accurately. Without all parties being brought within scope, it is likely that fraudsters will – upon the implementation of the CRM – turn their attentions to out-of-scope participants, resulting in an increase in scams enabled through these actors.

iii. A sole focus on complaint reduction would be misleading. PSP's complaint shares will vary in accordance with a number of factors, including their market share, and – indeed, their complaints being proportionally higher because they determine to implement a more stringent set of controls to combat scams (and if the customer then logs a complaint because they haven't been reimbursed, this isn't necessarily a reflection of the prevention controls the PSP has implemented).

iv. Careful thought should be given to the means in which any centrally collected statistics are made available; PSPs publicly sharing losses and preventions could potentially allow fraudsters to identify which PSP to target, which would create a risk in the increase in APP scams and fraud attacks taking place.

Given these challenges, and the recognised need to establish some form of assessment of the effectiveness of the Code, we would suggest that the following are considered:

i. Reimbursement volumes amalgamated across the industry to analyse how many consumers haven't suffered financial detriment as a result of the APP scam taking place.

ii. Customer held liable cases. These will assist the industry in understanding how effective the PSP care standards within the Code are.

iii. Industry marketing impact; measuring the success of joint industry ventures, such as Take 5, and standalone PSP activity;

iv. Aftercare and re-victimization occurrences; and

v. Customer group feedback.

When measuring the success of the code, it is important to remain cognisant that PSPs cannot control the amount of additional crime that will result because of the Code, and as a result the volumes are likely to increase.

Barclays is happy to work with whichever body governs the Code to support the work in putting some tangible success measures in place. These should be decided before the final Code is issued, so PSPs who sign up to the Code can implement the right reporting frameworks.

Additional questions for the Steering Group

Before the final Code is issued, we would appreciate guidance on the following issues and questions:

i. Clarification as to whether the following accounts are in-scope of the CRM:

   a. Consumers who have an account in the 'isles'

   b. Currency accounts

   c. BACs direct credit payments

ii. What would happen in the instance where the receiving account of the APP scam is a large business or corporate and therefore out of scope?

iii. What would happen to payments that are completed via push payment services that do not involve using the sort Code and account number, and how these would be handled within the Best Practice Standards which the Code is built on (e.g. services such as PayM)?

iv. Through the consultation document and the Code, both terms APP fraud and APP scams are used. For full customer transparency, and consistency in language, we suggest 'APP scam' is used consistently throughout.

v. For full transparency for consumers who had been scammed prior to the final Code being issued, further clarification to confirm that the Code is specifically for cases dated after the Code has been issued would be beneficial.

vi. We suggest that thought is given to considering the future scope of the CRM and how it may change, depending on factors such as the FOS jurisdiction limits.

vii. We are concerned that, whilst the FOS plays an important role in helping consumers resolve disputes, it is being asked to opine on an ever expanding range of issues and customer cohort – this includes its recent extension to its jurisdiction to include larger SMEs, and its potential extension to consider complaints in relation to a receiving bank in an APP scams.

This increasing remit is leading to PSPs having no certainty in terms of the applicable law and regulation which ultimately gives an inconsistent outcome for consumers. FOS adjudicating on whether or not firms and consumers met the standards under the Code will add to the work to be undertaken by FOS which we are concerned it is not adequately resourced or skilled to do.

Further, we are concerned that FOS will be acting in a quasi-judicial role which was not the purpose of their creation. For example, under the Code, a PSP may hold monies which are the alleged proceeds from a scam. The paying customer claims they are the victim of a scam and request the monies are returned. If the receiving PSP's customer claims the funds are genuine and they are not a scam, the receiving PSP cannot simply return the funds to the paying customer in reliance on the Code. Rather this would be a title claim to the money and in dealing with it the PSP must abide by the law. The paying customer may then complain to FOS under the Code forcing FOS to determine whether or not the title to the money is with the payer or the recipient.

We welcome views from the Steering Group as to how we can work together to mitigate the above points.

Yours sincerely,

Current Accounts, Payments, Insurance, and Information (CPII)

Dear Sir / Madam,

Thank you for the opportunity to respond to the consultation on the industry code for the reimbursement of victims of authorised push payment (APP) scams.

As ever, we have chosen to keep our comments tightly-focused on the key areas affecting Handelsbanken. We have therefore only addressed those areas where we feel our experiences add specific value or provide useful insight. In particular these relate to:

1. The scope and focus of the general expectations and standards for firms
2. How to fund the reimbursement of customers where the customer has not been grossly negligent, and no firm party to the code involved in the payment journey has breached any standards
3. Governance of the code going forwards

The scope and focus of the general expectations and standards for firms

Handelsbanken believes it is crucial that the general expectations and standards for firms to adhere to are scoped correctly. Whilst we agree with the categories of detection and prevention, we do not believe the latter is scoped adequately.

Prevention should start well before a payment is in process, and both Confirmation of Payee and customer warnings only focus on this late stage. It is our view that if proper Know Your Customer and due diligence checks are completed when accounts are opened - and that payment service providers (PSPs) such as banks truly know their customers - then accounts will not be opened for fraudsters.

This should be a clear and obvious starting point for both the code of conduct in relation to firm's standards, and also for liability and customer reimbursement: if a firm has opened an account for a fraudster, that firm should be liable for compensating the customer whom has been defrauded through an APP scam. Ongoing monitoring and due diligence checking by firms should also form a part of the standards firms have to adhere to; this would help identify and prevent the scope for mule accounts to be used for facilitating APP scams.

Without prevention being scoped in this manner, a huge number of APP scams will unrealistically - and inappropriately - be categorised with no party liable. This greatly disadvantages banks such as Handelsbanken, where our customers have been the victims of APP fraud, but where we have never been the beneficiary's bank in an APP scam.

How to fund the reimbursement of customers where the customer has not been grossly negligent, and no firm party to the code involved in the payment journey has breached any standards

We believe that, if the proper scoping and definition of firms' expectations and standards is achieved, there will - rightly - be fewer scenarios in which no party is liable and thus reimbursement should be jointly funded. However, in these circumstances, we would seek to avoid the implementation of a transaction charge on higher risk or higher value payments.

Governance of the code going forwards

It is Handelsbanken's preference, in the scenario where the PSR has ruled out taking on this responsibility itself, for the NPSO (now 'Pay.UK') to assume responsibility for the governance of the code.

HSBC BANK PLC

AUTHORISED PUSH PAYMENTS SCAMS STEERING GROUP:

DRAFT CONTINGENT REIMBURSEMENT MODEL CODE

RESPONSE TO CONSULTATION 28 SEPTEMBER 2018

14 NOVEMBER 2018

COVER SUBMISSION

Introduction

Following the establishment of the HSBC Group retail bank HSBC UK Bank plc on 1 July 2018, HSBC Bank plc (HSBC) is the UK's non-ring-fenced bank within the HSBC Group. HSBC Bank plc's customers in the UK include our Global Banking and Markets clients within our wholesale and investment banking division, relevant Financial Institutions, large UK Corporate Banking customers and customers of non-UK branches of HSBC Bank plc. This includes those customers for whom we provide Indirect Access to one or more of the UK's main payment systems via our own Direct Access to these systems under a contractual arrangement.

HSBC welcomes the opportunity to review and comment on the consultation issued by the Authorised Push Payments (APP) Scams Steering Group on the Contingent Reimbursement Model Code.

The scope of the Contingent Reimbursement Model Code applies to personal customers, micro enterprises (as defined under regulation 2(1) of the PSRs (employing fewer than 10 people and whose annual turnover is less than €2m), and Charities as defined under regulation 2(1) of the PSRs (annual income less than £1m).

The above sectors are managed by HSBC UK Bank plc and accordingly they have submitted a full response to the consultation.

However, there is one area which is not discussed in the Code but which may have a broader impact on non ring-fenced banking operations and where HSBC wishes to provide feedback. This is in the area of how the Code applies to Indirect Access to payment systems and Indirect Access Providers (of which HSBC is one).

The Code needs to consider and address where the Firm is an Indirect Access Provider and the payment is initiated or received by an Indirect PSP.

On this issue, the final Code must be clear that each legal entity is responsible for its role as a sending or receiving Firm in relation to an APP scam. Specifically, where a PSP provides a commercial access arrangement to another PSP requiring Indirect access services to UK Payment Systems, that sponsoring PSP is not responsible for APP scams relating to accounts with an Indirect PSP or the actions taken by that Indirect PSP. We believe that the sponsoring PSP is not responsible either when the victim is a customer of the Indirect PSP or when a payment is received into an Indirect PSP customer's account that is identified as the proceeds from an APP scam. The sponsoring PSP does not hold the bank/customer relationship and so cannot be responsible for the Indirect PSP's compliance with the Code or the reimbursement of the Indirect PSP's customer.

Similarly, there are instances where the receiving Firm will be an Indirect PSP. In this case, the Indirect Access Provider cannot be held responsible for Indirect PSP's level of care relating to account opening.

As a supplier of Indirect Access services, we will continue to communicate and provide information on all industry changes to our clients. In the event that the Code changes from its voluntary status to be regulatory or mandatory, we would of course work with our clients on a firmer basis.

This issue directly impacts on two of the consultation questions which are set out below:

Q9: Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

9.1 HSBC agrees that the reimbursement process should be between the sending Firm and its customer - this provides a level of simplicity for the victim - subject to there being an effective mechanism in place for the recovery of the compensation payment between the Firms.

9.2 We also strongly agree that the sending Firm should not be liable for the reimbursement where it has met the required standard for a sending Firm.

9.3 In the situation where the customer and sending Firm have met the appropriate standards of care, but the receiving Firm has not, there needs to be a clear mechanism for the receiving Firm to pay the sending Firm the cost of the refund. It is not clear at this stage whether this will be in place for when the Code is due to go live.

9.4 Consideration should also be given to what happens if the receiving Firm has not signed up to the Code, to ensure that Firms who have signed up to the Code are not funding reimbursement for the actions of Firms who have not signed up.

9.5 In the case where the sending Firm is acting as an Indirect Access Provider, the payment will be initiated by the Indirect PSP. In this case the sending Firm does not hold the bank/customer relationship and so cannot be held responsible for the Indirect PSP's compliance with the Code or the reimbursement of the Indirect PSP's customer.

Q17: Is a simple 50:50 apportionment for shared blame between firms appropriate? If not what is a sensible alternative?

17.1 Where there is shared blame between the customer's Firm (either the sending Firm or Indirect PSP) and the receiving Firm, our view is that at least initially, an equal apportionment of cost could reduce the numbers of disputes between Firms. However, this becomes complex depending on the nature of the respective blames and the materiality of the impact it had on the particular case. Thought also needs to be given to where blame is shared with a PSP who has not committed to the Code and where the remaining funding for the reimbursement comes from.

17.2 It will be important to ensure that the Code applies to all PSPs and electronic money institutions to ensure a consistent approach is achieved in apportioning costs. This principle applies irrespective of whether the institution is directly or indirectly participating in the relevant payment schemes. In particular the Indirect Access Provider cannot be held liable when it does not have the bank / customer relationship both from a sending and receiving perspective.

HSBC UK BANK PLC

AUTHORISED PUSH PAYMENTS SCAMS STEERING GROUP:

DRAFT CONTINGENT REIMBURSEMENT MODEL CODE

RESPONSE TO CONSULTATION 28 SEPTEMBER 2018

14 NOVEMBER 2018

COVER SUBMISSION

Introduction

HSBC UK Bank plc (HSBC UK) is the new ring-fenced UK retail bank within the HSBC Group, which opened on 1 July 2018. Our customers include HSBC personal and commercial customers in the UK, including those UK Business Banking customers categorised as Non-Bank Financial Institutions, UK Private Bank clients; HSBC UK also includes our other UK retail brands, M&S Bank and first direct.

HSBC UK welcomes the opportunity to review and comment on the consultation issued by the Authorised Push Payments (APP) Scams Steering Group on the Contingent Reimbursement Model Code.

HSBC UK recognises that the growth in APP Scams presents severe challenges to Firms and customers alike and we are committed to improving outcomes for victims of APP scams. For this reason, we have been supportive of the work undertaken by the industry to provide improved data on APP scams and to implement the industry Best Practice Standards (BPS) for victims contacting their Payment Service Provider (PSP), along with actions to be undertaken by the receiving PSP, including Confirmation of Payee.

HSBC Holdings Plc is a member of the APP Scams Steering Group.

We are committed to working towards implementing the Standards for Firms, and once the Code is finalised and issued, we are committed to implementing the Code. We have begun work to set this in train and remain committed to working with the industry and broader community to support the Code to achieve its objectives.

Throughout the development of the draft Code we have stressed the importance of ensuring that the final Code strikes the right balance between reducing the overall level of APP scams, protecting consumers and promoting the efficient functioning of the overall payments market; including evolving areas in the payments industry such as Open Banking, specifically Payment Initiation Service Providers (PISPs); and that the final Code is fully workable, widely adopted and aligned with the regulatory and legal landscape.

It is important to recognise that the Code is most effective if both Firms and their customers maintain vigilance against APP Scams, and that the main aim of the Code must be to ensure reduction in the level of APP Scams.

Our response below reiterates these points and provides our view on the outstanding issues set out in the consultation. In summary:

- Throughout the process and following discussions with our industry peers, we have supported and continue to support calls for regulation of the Code to ensure its adoption and effectiveness. Our concerns are that a voluntary Code cannot achieve the objectives of reducing APP scams nor protect consumers regardless of who they bank with. There are a number of elements of the Code which conflict with existing regulation or legislation; or which will require regulation, including around issues of

liability. A regulatory framework would provide a way of achieving the Code's aims and ensuring alignment with the wider regulatory and legislative landscape;

- We welcome the work of the evidential approach working group, and urge that their recommendations provide the clarity and consistency of approach needed for Firms and customers to demonstrate that they have met the required level of care. The complexity of agreeing and implementing these standards across multiple channels should not be underestimated and a period of implementation will be needed to allow the agreed standards to be adopted;

- More broadly, we support calls for an implementation period following publication to allow good operational preparation and provide the best customer outcomes from the outset. A number of elements of the Code, e.g. Confirmation of Payee, require major operational and technical change programmes and it is critical that there is sufficient time for this to be introduced effectively. We believe this should be supported by an industry programme to coordinate rollout to achieve consistency around non-competitive elements where possible;

- We do not believe Firms should, as a matter of principle, be responsible for funding reimbursement where they have met their level of care. To adopt such a model would deter Firms from committing to adhere to the Code, be a disincentive to invest in APP scam prevention, may distort competition and will not meet the objective of reducing APP scams. We support the work of the no-blame working group to consider the full range of funding options and suggest that this must be supported by cost benefit analysis and engagement with Government at a senior level where relevant before options are ruled out;

- Alongside additional layers of friction in the payment journey, to ensure customers have taken steps to protect themselves, there is a risk that the process of making a payment too complex for some customers. We are also concerned that an unintended consequence may be limitations on access to payment services where a customer is considered 'at risk' of APP scams. This could have the effect of limiting access to financial services – either directly or indirectly - for the most vulnerable in society and we do not support that outcome.

General Observations on the Consultation and Draft Code

Reducing APP Scams

We consider that the prime strategic aim of the Contingent Reimbursement Model (CRM) must be to reduce the volume of APP scams over a period of time. This is the first overarching provision of the draft Code, however, we reiterate our concern that we believe there is a real risk that the introduction of a CRM could, at least initially, see an increase in APP scams.

Although the draft Code has been developed to mitigate this risk where possible, we believe that a reimbursement environment may drive increased activity by scammers and reduce customer vigilance. There must be a mechanism to monitor this environment and to evolve the Code to respond accordingly through an appropriate governance model.

We also remain concerned that there will be attempts to bring out of scope fraud (first party fraud) into the APP Scam model along with conventional trade disputes.

More broadly, we do not believe the Code will stop APP scams from happening. A fully strategic and joined-up approach is required, in conjunction with the Home Office led Joint Fraud Task Force to provide Firms with the legal tools to be able to trace and recover funds at speed and deprive scammers of the funds.

The Voluntary Status of the Code

The Code and the industry Best Practice Standards (which parts of the Code are predicated on) are voluntary. Depending on the take-up of the Code across the industry, there could be unsatisfactory customer outcomes. This risks differing outcomes on complaints, which could undermine the Code and is neither fair to Firms who have invested in adhering to the Code nor to scam victims whose Firm (or receiving Firm) has not signed up. For example, if a receiving PSP is to blame but has not committed to the Code, the sending PSP will reimburse the victim but be without recourse to a refund. There is also a risk of stifling innovation to meet changing customer needs and requirements.

Nonetheless, such fairness must be balanced against the size and scale of different PSPs in the market and it is important the final Code does not create undue barriers or burdens for smaller players or otherwise distort competition. For example, the investment required for implementing the standards for Firms and/or the cost of reimbursing eligible victims may not be possible within a Firm's business model for offering a credit payment transfer facility (on which there is typically no margin like interchange fees on card payments).

Furthermore, there are a number of elements of the Code which conflict with the regulatory and legislative landscape on payment services including:

- No statutory basis to delay a payment under the Payment Services Regulations 2017;
- No statutory basis to freeze funds in these circumstances;
- No statutory basis to repatriate funds to a victim of an APP scam; and
- Conflicts and overlaps with the FCA Handbook oversight of Systems and Controls, the Senior Managers Regime where the FOS adjudicates on a Firm's identification of mule accounts.

Given that the Code is voluntary, it is currently unclear how it will be applied by the Financial Ombudsman Service (FOS). The FOS takes into account industry codes of practice when deciding what is fair and reasonable. Our experience of the FOS approach to other issues – such as PPI – is that it considers codes to represent good industry practice whether or not the Firm being complained about has signed up to that specific code. This means it is

possible that, in its adjudications, the FOS might not draw a distinction between Firms that have committed to adhere to the Code and Firms that have not. Furthermore, assuming the final Code will be taken into account by the FOS when determining complaints regarding APP scams, for both paying and receiving PSPs, there is a risk that a body of cases will build that will effectively make the Code mandatory.

We understand that the FOS' own approach to APP scams is under review and we do not yet know how it will take account of the final Code. Therefore it is even possible that the FOS could take an approach which differs to the Code, irrespective of whether a Firm has committed to the Code.

Given the above complexities, HSBC UK believes the Code should be brought into the regulatory framework for payment services, to ensure its widespread adoption, effectiveness and alignment with the wider regulatory and legislative landscape. We believe a voluntary Code cannot achieve the objectives of reducing APP scams nor protect consumers in a consistent way, regardless of which PSP they use. A regulatory framework is the best way of achieving the Code's aims, creating a level playing field for PSPs and ensuring the rules on APP scams have a necessary regulatory or statutory underpinning.

Friction in payments

The Code is expected to increase friction in payment journeys. We regard some of this as positive (such as customer messaging) in that it will help to reduce the risk of APP scams and encourage customers to pause and consider the risk of APP scams before making a payment. However, as work progresses to ensure Firms are able to evidence and drive customers to take steps to protect themselves, it is inevitable that more friction will be put into the systems and services customers use, for instance more robust querying of customers' payments. Inevitably some customers may find payment services more complex to use and there will be disruptions to genuine customer payments, albeit for legitimate, well intended reasons which will be an unfortunate consequence of the Code. As noted above, there may not be lawful grounds for delaying payments under the Payment Services Regulations 2017.

Implementation

The implementation timescales for the final Code are challenging. A number of elements of the Code require major operational and technical change programmes and a suite of legal and operational questions on the draft Code remain outstanding. The implementation timetable should take into account customer outcomes first. A timetable that leads to a poor customer experience for the first victims of scams to use the Code and a failure to deliver on the Code's Core Principles such as 'Consistency of Outcome' would not be welcome.

Confirmation of Payee will be a very important tool to protect against APP scams but its implementation is complex and challenging, particularly given the volume and scale of other change in the payments ecosystem during 2018-9. Implementation timescales will again be important to ensure a consistent approach across Firms and optimum customer experience. We are aware that the PSR will shortly be consulting on issuing a General Direction in relation to implementation which we will review and respond to in due course.

Whilst we recognise that until the final Code is in place, victims continue to be without recourse to formal reimbursement (beyond current industry practice on goodwill payments), HSBC UK urges that delivery of the final Code is not rushed and that a period from publication to implementation is provided to enable good operational preparation. This could be phased, to allow those elements a Firm can put in place quickly to be delivered, such as customer education, allowing the technically and operationally challenging aspects to be delivered with due care. If implementation is rushed there is a risk of poor customer outcomes, inconsistent results and insufficiently tested controls.

We would also suggest an industry programme to coordinate the initial roll out of the Code. This will enable non-competitive elements, where standardisation is beneficial (such as common customer messaging), to be identified and coordinated; and support a better customer experience of the changes. This is particularly critical in relation to Confirmation of Payee, where much greater coordination is needed to launch a cross-industry change in customer experience successfully. In particular, common rules are needed around matching standards and how 'partial matches' will be presented to maximise the benefits of Confirmation of Payee functionality.

Outstanding Questions

As the consultation acknowledges, there are still a number of critical outstanding questions.

Funding reimbursement when all parties have met their level of care

We do not believe Firms should, as a matter of principle, be responsible for funding reimbursement where they have met their level of care. To adopt such a model would create a longstanding and unquantified risk, deter Firms from adopting the Code, be a disincentive to invest in APP scam prevention, may distort competition (and some Firms exiting the market) and will not meet the objective of reducing APP scams. There are a range of other parties (such as telecoms companies and data handlers) that have a role to play in the broad prevention of APP scams and it is not fair to place the burden of reimbursement on one party only.

We welcome the focus of the no-blame working group to consider the range of options and encourage this group to consider potential solutions in a fair and balanced way, which should include full cost-benefit analysis and, where relevant, be considered at a senior level in government. We encourage full consideration of legislative solutions that follow precedents elsewhere such as the Criminal Injuries Compensation Scheme.

Standards of evidence – Firms' and customers' level of care

Clarity is needed regarding the standard of evidence that will be required by Firms to demonstrate that they have met the required level of care to their customers or as a receiving PSP. A clear evidential approach is critical to ensure a robust and consistent implementation of the final Code, to encourage PSPs to adopt it, and to ensure eligible victims are reimbursed. We welcome the work of the evidential approach working group, however, in the absence of certainty on the evidential approach, preparing for implementation remains challenging.

For customers, the draft Code has designed the provisions governing the reimbursement of victims so that it is presumed a victim will be reimbursed unless any of the matters set out in R2(1) and (2) of the draft Code can be established. We believe customers should be required to take positive steps to avoid APP scams, which fit with a clear evidence framework to provide a clear balance of risk and responsibility between Firm and customer.

Whilst we support an approach that provides a different treatment to evidential standards for customers who may be considered vulnerable, we are however, concerned that this may result in unintended consequences. A consequence may be PSPs choosing to undertake a KYC impact assessment to assess vulnerability against the broad definition in the Code and limit access to payment services or increase costs if Firms feel the cost of complying with the Code is prohibitive.

Alongside additional layers of friction in the payment journey, to ensure customers have taken steps to protect themselves, there is a risk that the process of making a payment becomes too complex for some customers. This could have the effect of limiting access to financial services – either directly or indirectly - for the most vulnerable in society and we do not support that outcome.

Governance and operation

The governance and operation of the final Code must be resolved before it can go live. Roll out is likely to require considerable cross industry collaboration, to create new inter-PSP communications and processes and to share solutions and best practice. A long term solution is required that can manage the emerging challenges of the Code, review effectiveness independently and evolve the Code accordingly. As set out above, we believe that a regulatory approach is the most appropriate way to resolve this challenge.

As the consultation acknowledges, the outstanding issues highlighted are not exhaustive. For example, the consultation does not cover the governance of the Steering Group and how the final decisions on the outstanding issues will be made (including those not consulted on in this consultation), the implementation timetable nor the reimbursement model in a 'shared blame' scenario where both customer and Firm(s) have not met their level of care. Given the importance of all the outstanding issues, and in the absence of a

regulatory approach to delivering the Code, we believe that a further public consultation would be necessary, to consult on the solutions to the outstanding issues and ensure that the best and fairest outcomes for the whole community are achieved.

Response to Consultation Questions

Q1: Do you agree with the standards set out in the Standards for Firms?

1.1 In broad terms, we agree with the standards set out in the draft Code's 'Standards for Firms.' However, there are a number of outstanding questions and concerns that HSBC has raised with the Steering Group regarding the Standards for Firms which we feel it is important to reiterate in our response to this consultation. These concerns cover:

a. Standard of evidence

b. Effective Warnings

c. The implementation of Confirmation of Payee

d. Delaying payments, freezing payments and repatriation of funds

e. Best Practice Standards

f. Identifying mule accounts

1.2 Firstly, the draft Code is not clear on the **standard of evidence** Firms would need to demonstrate that they have met the required level of care to their customers or as a receiving PSP. Standards and expectations need to be clearly documented as far as possible to ensure that there is a level of consistency across Firms. Furthermore, the challenge of implementing these changes should not be underestimated. Processes will need to be changed across multiple customer channels, alongside an already complex technical and regulatory change agenda in payments. We welcome the work of the Evidential Approach working group in considering this issue, but clarity on the standards for evidence is essential for planning the Code's successful implementation.

1.3 Furthermore, given the FCA Handbook sets out the regulatory control and oversight of Systems and Controls (SYSC) and the Senior Managers Certification Regime, requiring Firms to implement risk based controls, we have asked in the Steering Group and the Legal and Regulatory working group how a Firm will be assessed as having met this requirement. There remains a risk of conflict between these requirements and the requirements of the Code and this could present challenges for the Financial Ombudsman Service (FOS) if they find they are assessing controls which fall within the jurisdiction of the FCA.

1.4 We support the Code's emphasis on **Effective Warnings** to customers, including appropriate actions for those customers to take to protect themselves from APP scams. However, the draft Code suggests an expectation of different warnings being developed for a variety of customer types and in understandable language. This presents a considerable implementation challenge, not least in terms of testing time to develop messages that are impactful and meaningful to customers and to ensure messages are appropriate for different customer types that leads to prompt customer response.

1.5 **Confirmation of Payee** is an important tool in APP scam prevention. However, like many other PSPs, implementing a Confirmation of Payee solution requires complex and challenging operational change across a number of channels and technologies, alongside an already complex technical and regulatory change agenda.

1.6 Our current expectation is that there will be a high degree of 'partial matches' given different PSP account naming standards, including marital and business names. Whilst we would expect volumes of partial matches to reduce once Confirmation of Payee solutions become established and more refined, the Code is not clear on the status of a 'partial match' and it is essential that the industry has clarity on how such cases will be treated.

1.7 As noted above, we would like to see a much greater degree of industry coordination and collaboration on the delivery of Confirmation of Payee to support a better customer experience of the service and to ensure it delivers the intended benefits.

1.8 We note that Firms are encouraged to take steps to **delay payments** where there are concerns about APP scams. However, there is currently no legal basis to delay a payment beyond standard fraud checks, and to do so would be contrary to the Payment Service Regulations 2017 and may breach the contractual relationship between the PSP and customer. PSPs cannot be expected to do this under current regulations.

1.9 Likewise, the draft Code is not clear on the legal basis for **freezing funds** on identifying concerns that they may be the proceeds of an APP scam. If a Consent/Defence against Anti-Money Laundering Suspicious Activity Report (DAML SAR) is submitted, the reporting PSP will be under an obligation to freeze the funds pending consent or a freezing order. In the absence of a statutory basis, PSPs will need to consider whether this is permitted under their customer's terms and conditions. The law does not oblige PSPs to do this, instead banks carry the risk whilst trying to reimburse victims where they can.

1.10 Within the CRM process, we have challenged this point in the draft Code as it appears to oblige PSPs to freeze funds without an underlying change in law. If the Code requires banks to amend their terms and conditions to allow funds to be frozen, then an underlying legislative change is required.

1.11 In terms of **repatriation**, the industry Best Practice Standards (BPS) stop at the point at which receiving Firms determine whether or not they would return funds in a beneficiary account to the victim. These standards, deliberately, do not place any obligation on the PSPs to return the funds to the victim, because there is no timely or efficient legal means to repay funds to the victims of an APP Scam. Instead, in the absence of legislative change, the BPS allows for the current status quo whereby receiving PSPs weigh up the litigation risk of:

a. Paying funds to the victim, and risking a claim for breach of mandate by its customer for removing funds on a PSP's determination of perceived

wrongdoing (with no required burden of proof) and returning them to the victim; and

b. Paying the funds to the receiving customer and risking a claim by the victim for breach of constructive trust in respect of the funds the PSP held, potentially comprising some or all of their scam payment.

1.12 It is not yet clear how the FOS intends to adjudicate whether the bank has assessed this correctly and whether it has met a required (yet to be defined) standard of evidence. There is a difference between civil (balance of probabilities) and criminal (beyond reasonable doubt) evidential standards and the banks will not have the full facts in the same way as a court in order to make legally sound determination which the FOS can then assess. In our view, legislation is needed to provide the legal foundation for banks to repatriate funds and protect PSPs and customers against the risks set out above.

1.13 In a number of places, the Standards for Firms place a reliance on the Best Practice Standards (BPS). However, the BPS are voluntary and many PSPs are not participating in the BPS. We suggest that the Code make clear that committing to the Code includes adoption of the BPS.

1.14 As a receiving Firm, HSBC works hard to identify accounts that are used for any fraudulent purpose, including mules, and to respond quickly when we do so. However, it should be noted that there are significant difficulties in identifying money mule accounts, particularly before they are used for the first time to handle fraudulently transferred funds. Both law enforcement and industry initiatives have identified that fraudsters often recruit customers with existing payment accounts to be mules, with the payment account opened legitimately, with valid documentation and no criminal record or other fraud risk factors.

1.15 To support our identification of accounts being used for fraudulent purposes, including mules, we utilise a number of sophisticated system and risk based controls to support this, subject to FCA supervision and oversight. The FCA exercises these powers using its Handbook which sets out the regulatory control and oversight of Systems and Controls (SYSC) and the Senior Managers Certification Regime, which makes individuals personally accountable where they hold a Senior Manager Function. We note that there is a potential overlap with the FCA's SYSC regime and the SF2(3) in the draft Code, and potentially the FOS adjudicating on this aspect of the Code in relation to a Firm's system and risk based controls to identify a mule account. We suggest this potential overlap should be considered and clarified to avoid a risk of conflict between this regulation and the requirements of the Code.

Q2: We welcome views on whether the provision that Firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable Firms to avoid reimbursing eligible victims

2.1 The provision that Firms can consider whether compliance with a particular standard would have helped prevent the APP scam is an important provision to allow case by case consideration, for both Firms and customers. It is equally important that this provision is applicable for customers, as set out in R2(1), to ensure victims are only assessed on the basis of matters that would have had a material impact on preventing the APP scam that took place. Therefore it is fair that Firms can also consider compliance in relation to whether it would have helped prevent the APP scam against the Standards for Firms.

2.2 We do not accept that the policy means eligible victims will not be reimbursed, but rather that the Code will rightfully assess cases on an individual basis and taking into account those factors that have had a material impact.

Q3: We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of their parties have met their levels of care

3.1 To date, the Code does not address how cases should be dealt with when both Firm(s) and the customer have not met their level of care. Without a clear position on the overarching policy of reimbursement in such circumstances, it is not possible to determine how the provisions above might apply in this situation. However, we do not believe that a customer who has not met their standard of care should, as a matter of principle, be entitled to a reimbursement. It is only appropriate that a customer is reimbursed by the PSP where they have met their standard of care and a Firm(s) has not. This does not preclude individual Firms making a goodwill payment to their own customers, if it should chose to do so.

Q4: Do you agree with the steps customers should take to protect themselves

4.1 R2(1) (a) to (g) sets out those matters which Firms are expected to establish if they wish to choose not to reimburse a customer. As such, these are not steps which customers should take to protect themselves, but measures against which Firms must be able to provide evidence in order to consider whether to reimburse customers. The draft Code sets a low threshold with no need to evidence compliance with those standards.

4.2 In our view, a key strategic aim of the Code is to reduce the incidences of APP scams and therefore it is important to set out clear customer standards which will assist in

the reduction of fraud arising from APP scams. We would like to see the steps that customers should be expected to take to protect themselves framed as positive steps, set out as Standards for Customers in the Code.

4.3 These steps should be set out as specific, measurable and possible to evidence. We do not believe this is the case with the wording in the draft Code which is open to interpretation and non-specific.

4.4 In our view, the current draft Code sets a very high bar for Firms to challenge customers and includes a number of points which are not possible to evidence or very difficult to obtain for historical or longstanding scams (e.g. investment scams), particularly if customer records have been destroyed for legal reasons. Without significant change, it would be very difficult for Firms to refuse a customer claim on the basis that the standard of care has not been met. This has various unintended consequences, with Firms very open to First Party Fraud and risking increased activity by scammers targeting customers.

Q5: Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for Firms to provide extra protections?

5.1 We agree that it is important that customers who may be considered vulnerable receive extra help to protect themselves against APP scams and that they should receive different treatment in terms of reimbursement. However, in practical terms, the draft Code is not clear enough on how this should be put into practice, and the commentary in the consultation documents demonstrates that PSPs are expected to utilise a considerable degree of individual interpretation to determine both whether the customer is vulnerable, and whether this had a material impact on the customer's ability to protect themselves against that scam. This is therefore a very difficult area for PSPs to manage in a way that will provide consistent outcomes for customers. Specifically we note:

- It is inherently difficult to define a 'vulnerable customer' both at a customer and business level. As the consultation describes, just about anyone can become vulnerable to APP scams at any point and for many reasons. A restricted list of circumstances is not appropriate, nor is an open interpretation and will not bring consistent outcomes for customers;
- Determining vulnerability is operationally challenging for a PSP. To balance our duty of care and privacy of customers, it is difficult to put in place practical steps for customer facing staff to identify a vulnerable customer, particularly someone who may be temporarily vulnerable, and to protect them against APP scams;
- There may be a difference of opinion between the sending and receiving Firms as to whether the customer is vulnerable and whether this had a material impact on their ability to protect themselves against the APP scam.

This may result in scenarios where the sending PSP is arguing the customer should be reimbursed and the receiving PSP is disputing that point. Although the customer would be reimbursed by the sending PSP, this may be a challenging scenario for dispute resolution;

- Regrettably, without a standard of proof for vulnerable customers that can be evidenced in a sensitive way, an unintended consequence will be that consumers who have acted recklessly will claim they were vulnerable to the APP scam so as to receive reimbursement.

5.2 The British Institute of Standards PAS 17271 which is referenced in the draft Code provides some structure to what may be considered potential vulnerabilities. Although this provides some clarity, not all of them are relevant to APP scams and some vulnerabilities may only be relevant and / or appropriate to different types of scams.

5.3 We are concerned that an unintended consequence of the approach to vulnerable customers may be limitations on access to payment services where a customer is considered 'at risk' of APP scams. Furthermore, layers of friction in the payment journey to ensure customers have taken steps to protect themselves could make the process of making a payment too complex for some customers. This could have the effect of limiting access to financial services – either directly or indirectly - for the most vulnerable in society and we do not support that outcome.

5.4 Given the importance of supporting vulnerable customers and the operational challenges this presents, we suggest the Code is supported by a suite of case studies designed to provide greater clarity and consistency on how Firms should treat different scenarios. These case studies would describe a range of victim circumstances and scam scenarios and provide guidance on how the Code is expected to manage such cases, including scenarios where the customer is not determined as vulnerable, or where they are determined as vulnerable, but it is considered reasonable to expect them to have protected themselves. Case studies should be regularly updated with "real-world" case studies.

5.5 Consideration should be given as to whether reimbursement for one APP scam closes the door to future claims (e.g. consumer suffers an APP scam and is reimbursed and then makes future payments to the same or similar payee). We have seen APP scam cases where the same individual has been convinced by a fraudster to make a payment again, after they have been revealed to be a fraudster previously (for example, a romance scam where the fraudster persuades the individual they are in a relationship again); or fallen prey to a similar type of fraud again, such as an investment scam. There is currently no legal ground for refusing to execute a payment instruction from a customer unless there is clear evidence it is fraud.

Q6: Do you agree with the timeframe for notifying customers on the reimbursement decision?

6.1 Yes. We agree with the proposed timescale of informing the customer on the reimbursement decision no later than 15 Business days after the customer reported the fraud. However, it should be noted that this gives some Firms longer to consider than others, depending on whether they are open 5 or 7 days a week.

6.2 We also agree that there should be a longer time period of no more than 35 Business days in exceptional circumstances, provided the PSP advised the customer of this longer time frame.

Q7: Please provide feedback on the measures and tools in the Annex to the Code, and whether there are any other measures or tools that should be included?

7.1 Many of the measures and tools in the Annex to the Code are voluntary. Others have not yet begun implementation and therefore the status of these measures in relation to FOS adjudications is uncertain.

7.2 We understand that the work on the 'Consented Standardised Information Set Data Sharing' initiative is no longer being progressed and is therefore not relevant to include.

7.3 There is no indication of the channels which would be used for each of these measures or how their implementation interacts with the standards of care. For example, a number of the measures rely upon direct contract with the customer as part of the payment initiation, when payments are typically instructed through digital channels.

Q8: Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the Firms involved?

8.1 HSBC UK agrees in principle that customers meeting their requisite level of care should be reimbursed, regardless of whether the Firms have, or have not, met their requisite level of care. However, we do not believe that Firms should have liability for the reimbursement, if they have met the Firm's required standard of care.

8.2 It remains our view that there is a very real risk that such a model will be targeted by organised criminals who may quickly learn that manufactured APP scams could generate significant returns from PSPs reimbursing victims. This could run counter to a core aim of the Code, which is to reduce the occurrence of APP scams.

8.3 Critically, we must therefore ensure customers are vigilant. As per paragraph 3.49 in the consultation, it is presumed that a victim will be reimbursed unless good reason can be established that the customer should not be – and so evidence on the customer's level of care is critical, as described above and in our response to Question 4. The Evidential Working group needs to consider how this will work in practice, and how such evidence will be sourced against those steps the customer is expected to follow which are not within a PSP's line of sight. There need to be transparent and

clearly understood standards that the customer needs to meet to evidence that a customer has achieved the requisite level of care.

8.4 A key strategic aim of the Code is to reduce the incidences of APP scams and therefore it is important to set out clear customer standards which will assist in the reduction of fraud arising from APP scams. For parity we would like to see the steps customers can take and be expected to take to protect themselves set out as Standards for Customers in the Code.

Q9: Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

9.1 HSBC UK agrees that the reimbursement process should be between the sending firm and its customer - this provides a level of simplicity for the victim – subject to there being an effective mechanism in place for the recovery of the compensation payment between the Firms.

9.2 We also strongly agree that the sending Firm should not be liable for the reimbursement where it has met the required standard for a sending Firm.

9.3 In the situation where the customer and sending firm have met the appropriate standards of care, but the receiving Firm has not, there needs to be a clear mechanism for the receiving Firm to pay the sending Firm the cost of the refund. It is not clear at this stage whether this will be in place for when the Code is due to go live.

9.4 Consideration should also be given to what happens if the receiving Firm has not signed up to the Code, to ensure that Firms who have signed up to the Code are not funding reimbursement for the actions of Firms who have not signed up. We reiterate this demonstrates a clear need for a regulatory framework to underpin the Code to provide a level playing field for PSPs providing reimbursements to victims.

Q10: What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the Working Group consider?

10.1 As set out above, we do not believe Firms should be responsible for funding reimbursement where they have met their level of care. To adopt such a model would create a longstanding and unquantified risk, deter Firms from adopting the Code, be a disincentive to invest in APP scam prevention, may distort competition (and risks some Firms exiting the market) and will not meet the objective of reducing APP scams.

10.2 The options provided in the consultation divide broadly between higher charges being levied on customers (insurance or a higher transaction charge), an industry fund into which Firms and other parties (such as telecoms, data handlers) contribute, or a legislative change to unlock funds or provide a government run scheme.

10.3 HSBC UK considers it would be against the spirit of the Code for customers to effectively fund the reimbursement, either directly or as a result of a pricing increase,

which is likely to be the result of an industry funded approach. We do not support a transaction charge as we believe this goes against what our customers would consider acceptable.

10.4 We believe a fair and sustainable model for funding such reimbursement must be identified. We welcome the work of the no blame working group to consider the range of options and encourage this group to consider potential solutions in a fair and balanced way which should include full cost-benefit analysis and, where relevant, be considered at a senior level in government. We encourage full consideration of legislative solutions that follow precedents elsewhere such as the Criminal Injuries Compensation Scheme.

Q11: How can firms and customers both demonstrate they have met the expectations and followed the standards in the Code?

11.1 We agree that there is a need for a measurable, understood and consistently applied approach for both customer and Firm which shows that they have followed the standards in the Code. Otherwise there will be a large number of cases where it is not possible to ascertain with certainty whether standards have been met. More work is needed to determine the clear evidential standards for both Firms and customers. As noted above, there is a difference between civil (balance of probabilities) and criminal (beyond reasonable doubt) evidential standards and the banks will not have the full facts in the same way as a court in order to make legally sound determination.

11.2 The Confirmation of Payee service is rightly seen as a valuable tool in tackling APP scams and clear positive and negative results will assist in determining whether the requisite level of care has been achieved by the customer. However, there will be many incidences of "partial match results" partly due to different naming standards by banks, including marital names, the naming of joint accounts and business trading versus legal names.

11.3 Implementation of Confirmation of Payee is complex and challenging, particularly given the volume and scale of other change in the payments ecosystem during 2018-9. Care must be taken regarding the implementation timescale to ensure a consistent approach across Firms and optimum customer experience. We are aware that the PSR will shortly be consulting on issuing a General direction in relation to implementation which we will review and respond to in due course.

11.4 The evidential approach working group will need to carefully consider the evidence available in other areas of the standards and what is admissible. Evidence available from management information including call logs will need to be acceptable, for instance in showing if an Effective Warning has been given.

Q12: Do you agree with the issues the evidential approach Working Group will consider?

12.1 We support the need for an evidential approach which will allow Firms and customers to demonstrate that they have followed the standards in the Code and have met their duty of care.

12.2 The evidential approach should be measurable, understood and consistently applied. Otherwise there will be a large number of cases where it is not possible to ascertain with certainty whether standards have been met.

12.3 We therefore support the creation of the evidential approach working group to assess how Firms approach investigating and assessing whether Firms and customers have met their requisite level of care. This will include, but not be limited to, Confirmation of Payee responses, telephone call logs and email communication.

12.4 The communication to customers of the standards to meet their level of care should also to be considered.

12.5 The working group also needs to consider what happens when it is not possible to ascertain whether the standards, and so meeting the duty of care have been met. In this situation is it assumed that the level of care has not been met, unless it can be proven otherwise.

Q13: Do you recommend any other issues are considered by the evidential approach Working Group which are not set out above?

13.1 The working group needs to consider whether all parties in the payment journey need to provide evidence of meeting their duty of care. Although the Code is voluntary, in reality there are issues with this, and the Code would need to apply to all PSPs to provide a common experience of the Code across all customers. Many customers are "multi-banked" and so differences in approach would quickly become evident.

13.2 In respect of PSD2 and Open Banking we note that PSD2 requires parity of journey (or better) for the TPP channel so that health warnings and 'effective warnings' and Confirmation of Payee are permitted.

Q14: How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

14.1 As we set out above in response to question 5, it is difficult to define a vulnerable customer. As the consultation describes, just about anyone can become vulnerable to APP scams at any point in their lives, for many reasons. For this reason, determining and evidencing vulnerability is operationally challenging. To balance our duty of care and privacy of customers, PSPs are very limited in how an operational team can establish whether a customer is vulnerable and determine evidence of that vulnerability.

14.2 In our response to question 5 we suggested case studies that could describe a range of victim circumstances and scam scenarios and provide guidance on how the Code is expected to manage such cases, including scenarios where the customer is not determined as vulnerable, or where they are determined as vulnerable, but it is considered reasonable to expect them to have protected themselves. Examples of evidence should be developed alongside this, to provide acceptable parameters, and updated as real world cases are experienced to share best practices to protect consumers.

Q15: Please provide views on which body would be appropriate to govern the Code

15.1 HSBC UK concurs that it is important to determine the governance function for the Code as it is implemented and to oversee future developments. We agree that UK Finance is not the correct body given its role as a trade body representing banks and others in the payments industry.

15.2 We consider that the Steering Group is not an appropriate body to govern the Code in the long term.

15.3 Given the challenges of managing a voluntary Code, we reiterate our position that we believe the Code should be a regulatory initiative.

Q16: Do you have any feedback on how changes in the Code should be made?

16.1 As outlined elsewhere, we remain concerned that the Code is being introduced very rapidly whilst it is still being developed and finalised, which increases the risk of an inconsistent customer and Firm experience.

16.2 As such during the first 12 months there should be quarterly review points and a mechanism for feeding through any major issues and have flexibility for delivery timeframe to allow those to be addressed and prevent customer detriment.

16.3 In terms of change management, substantial changes will require consultation. Minor changes can be implemented on a regular basis, subject to a reasonable notice period, and appropriate governance arrangements to manage the process

Q17: Is a simple 50:50 apportionment for shared blame between firms appropriate? If not what is a sensible alternative?

17.1 Where there is shared blame between the customer's Firm and the receiving Firm, our view is that at least initially, an equal apportionment of cost could reduce the numbers of disputes between Firms. However, this becomes complex depending on the nature of the respective blames and the materiality of the impact it had on the particular case. Thought also needs to be given to where blame is shared with a PSP who has not

committed to the Code and where the remaining funding for the reimbursement comes from.

17.2 It will be important to ensure that the Code applies to all PSPs and electronic money institutions to ensure a consistent approach is achieved in apportioning costs.

Q18: Would the ADR principles as adopted by Open Banking in Section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the Code?

18.1 HSBC UK supports considering the use of an Alternative Dispute Resolution Service as an appropriate solution. This is, however, likely to be labour intensive and require a disproportionate investment of resources for the industry and its benefits should be kept under review.

Q19: What issues or risks do we need to consider when designing a dispute mechanism?

19.1 A prime issue is that since the Code is voluntary and might not be adopted by all PSPs or other payment institutions, there will be complex situations arising from, say the sending firm claiming not to be using the Code, whereas the receiving firm is (or vice-versa).

19.2 The short timelines also make it is difficult to establish a clear and transparent rule book.

Q20: What positive and/or negative impact do you foresee for victims of APP scams as a result of the implementation of the Code? How might the negative impacts be addressed?

20.1 If the Code works well there will be a clear and transparent set of standards that a customer needs to meet to ensure that reimbursement is obtained. There should be a clear process for the customer to obtain reimbursement from the sending firm.

20.2 There is an escalation path for the consumer if they consider that their claim is unfairly not being met, by approaching the FOS (see the FCA Consultation on extending the jurisdiction of the FOS to include APP scams).

20.3 A negative impact could happen if the Code is implemented before all issues have been resolved or if all PSPs are not included in the Code. This could lead to confusion and a poor customer outcome. It remains unclear what standards the FOS will apply in assessing whether the customer should be reimbursed.

Q21: What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the Code? How might the negative impacts be addressed?

21.1 The overly rapid implementation of the Code has the potential to create a high administrative and operational burden for Firms and other parties. We suggest that early adopters share learnings with others to smooth implementation. UK Finance could potentially facilitate such support for impacted Firms.

21.2 To avoid a confused customer journey, consistent internal processes for assessing claims would support consistent industry outcomes and better customer experience

Q22: Are there any unintended consequences of the Code, particularly those which may impact on customers, which we should be aware of?

22.1 HSBC UK is concerned that there is a risk of an increase in APP scams and first party fraud and that there may be attempts to gain access to the Code for non-APP Scam issues. This will require careful monitoring once the Code is introduced.

22.2 We are also in agreement that the remedies suggested in the Code should minimise disruption to legitimate payment journeys. The Code correctly allows Firms to screen or hold suspect payments on a risk-based approach to seek to protect customers targeted by APP scams. Nevertheless, there will always be a risk in this scenario that some genuine customers will be impacted or disrupted.

22.3 If APP scams continue to increase there would be a growing risk of friction being introduced in the payment system as Firms would need to screen, delay or query payments. The PSR consultation on APP scams noted that Japan and South Korea have had a level of success in anti-APP scam measures but this does involve delaying payments if they are above certain levels, or putting maximum limits on payments.

22.4 If genuine payments are held up or even not made there is a risk of legal issues (for instance if a house purchase falls through). The Firm should be protected if it can justify the rationale for its action.

Q23: How should the effectiveness of the Code be measured?

23.1 In our view there are two main areas by which the Code needs to be measured. The first is that the Code needs to be transparent and consistently applied, with the actions required by both customer and Firms to be understood and measurable. This will reduce the numbers of disputes and cases raised to the Financial Ombudsman.

23.2 There needs to be agreed Management Information to track Key Performance indicators. For instance, the numbers of disputes will be a key piece of Management Information post implementation.

23.3 The success of the Contingent Reimbursement Model Code will be whether the volume and value of APP scams reduce. This is of critical importance given the distressing nature of an APP scam to customers, even if they are reimbursed because they have met their level of care.

23.4 Finally, in the absence of a regulatory framework, we would support a self-attestation process for Code subscribers, reporting to the Governance body, in the same way as is the model for the Code of Conduct for Indirect Access to Payment Systems, whereby Code subscribers complete a self-assessment each year against standardised criteria from the administrators of the Code.

13th November 2018

By email:
app-scam-pso-project@psr.org.uk

Lloyds Banking Group
7th Floor
125 London Wall
London
EC2Y 5AS

Dear Sir/Madam,

Lloyds Banking Group (LBG) is pleased to be given the opportunity to respond to the consultation launched by the APP Scams Steering Group.

We take our commitment to fraud prevention seriously and have long shared the concerns expressed by the Payment Systems Regulator, consumer groups and others on the level of harm caused to consumers by authorised "push payment" (APP) fraud. For many years we have invested considerable resources in reducing the incidence of this fraud focused on customer education, preventative and detective controls and processes to repatriate funds to the victim.

We are confident that our investment in this control framework has resulted in the vast majority of APP fraud targeted at LBG's customers being unsuccessful. However, we recognise that the impact of fraud can be significant for our customers and we are committed to continuing to work collaboratively with other industry participants to reduce the harm caused by this fraud type even further.

We are generally very supportive of the contingent reimbursement model which has been proposed and believe that it broadly reflects the procedures we have operated for several years when considering compensation for affected customers. We believe that there could be considerable benefits from implementing such a scheme across all Payment Service Providers (PSPs) including:

- Helping to retain consumer confidence in the UK payments system;
- Raising the standards of fraud prevention across everyone involved in payments, including PSPs and consumers;
- Providing greater certainty to consumers on reimbursement at a time when they are having to deal with the emotional and financial impacts of being the victim of crime;
- Reducing the reputational impact of payment providers not compensating certain victims of APP fraud based on the fact that we could show that we have adhered to an industry-wide reimbursement scheme.

There are, however, a number of additional considerations which will need to be taken into account when finalising the Code. We have included further details of these in our responses to your consultation questions which follow.

In respect of the Standards for Firms (section “SF”) this already closely aligns with the procedures we already operate to prevent APP fraud from occurring. With the exception of clause SF1(3) and SF2(2) (which both relate to confirmation of payee which has not yet been launched) our procedures closely align with these standards. We have commenced an internal project to review the effectiveness of these procedures and to identify any areas where we believe they can be enhanced.

We also already have an existing process for considering customer claims of APP fraud and whether there are grounds to make an ex-gratia refund of the monies lost. We have commenced a project to update the procedures operated by the teams which consider these claims. We expect to be able to comply in full with the provisions of the Code after it is finalised and we will await further regulatory guidance on their expectations around implementation. This is provided, of course, that the content of the final Code do not differ markedly from those contained in the draft which was published in September.

We would be pleased to discuss any part of our response with you in more detail.

Yours faithfully,

Fraud and Financial Crime, Retail and Community Banking
Lloyds Banking Group

CRM Consultation – Lloyds Banking Group Response

Q1 Do you agree with the standards set out in the Standards for Firms?

Lloyds Banking Group is supportive of the contingent reimbursement model (CRM) proposed by the independent steering committee and we believe that there will be considerable benefits from it being widely adopted across the payments industry.

The Standards for Firms and, for that matter, the General Expectations for Firms, align closely with the procedures we have operated for several years to reduce the incidence of push payment fraud. We agree that they reflect a comprehensive list of the steps that PSPs can take to reduce the harm that this type of fraud causes.

That said, it is worth noting that the introduction of PISPs into the payment landscape following the introduction of Open Banking creates a potential complexity as payments from one account can potentially be instigated through the PISP of a completely separate organisation.

We believe the Code should be clear that the payment provider initiating the set-up of the beneficiary for a payment should be expected to undertake Confirmation of Payee and be responsible for providing effective warnings.

Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims.

We believe it is essential that the assessment outlined under point R2(1) takes into account whether any divergence from the standards on firms would have had a material effect on preventing the APP fraud that took place.

We believe it would be unhelpful for the standards in the code to be considered a “checklist” for firms to follow and it is likely to become such a document if reimbursement is assessed in a binary manner. If reimbursement becomes mandatory regardless of whether standards would have been relevant then PSPs will most likely respond in a simplistic, compliance-oriented manner. This will most likely result in them missing the opportunity to apply judgement as to the steps which are most likely to prevent the scam in question.

That said, where firms rely on this section of the standards then we believe it is incumbent on them to evidence why this is appropriate otherwise we acknowledge that this could be abused by some PSPs as a means of not making otherwise valid reimbursements.

Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

Unfortunately, Lloyds Banking Group has extensive experience of our customers falling victim to APP scams and we are well aware of the techniques employed by fraudsters and how they adapt over time. It is our firmly held view that preventing APP fraud is a shared responsibility: between PSPs, consumers and others such as telecommunications companies. We believe that this fact needs to sit at the heart of the design of any reimbursement code and it supports our view that joint-blame cases should have no reimbursement made.

Indeed, we believe that the consumer is at times best placed to stop the scam being successful. The fraudsters who perpetrate APP scams are adept at using confidence tricks on their victims and once these are underway, it can be hard to convince the victim that they are being scammed. This is why we often see otherwise effective warnings from PSPs being unsuccessful in preventing the scam. It is clear from years of us closely reviewing cases of successful and unsuccessful APP fraud that the best time to prevent it occurring is at the very start (i.e. before any PSPs have become involved) and that consumers play a key role in doing this.

A case where none of the parties has met their level of care could amount to a situation where the sending PSP has provided an effective warning but failed in some other aspect of the standards of care. In this case, if the consumer ignored the effective warning then we believe it is appropriate that they are not entitled to a refund, regardless of any later failings on the part of either PSP.

Q4 Do you agree with the steps customers should take to protect themselves?

We are broadly supportive of the steps that customers should take to protect themselves which are incorporated into section R2. As stated in our response to question 3, we believe that it is the consumer themselves who is often best placed to stop the scam being successful.

That said, we are concerned about the impact of the code on preventing "malicious payee" scam types such as purchase scams or investment fraud. These typically involve the victim paying their intended beneficiary the intended amount, without any redirection on the part of the fraudster. These frauds can be extremely complex for PSPs to prevent because warnings are likely to go unheeded and payments will be correctly authorised by the customer and be sent for their intended purpose. Providing an "effective" warning for such payments will be challenging for PSPs and attempts to spot them using transactional data and customer analytics will most likely impact high volumes of genuine payments.

If this section of the Code remains unchanged then it will result in a reduction in the level of care on the part of consumers and an increase in the number of successful scams. PSPs will also start to interrupt large numbers of genuine transactions to spot those which are related to fraud.

To enhance the effectiveness of the Code in achieving its stated aims, we believe that an additional clause needs to be added into R2(1) to cover steps that consumers should take to avoid falling victim to such scam types, along the lines of:

- *Failing to take reasonable steps to satisfy themselves that the payment was for a legitimate purpose.*

Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

We broadly agree with the points made in the consultation document regarding the approach for customers vulnerable to APP scams. In particular:

- We agree with using the term "customers vulnerable to APP scams" rather than simply "vulnerable customers" since using the latter could inappropriately extend additional protections to situations where this is not entirely appropriate.
- We agree that such customers should receive additional help to protect themselves and that there should be a general obligation on PSPs to offer this additional protection whenever relevant vulnerabilities are identified.
- We agree that there should not be an automatic requirement to reimburse all customers who may be classified as vulnerable but that this should be considered on a case by case basis.

However, we disagree with section R2(3) that such customers should be reimbursed nothwithstanding the provisions of R2(1). We believe that there could be a number of unintended consequences from adopting this approach.

Firstly we believe that it could simply encourage some victims of APP fraud to erroneously claim that they were vulnerable at the time of the scam. Given the sensitive nature of this topic, it may be complex or inappropriate for a PSP to refute this point providing them with an obligation to provide a refund. For example, if a customer was recently bereaved and believed that this made them increasingly vulnerable to APP scams then it is not clear to what extent this should be evidenced. Requesting, for example, a copy of a death certificate, may appear inappropriate and totally insensitive. On the other hand, given the additional protections which declaring a relevant vulnerability afford, it is reasonable that a PSP may request some form of corroboration before relying on it.

Secondly, it could increase the prevalence of APP fraud if a cohort of consumers believes that they are afforded an automatic right to reimbursement. This would be entirely contrary to the main objectives of the code. This could arise either from consumers misunderstanding the code and believing that it provides an automatic right of reimbursement for certain groups (for example those above a certain age) or by lowering the general standard of care from those who assume they will meet the definition of vulnerability.

Indeed, this could even extend further to fraudsters deliberately targeting such customers (knowing that they are even more likely to fall for the scam) and increasing the rate of fraud in vulnerable customer groups.

Thirdly, it could result in some PSPs choosing to "de-risk" their business by not offering services to customers who may meet the definition of vulnerability.

We believe that these unintended consequences can be avoided and that it would be more appropriate to consider vulnerability in the context of whether one or more PSPs took reasonable steps to respond. This would amount to additional standards on firms to:

- Take reasonable steps to identify customers who may be vulnerable to APP scams;
- Take reasonable steps to respond to such situations being identified.

Fourth, depending on the nature of the customer vulnerability, there are cases where it will be necessary for the victim to ensure that their own PSP is aware. For example, if a customer has a long-term cognitive impairment this may not be immediately (and initially) apparent to a PSP though it will be important that they are aware so as to respond appropriately. On a case by case basis, we believe there should be an obligation for consumers to inform their PSP of relevant vulnerabilities in advance and (again, on a case by case basis) the PSP should not necessarily be held liable for reimbursement if they have failed to respond to a vulnerability which is not apparent

Finally, we would note that the wording of the code itself differs from the approach set out in the consultation document. Under R2(3) the code states:

- *A Customer is vulnerable to APP fraud if…. This should be assessed on a case by case basis. In these circumstances, the Customer should be reimbursed notwithstanding the provisions in R2(1).*

To align with the position outlined in the consultation document we would suggest that this is reworded to say:

- *A Customer is vulnerable to APP fraud if…. In these circumstances, decisions on whether to reimburse the Customer should be made on a case by case basis.*

We have seen case studies in the past where employees of Lloyds Banking Group have gone to considerable lengths to protect vulnerable customers from fraud including providing multiple warnings. For example, in one case study a 78 year old customer sent nearly £70k as part of a safe account scam in two visits to one of our branches. They were served by different colleagues each time, and on each occasion they were given explicit warnings about the prevalence of such scams (a point the customer does not refute). Despite this, they gave their explicit consent for the payments to be made. In the circumstances of this case the customer would most likely be considered vulnerable to scams and under the terms of the draft Code would be entitled to a reimbursement – even in spite of the explicit warnings given. We do not believe that this outcome is aligned with the objectives of the Code that were set out by the Payment Systems Regulator at the outset.

Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?

We agree with the proposal for most reimbursement decisions to be communicated within 15 days. We also agree that the code should provide the flexibility in exceptional circumstances and we agree that 35 days is appropriate for this purpose.

Q7 Please provide feedback on the measures and tools in the Annex to the code, and whether there any other measures or tools that should be included?

We believe that the contents of the annex are broadly comprehensive. However, we would note that this section of the document is likely to be dynamic in nature and hard to keep up to date. It may be more efficient to remove it from the code itself maintain it elsewhere, for example on a public website.

In addition, we would also argue that the contents of the section headed “network-level transaction and data analytics” have been summarised to such an extent to be largely worthless. Using software to detect APP fraud from analysing patterns of transactions is notoriously hard and considerably more challenging than doing the same for unauthorised fraud types. Whilst we agree that it should be a standard on all firms to use these techniques, it needs to be understood that this is a backstop control which will prevent little fraud on its own.

Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

One of the core principles of the code that was outlined by the PSR at the start of 2018 was consistency of outcome. We agreed with this principle in the original consultation and remain of this view. Therefore, we are supportive that all customers who meet the requisite level of care should be reimbursed as to do anything different would conflict with this core principle.

That said, and for the same reason, we believe it does not necessarily follow that a PSP should directly bear the cost or reimbursement in such “no blame” cases. Whilst they may administer the immediate refund to the victim, we believe that a solution needs to be found to create a sustainable funding source for “no blame” cases. We are supportive of the ongoing work to establish this funding and, indeed, a director of Lloyds Banking Group will be acting in the role as co-chair for this working group.

Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

We believe that the most straightforward means of implementing the code is for the sending firms to administer any reimbursement. This is consistent with the industry Best Practice Standards which place an obligation on the sending firm to take overall responsibility for handling any fraud claim.

That said, there are some risks associated with this approach in that sending PSP bias may mean that they do not consider themselves at fault when this is the case. There are clearly mechanisms to manage this risk including regulatory supervision, any oversight performed by the body responsible for code governance and individual rulings from the FOS. However, these may not immediately identify where this is the case leaving some victims disadvantaged for a period of time.

We believe that the steering committee should consider whether a separate body should be responsible for reviewing all APP fraud claims and for administering reimbursements to customers. This could be the same body which is responsible for governance of the code. A draw-back of this approach would be the high cost and complexity of establishing such an operation.

Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?

We believe that the list of funding options for “no blame” cases outlined in section 4.6 of the consultation document is comprehensive.

We believe that any funding approach for such cases needs to be sustainable over time and also not lead to large surpluses whilst also spreading the costs amongst all parties who have a role to play in preventing APP fraud. Finally, it needs to be reasonably straightforward to deliver and implement.

To achieve these goals, it is most likely that a combination of one or more options working in conjunction could provide a workable solution.

Considering each of the options in turn:

- We believe that a customer levy on payments is the most appropriate potential source of funding. Given the volume of faster payments (and the fact that APP scams are relatively rare in the context of these high volumes) we believe that a relatively trivial sum could be added to some or all payments to create a sustainable funding source. Indeed, simply levying the charge could raise awareness of scams amongst consumers in a similar way to how the "plastic bag tax" raises general awareness of the impact of waste upon the environment. Since most consumers would pay this (hopefully) trivial charge relatively frequently it would provide a continual reminder of the importance of taking steps to prevent scams.
- Contribution mechanism from all parties with an ability to prevent APP scams: this option has considerable merit. However, the design of such a scheme would need to genuinely extend to all those who can prevent APP fraud (including telecommunications companies, money transmittance services etc) for it to be effective.
- We do not believe there is merit in progressing with the concept of insurance products or different account types. Such developments would most likely only create conduct risks around their sale to consumers and would also not be consistent with the spirit of the code around extending protections to all. Consumers opting in to such an insurance product may lower their standard of care and increase the number of APP scams which are successful. Finally, there may be competition issues around such developments if product features were effectively enforced by virtue of a voluntary code.
- We support "fines" being levied in shared blame scenarios and believe this is consistent with the spirit of the code.
- We support in principle the concept of unlocking funds in dormant accounts though we would not that using these funds in this way would require legislative change. Also, whilst it would be a useful initial source of funding it would not last very long.
- Finally, we are supportive of a government run scheme being investigated further.

Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

We broadly agree with the points made in the consultation document about the importance of evidence in establishing whether the code has been met.

Some aspects of the Code will lend themselves to producing an audit trail of the events of the time. For example:

- For any payments made by telephone, most PSPs will most likely be able to produce call recordings which will provide a record of whether effective warnings were given.
- Equally, for any payments made by online banking, PSPs should be able to produce a record of what warnings were provided on screen and the consumer's response to them.
- Whilst not yet implemented, it is most likely that records from Confirmation of Payee will be available to be reproduced in an evidential format.
- The outcome of any transactional data and customer behaviour analytics should be possible to be produced as clear evidence including the steps taken by the PSP to temporarily block payments and to check with the customer whether they have taken steps to avoid falling victim to APP fraud.
- For receiving firms, there are existing obligations under the Money Laundering Regulations to retain records from account opening around the identity checks performed on applicants.
- Regarding the obligations on PSPs following notifications of successful APP frauds, it should be reasonable to produce records from the time on what steps were taken.

However, there are other aspects of the standards contained within the code which may not lend themselves easily to audit trails being kept. These include:

- The events that may cause a consumer to share their personal security credentials and whether any payments which followed should be considered as authorised or unauthorised payments.
- The steps consumers take to satisfy themselves that a payee was the person they were expecting to pay.
- Where the victim is a microenterprise or charity, whether the organisation has any internal procedures for approval of payments and whether the versions available were indeed the ones in place at the time of the scam.
- PSP warnings given in a face-to-face environment, such as a bank branch, may not be easily recorded in the same way as those given over the phone or by on-screen warnings.

However, for each of these we believe that it is reasonable for consumers to be able to produce some records of the steps that were taken from the time and this will be important for the established working group to consider. For some types of scam, it will be evident that certain steps were not taken based on negative evidence. For example, in a case of investment fraud, a victim may state that they checked the legitimacy of the firm they believed they were investing with on the FCA website. In a situation such as this it may be the case that firms can show that the firm in question was not contained on the FCA register.

Over time, we believe that the Financial Ombudsman Service will have a key role to play here since they will establish precedents around the nature and extent of evidence required and the extent to which any one party can rely on the word of the other when considering an APP fraud claim.

Q12 Do you agree with the issues the evidential approach working group will consider?

We agree with the issues the evidential approach working group will consider.

Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

We don't believe there are any other issues which require consideration.

Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

We have provided more general comments around the approach to vulnerability in our response to question 5.

In respect of evidential standards, we believe that this issue introduces considerable complexity.

- Firstly, a PSP may require the consent of a customer to retain records regarding certain vulnerabilities. This can impact on a PSPs ability to respond and also to being able to assess vulnerability as part of any APP fraud claim.
- Secondly, there may be times where a requirement to produce evidence to support an APP fraud claim may conflict with a PSP avoiding being overly intrusive. For example, if a customer was recently bereaved and believed that this made them increasingly vulnerable to APP scams then it is not clear to what extent this should be evidenced. Requesting, for example, a copy of a death certificate, may appear inappropriate and totally insensitive. On the other hand, given the additional protections which declaring a relevant vulnerability afford, it is reasonable that a PSP may request some form of corroboration before relying on it.
- Finally, when considering vulnerabilities it is most likely that judgement will be necessary and the degree to which the customer is vulnerable will be important. For example, a customer suffering from dementia may initially experience mild lapses in memory which could then worsen over time. The nature and extent of their symptoms will be important when considering their vulnerability which may therefore require some PSPs to ask for copies of medical records. This could be complicated

further if a fraud claim is lodged several months or years after the fraud occurred, or even after the death of the victim, meaning an assessment needs to be made around the extent to which the victim was vulnerable at the time.

To address this, we support the adoption of industry-wide standards which could apply to all PSPs so that evidential standards in this sensitive area are based on industry norms rather than decisions made by individual PSPs.

Q15 Please provide views on which body would be appropriate to govern the code.

We believe that the Code is relatively unique in UK financial services and that there is no obvious answer to the question of who should govern it.

Certainly, we agree that UK Finance would not be an appropriate owner on the grounds of their conflict of interest. We agree that there is merit in considering further the option of the code being governed by the New Payment Systems Operator.

We believe it is most important that whoever does govern the Code is provided with sufficient resources to do so and is appropriately independent from any stakeholders who have an interest in the code.

We do not support the suggestion referenced in the consultation document that the existing steering committee should remain in place in order to support the ongoing governance of the code – on the basis that it was created for a specific purpose which will, shortly, be complete. That said, we do welcome the proposal to establish an advisory body to support the governance of the code and it may well be the case that there is considerable overlap in the membership of these two bodies.

Q16 Do you have any feedback on how changes to the code should be made?

We broadly agree with the proposals suggested in the consultation document:

- That changes to the code should be allowed on an *ad hoc* basis;
- That periodic reviews should take place;
- That the first of these should take place around a year after the code is finalised;
- That, thereafter, the reviews should take place approximately every three years.

We believe that it should be written into the governing principles of the code that whoever undertakes this role (see our response to question 15) should have the autonomy to decide:

- The frequency of any reviews and updates;
- Whether any updates need to be issued for full public consultation or for consultation amongst the advisory body.

As a voluntary code, we believe it is also necessary for any changes to the code to be consulted on amongst all existing signatories to the code and that adoption of the code from any signatory can lapse upon each update.

Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

We believe that there is merit in the 50:50 apportionment which is proposed.

Each individual “shared blame” case will, inevitably, have different degrees of blame. However, trying to quantify these will be largely impossible. Furthermore, it may be the case that it was a small error by one PSP which ultimately caused the fraud to be successful, whilst larger errors by the other PSP in the same case may have had less impact. We believe that any alternative to a simple, fixed apportionment is likely to just create complexity whilst not contributing anything to the prevention of APP fraud.

That said, in our opinion the sending PSP is generally better placed to prevent an APP scam than the receiving PSP. Therefore, an alternative suggestion could be to set the apportionment at 75:25 (respectively) to align with this.

Q18 Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the code?

In our response to question nine we stated that we were generally supportive of the proposal for the sending firms to administer any reimbursement. This is consistent with the industry Best Practice Standards which place an obligation on the sending firm to take overall responsibility for handling any fraud claim.

In undertaking this role, the sending firm will be required to:

- Undertake an assessment of their own compliance with the standards set out in the code, producing evidence as appropriate.
- Make contact with the receiving bank and request that they do the same. We would expect the receiving bank, in responding to this request from the sending bank, to make a clear affirmation of whether they believe they have met the required standards set out in the code and to produce, on demand, evidence to justify this position.
- Make a decision, in line with the code as to whether the victim is entitled to reimbursement and, where appropriate, administer this reimbursement.

As such, the sending bank should not be required to make an assessment of the receiving bank's compliance with the code, and request reasonable evidence to justify any conclusions reached by the receiving bank. We do not believe that this process of PSPs sharing evidence would conflict with any legal obligations such as those contained in the Data Protection Act on the basis that we are referring to de-personalised evidence being shared.

Where this leads to a dispute between firms then we believe that section 7 of the Open Banking Dispute Management code of practice would be an appropriate method of resolution. An alternative model could be the schemes operated by Visa or Mastercard for considering chargeback claims between issuers and merchants. In our experience these are well established, rigorous and low cost – factors which are achieved through a strict rules-based system which all parties must adhere to for a claim to be considered.

That said, also in our response to question 9 we suggested whether an independent body could be established to assess all APP fraud claims (which could be the same body responsible for governing the code). If such a body were established then there may be less need for a separate dispute mechanism.

Q19 What issues or risks do we need to consider when designing a dispute mechanism?

In offering a dispute mechanism, there is a risk that one or more PSPs abuse the system by referring cases which could reasonably have been resolved without one. We believe that this needs to be factored into the design of the scheme, most likely by placing the costs of arbitration onto the firm which is ultimately found to be at fault. We believe that this will ultimately result in as few cases as possible being referred in the first place.

We believe that risks to consumers from operating such a scheme can be eliminated by virtue of the separate obligation in the code for the sending bank to administer the reimbursement, regardless of fault.

For larger PSPs, this obligation will most likely have only a low impact provided that arbitration ultimately results in the PSP at fault bearing the reimbursement cost. However, for smaller PSPs this may not be the case and that for high value APP fraud cases the cost of initial reimbursement could impact their solvency. Therefore it will be important for decisions to be reached in a timely manner.

Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

We believe that there are a number of positive impacts for consumers as a result of the code being introduced. Provided the code is well designed, these will include:

- A reduction in the incidence of scams as a result of standards being raised across the whole industry (including amongst consumers);
- Greater awareness of the steps that can be taken for a consumer to not fall victim to an APP scam in the first place;
- For victims of APP scams, greater certainty around whether a reimbursement will be given.
- Increased confidence in the UK payments system;
- For customers who are vulnerable to APP scams, greater protection being offered by PSPs to prevent scams happening in the first place.

That said, there are a number of potential negative impacts.

- Consumers may misunderstand the design and wording of the code and assume that they are afforded some sort of "guaranteed" reimbursement. This may result in a reduction in the level of care amongst consumers and an increase in the incidence of fraud. We believe this can be addressed through clear and consistent messaging from all parties involved with the code around its design and operation.
- As mentioned previously, depending on how the provisions for customers vulnerable to APP fraud are designed, there may be a reduction in the level of care amongst this cohort of consumers leading to an increase in the incidence of fraud or, indeed, fraudsters targeting such customers even more. We have commented on how this can be addressed in our response to question five.
- Depending on how firms respond, there is an increased risk of genuine payments being interrupted as a result of steps being taken to comply with this code. This could include:
    - Increasing number of payments being temporarily blocked whilst PSPs undertake checks with the customer and provide effective warnings;
    - An increase in the time to make payments due to the need to provide effective warnings;
    - Payments being delayed whilst PSPs undertake checks;
    - Inbound payments not being immediately applied to customer accounts whilst PSPs undertake checks relating to authenticity;
    - Difficulties obtaining access to banking facilities, particularly for those who do not have a large credit footprint or standard identity documents (e.g. UK passports or UK driving licences);
    - PSPs potentially choosing to "de-risk" for example, by choosing not to provide services to those who may be vulnerable to APP scams.

We believe that some or all of these are inevitable consequences of the code being introduced, though each firm's approach to aligning with the code will create opportunities to differentiate their services from other PSPs. For example, PSPs which invest in more sophisticated fraud detection tools will be able to offer customers faster and more efficient payment services whilst not increasing the risk of APP fraud.

Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

We believe that there are a number of positive impacts for firms as a result of the code being introduced. Provided the code is well designed, these will include:

- A reduction in the incidence of scams as a result of standards being raised across the whole industry (including amongst consumers);
- Increased confidence in the UK payments system;
- A reduction in the reputational risk relating to cases of scams on the basis that firms should be able to point to an agreed voluntary code to explain their actions at the time the scam took place and when justifying why a reimbursement was or wasn't given.

We are concerned about section R4 of the code and the rights it affords victims to refer negative reimbursement decisions immediately to the Financial Ombudsman Service. We believe that this is a particularly unhelpful section of the code which extends a narrative that all APP fraud is the fault of PSPs and that they are singularly able to prevent it. We believe that preventing APP fraud is a shared responsibility: between PSPs, consumers and other bodies such as telecoms companies.

The existing process for authorised and unauthorised fraud claims within Lloyds Banking Group is for:

- A decision on the fraud claim to be made by a specialist fraud team;
- If the customer is unhappy with this decision, they can refer the case to a separate complaint handling department within the bank;
- If they remain unhappy with the response from this department they can refer the case to the FOS.

There is no evidence that this process does not work and, indeed, we have historically seen that fewer than one in fifty victims of APP fraud referring their case to the FOS. Furthermore, it does not necessarily follow that every APP fraud claim is an expression of dissatisfaction regarding the conduct of their PSP from the victim.

We strongly believe that section R4 should be amended to be consistent with this existing approach. Victims would have the right to take their case to the FOS, though only after first referring it to their bank's own internal complaints process. There is additionally a risk that the FOS will simply be deluged with cases that could easily have been handled within PSPs.

We do not believe that the above approach would result in material detriment for consumers. We support the requirement for claims to be considered within 15 days, as standard, and any resulting complaints would be required to be considered also within 15 days as per the Payment Systems Regulations. Therefore, consumers would have to wait, at most, 30 days from raising an APP fraud claim to be able to take their case to the FOS (if they so wished). We do not believe that this is unreasonable, particularly given that the timeframe for the FOS to review such cases will most likely extend to several weeks (or perhaps longer).

Indeed, under the current wording of the code, the FOS will most likely be deluged with cases that could have been handled by PSPs own internal complaint handling departments. This will simply elongate the timeframes of handling all such cases and lead to a worse outcome for consumers overall.

Under R3(1)a, we would suggest that where firms extend the claim handling period from 15 days (up to 35 days) then immediate information is provided on how to refer the case to the PSPs complaint handling teams, with FOS rights commencing no later than 15 days hence.

We do not agree with point 3.82 of the consultation document which suggests that the "early consent" rule under DISP could be used to effect this aspect of the code and we would suggest that this rule was designed for an entirely separate purpose.

Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?

We have nothing further to add in response to this question above and beyond the points made already.

Q23 How should the effectiveness of the code be measured?

We believe that the most important outcome in respect of APP fraud is to stop it happening in the first place. Even in the situation where a victim is reimbursed, a fraudster will have benefited. Therefore we believe that the success of the code should be primarily measured in terms of the reduction in levels of APP fraud.

In addition, the level of support provided to consumers in the aftermath of APP frauds should be measured. The key measure implied by the code is around the timeliness of reimbursement including:

- The number of claims assessed within 15 days;
- The number of claim decisions overturned by PSP complaint handling teams;
- The number of claim decisions overturned by the FOS.

Draft Contingent Reimbursement Model Code: Nationwide Consultation Response

Overall Comments

Thank you for the opportunity to comment on this consultation.

Nationwide is committed to ensuring all our members have the support and education they need to manage their money effectively and to understand and avoid scams. As a mutual we are owned by and run on behalf of our members. We are particularly concerned about vulnerable customers and have set up a specialist support service to help members who face financial difficulty for issues like long term illness.

Nationwide is also seeking to play a role in financial education. Our Open Banking 4 Good initiative was recently launched as part of the Cabinet Office's Inclusive Economy Partnership. This piece of work is funding fintech partners to harness the power of Open Banking to deliver tools that will help everyone manage their money more effectively. Additionally, we continue to invest in our branch network.

So, key to Nationwide's strategy is to look after our members and their money. Preventing authorised push payment (APP) scams is important to us - and we would like to continue to engage with the PSR and industry to address this customer risk.

In our January 2018 Contingent Reimbursement Model (CRM) consultation response, Nationwide supported the development of "*a fair, clear, limited and agreed Contingent Reimbursement Model*" to incentivise both PSPs and customers to take appropriate care to prevent APP scams at different stages of the payment journey. We welcome that this incentivisation is reflected in the CRM core principles and continue to think our vision of the CRM is important which leads us to a number of focal comments on the draft Code. We believe:

- The Standards for Firms need additional scoping and detail - particularly to further incentivise receiving PSPs to detect and restrain mule accounts and APP scam proceeds.
- The Standards for Customers require greater specificity and a higher requisite level of care – to ensure that customers are clear on the steps that they are expected to undertake, to minimise the scope for disputed reimbursement outcomes and to ultimately drive scam prevention.
- That a defined Code, shaped by our proposed enhancements, should minimise or eradicate the number of 'no blame scenarios' and this would be the basis on which we would agree, in principle, with customer reimbursement in a 'no blame' scenario.
- For residual 'no blame' cases a sustainable funding model would need to be developed which provides the correct incentive for all parties with the power to prevent APP scams to take requisite care (including for example, online market places). We retain our original position[1], that a central fund financed solely / directly by PSPs would not provide such an incentive. Further, this funding model must be accompanied by standards which are defined and of a requisite level, so that firms and customers remain incentivised to take sufficient care. It must be remembered that APP scams are a crime, the proceeds of which could fund other illegal activities. We perceive there is a risk of a central fund inadvertently serving to perpetuate this crime. Therefore, it should cover a narrow range of no blame situations in which requisite care has been taken rather than in any way incentivising a minimum level of care by parties.
- There is a need for greater consideration and clarification of the definition and requirements regarding vulnerable consumers to ensure fair and balanced outcomes.
- That in a 'customer blame' scenario (where the customer has not complied with their obligations), the customer should not be reimbursed (to reflect a proper incentivisation to the customer) and in a scenario where both PSPs are to blame and the customer is not (i.e. 'shared PSP blame') a 50:50 allocation model should be adopted up to a certain transaction value – over which a separate dispute resolution process could be incepted to determine each PSP's contribution more precisely.
- Identification of the correct evidentiary standards, through the work of the Evidential Approach Working Group, will be vital for customers and PSPs.

[1] Expressed in our January 2018 consultation response

- A clear rule set needs to be established covering situations such as when all parties are at fault and when one PSP has adopted the Code but the other PSP to the transaction has not. It's particularly important to identify and address the implications for firms and customers meeting the requirements of the Code when another PSP does not sign up to, or only partially implements, the Code.

Additionally, as identified in the consultation paper, the Alternative Disputes Resolution process will be a key area of development – we welcome the Steering Group work on this.

We believe industry focus in all of the above areas is critical to translate core principles into an effective, sustainable and enduring collective response that drives positive outcomes and reduced instances of scam.

More generally, there is a need for clear delineation of the Code with other industry standards, such as those of Confirmation of Payee (CoP). The CRM is likely to encompass other APP scam prevention mechanisms over time (e.g. Transaction Data Analytics). A lack of alignment, prioritisation and clarity between the CRM and the rules of relevant solutions could result in incomplete consumer protection, delayed adoption, inconsistent implementation and operation. It could additionally complicate ongoing development and governance. For example, it is not clear to which party comments on the development of some elements of CoP should be addressed. For this reason, we believe that while the CRM as a voluntary code can specify adoption of a measure, the underlying rules, requirements and liability arising from the operation of that measure should be specified as part of the rules of the solution. Close working relations will be necessary between the future governance body of the Code and the bodies delivering solutions such as Transaction Data Analytics.

In terms of CoP, we would ask that the 'clear negative' within the Code be defined and believe this should encompass the 'no match' and 'close match' negative responses within the Pay.UK CoP solution.

There will be cost and resource implications for PSPs in complying with this Code – including underlying requirements for CoP. This is at a time of intense industry activity to deliver Open Banking and Secure Customer Authentication. For smaller firms and new entrants, adherence to the Code must not be uneconomic. The development of third party vendors to meet some requirements could help with this but this should be factored into implementation plans. We would ask for this to be considered in the timing of the implementation of the Code – adoption of a phased approach is recommended - and we continue to request the assessment of practical and economic effectiveness of any new measures prior to requiring adoption through the CRM.

Q1 Do you agree with the standards set out in the Standards for Firms?

We attach our detailed comments on the draft Code (including the Firm standards) in Annex 1.

We firmly believe that there is a need and scope for greater specificity in the Standards for Firms – particularly in terms of the standards for receiving firms given the important role they have in preventing the operation of mule accounts and detecting and restraining APP scam proceeds. The CRM must incentivise receiving firms to take requisite care – relying too heavily on, say, effective warnings on the sending side will not address all the issues.

For sending firms we would also advocate that effective warnings are standardised and to the extent possible agreed by the FOS etc. An analogy could be drawn with the standardised wording used elsewhere in the industry e.g. "*the value of your investments can fall, and you may not get back your original investment*". Adoption of standardised effective warnings will ensure clarity and consistency of consumer messaging and assist consumer education.

It would be helpful to have additional clarity, perhaps via examples, on the intent of SF2(2)(a) "*Firms should not use Confirmation of Payee as a means to reduce their risk of potential liability for funding the cost of a reimbursement to a Customer in a way that would be likely to prejudice or unduly disrupt legitimate payments.*"

As above we would encourage delineation and clarity between the requirements of the CRM and the CoP standards. Further, the text in SF(2)(a) appears to be a principle / guidance, rather than a scam prevention standard upon which liability should be determined, and so this should be included in the General Expectations for Firms, if it is to appear in this document.

There is a cross industry and longer-term perspective to consider here as well, which also focuses on the opportunities to do more on the receiving side in 2019 and beyond. Key examples include anti-money mule solutions. There are also developments in the infrastructure layer of the payments supply chain, using end to end payments data and network effects, that complement this ambition. We'd encourage the PSR to join us in supporting these initiatives and to help enable their implementation where there may be regulatory or legal issues to work through.

Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims.

We believe that causation must be an essential element of the assessment of reimbursement and that unless the Code incorporates a causal link between the breach of the PSP or customer standard and occurrence of the scam, it risks creating perverse outcomes and/or distorting the intended incentivisation of all parties in the transaction to take requisite care.

In most cases, we think it will be clear if compliance with the Code could have prevented a successful scam. An example might be in the case of CoP if the knowledge of a payee's identity would have stopped an APP scam. If the payee account name is that of the intended payee and the CoP match would have been 'correct' then a failure in the deployment of this solution would not be relevant to preventing this scam and reimbursement would not be appropriate.

Whilst we note the concern that this provision may lead to reimbursement claims being declined, if it is being applied by firms incorrectly or unfairly that decision would ultimately be susceptible to overturn by the Financial Ombudsman Service (FOS). Further, the FCA Handbook Dispute Resolution rules require firms to take account of adverse FOS decisions in their subsequent decision-making processes.

Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

Given a clear and defined model, we anticipate the situation in which it is not possible to allocate 'blame' would be unusual and assume that this question is being asked outside the context of vulnerable consumers.

However, in the scenario, where no party meets the required standard we do not believe customers should be reimbursed. The rationale for this outcome is consistent with that intended for the 'no blame' scenario in which a customer will receive reimbursement because they have met the requisite standard (irrespective of whether any other party was at fault or not). In particular, this approach would incentivise customers to take requisite care.

Section 4.6. of the consultation suggests that in a scenario where the PSP(s) and the customer are both to 'blame', the firm at fault could be asked to contribute to a central fund in the form of a fine. If this proposal is to be taken forward, we would stipulate the following parameters for any 'fining' model:

- Any fine should not be the full amount of the loss (reflecting that the other party was also part of the loss).
- The PSP's breach must have a causative effect on the scam.
- The central fund should not be funded solely by PSPs to ensure it incentivises other parties to drive down APP scams.
- Where both the sending and receiving PSPs are at fault - both should contribute to any fund.
- The accompanying standards on all parties are defined and of a requisite level, to incentivise all to do more than the minimum (please see our response to Questions 4 and 8).
- The sufficiency of the fund and any fall back is considered, and effective non-PSP funded solutions identified to prevent impact on wider services.

And of course, an effective administration and governance mechanism would need to be established.

Q4 Do you agree with the steps customers should take to protect themselves?

We believe that greater specificity in the Standards for Customers will introduce more certainty for all parties, remove scope for dispute and ultimately drive scam prevention. It will also be essential to the operation of a sustainable central funding model. Our agreement in principle to customer reimbursement in a 'no blame' situation is on the basis that the standards and obligations for all parties are more sharply defined, and so by design, instances of 'no blame' should be minimised.

We provide our detailed comments in Annex 1. In summary we would strongly advocate:

- Requiring customers to follow and act upon PSP warnings - rather than prohibiting customers from ignoring warnings.

- Requiring customers not to share access to their personal security credentials – rather than asking them not to 'recklessly' share their details. This requirement should be positioned so as not to discourage customers from using Open Banking.

- Micro-enterprises and charities should be required to have an internal payment process with safeguards against APP fraud risks – rather than the obligation to reimburse them being determined by whether they complied with their existing internal process. Otherwise, those without a process would be better placed under the CRM than those with, because they would not be held to account for failing to follow that process.

- The obligation to act openly and honestly should extend to the payment journey and not just the reimbursement claim, as currently described in the CRM. A customer's failure to act openly and honestly during the payment journey has implications on the PSP's ability to provide adequate warnings to prevent the scam.

- We believe the term "clear negative result" in R2(1)b should be defined. We believe this should include the 'no', and 'close match' CoP results contained within the Pay.UK CoP solution. This definition would be consistent with the Pay.UK position but clarity from the APP Steering Group and within the CRM on this would be valued however, as would the relative position of the CRM with other CoP verification outcomes

within the Pay.UK solution. We would reiterate our position above, on the need for clear alignment and delineation of the Code and the rules of underlying measures.

If customer standards are too low they may not be incentivised to take care if they believe that their exposure to APP scam losses is underwritten by the Code. This lack of caution could be exploited by fraudsters.

Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

We are sure the APP Steering Group would agree this is a complex topic and understand the requirement for further guidance and consideration.

The approach suggested in the consultation is for PSPs to reimburse a vulnerable customer if they could not reasonably (at the relevant time) be expected to protect themselves from the APP fraud. The dynamic nature and broad definition of vulnerability within the Code will make it practically impossible for PSPs to always identify vulnerability prior to a scam occurring – particularly in digital channels where the interaction may not involve seeing and/or speaking to customers. We believe this must be recognised in the application of SF1(4) and R2(3).

In essence, the Code seeks to incentivise PSPs to take every effort to protect 'vulnerable customers' but the breadth and application of that definition means that it will cover incidences in which the PSP could not therefore have reasonably known and could not have taken additional steps to prevent the scam over and above those which it would extend to all customers. The definition of vulnerable consumers therefore spans a spectrum from where the sending PSP could have taken steps to prevent to situations where there is no PSP 'blame' associated with the non-identification of the customer as vulnerable (i.e. the sending PSP has complied with SF1(4)).

In these scenarios there is an argument, that if a PSP meets requisite standards and could not have identified the customer as vulnerable, that no party is 'to blame' and therefore the logic and option - that payments to such vulnerable consumers should be met from the central fund proposed for the 'no blame' situation - could be explored. If funding for such cases were to come from a central fund, we believe it would also be sensible to develop industry-wide controls to ensure consistency (as far as possible) in how PSPs' classify customers as vulnerable.

To help in the operation of this model therefore, we would:

- Encourage re-assessment of the scope of the definition of vulnerability, particularly the dynamic elements which make the definition very broad and make it more difficult for PSPs to identify that vulnerability; and
- Ask the Evidential Approach Working Group to develop clear sensitive evidentiary standards, including tests, to enable the assessment of how the vulnerability affected a customer's ability to act on an effective warning or to use CoP etc. Or, in other words, demonstrate how the vulnerability played a part in the decision to transact. The Working Group could produce and use case studies and examples to test the practicality and robustness of the vulnerable customer definition and rules and inform the development of evidentiary standards.

We suggest the potential positive and negative unintended consequences of these requirements for vulnerable consumers need to be scoped and understood. A likely consequence will be that some consumers will falsely claim vulnerability to receive reimbursement where they have failed to adhere to the Customer standards. Another is there may be limitation of functionality (e.g. restrictions on an account) or offerings to vulnerable consumers by some PSPs - particularly in the case where a vulnerable consumer has already been victim of fraud. However, this latter restriction could protect the customer from further scams.

We think the PAS 17271 has value but would need to conduct an impact assessment in order to comment on the appropriateness of its adoption as part of the Contingency Reimbursement Model (as per paragraph 3.73 of the consultation). We would not support adoption or consideration of this by the FOS in its assessments however

until parties have had a full opportunity to properly assess this British Standards specification. This could also form part of the consideration of the Evidential Approach Working Group or a separate consultation.

Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?

We agree with this timeframe. However, in relation to R4 in the draft Code we feel there should be a requirement that aligns with established and proven redress procedures. This is the relevant extract:

Where a Customer has received a negative reimbursement decision, all the Firms involved will take all reasonable steps to enable a Customer who is eligible and wishes to do so, ***to commence immediately the process of challenging that decision*** *with the Financial Ombudsman Service.*

To challenge a rejection, the customer should complain to the PSP in the first instance rather than the FOS. A PSP should be able to review its decision before the customer refers their challenge to the FOS. We appreciate these complaints would then need to be considered by the firm at pace given the customer's likely circumstances, but our concern would be that without the firm's internal complaint process being initiated, there is a risk the FOS may become over-stretched, receive cases prematurely and / or that allowing immediate access to the FOS could unintentionally create further delay in the redress process.

We would encourage the Steering Group to liaise with Pay.UK to understand their CoP timeframes for PSPs responses to customers prior to onward escalation to ensure that these are aligned as far as possible.

Q7 Please provide feedback on the measures and tools in this Annex, and whether there any other measures or tools that should be included?

Greater information is needed to enable comment on some measures. Some of the solutions proposed to be included in the CRM are at conceptual levels and a long way from final solutions and currently the cost, operational impact and effectiveness of these are unknown. This includes the Economic Crime Information Sharing and Transaction Data Analytics solutions. We believe the industry would need to understand more about these and other solutions (including legal and regulatory compliance and final design of solutions) before being able to commit to incorporate them within the CRM.

Again, we would request that there is a clear delineation and prioritisation in the rules for these new measures and in the CRM to provide clarity of obligations for parties implementing and simplify ongoing governance.

For smaller firms and new entrants, adherence to the Code must not be uneconomic. The development of third party vendors to meet some requirements could help with this but this should be factored into implementation plans. We would ask for this and industry capacity to be considered both in the obligations placed on PSPs and the timing of the implementation of the Code – adoption of a phased approach is recommended. We continue to request the assessment of practical and economic effectiveness of any new measures prior to requiring adoption through the CRM.

Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

We believe that if the Code is developed to a clear and sufficient level instances of the 'no blame' solution should be eradicated or minimised.

In principle, we agree that if customers have met the requisite standard of care they should be reimbursed on the basis that the standards / obligations for all parties are more sharply defined, including as suggested in Annex 1, and so by design, instances of no blame should be minimised.

For reimbursement in a no blame scenario to be successful a fair, inclusive and sustainable funding model would need to be created which incentivises all parties to take requisite care. This must be accompanied by clear standards of a sufficient level to avoid creating a central fund that may drive firms and customers to do the minimum.

We believe that a model funded directly or solely by PSPs would not provide the correct incentive for PSPs to take requisite care and be unfair where they have. We would not support such a model. It would also not incentivise other parties with the ability to reduce APP scams to take action e.g. online market places.

We discuss our thoughts on potential funding models in our response to question 10 below.

Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

To ensure a simple and clear customer experience for a customer who has been victim to an APP scam, we agree that the sending firm should administer the reimbursement.

The practicality of this approach is dependent upon the inter-PSP model and, more generally, the mechanism for the sending PSP to engage the receiving PSP to determine and confirm the receiving PSP's adherence to its standards. This will be more complex in the case where the receiving firm does not participate in the Code and the inter-PSP model will need to specifically accommodate this scenario.

Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?

Please see our response to question 8, with regard to reimbursement in a no blame scenario.

Reimbursement in a 'no blame' scenario is a complex question as reflected by the Steering Group's ongoing work in this area. We participate in the No Blame Advisory Group and will support the efforts to identify viable short- and longer-term funding options as well as appropriate sustainable governance for such funding.

We think it is crucial (both for the practicality of any funding model and to ensure the Code achieves its intended outcomes) that the scope and need for 'no blame' funding is minimised as far as possible. To achieve that:

- Firstly, we would reiterate that greater specificity within the Code is required to ensure it is clearer and more certain in any given scam scenario - which party is to 'blame' (and we have suggested certain modifications to the Code in Annex 1 to achieve this).
- Secondly, greater and more frequent repatriation would ensure that stolen funds are recovered more often and are available to be returned to the victim (this would also ensure those funds are taken away from the fraudster, again furthering the Code's objectives). We would therefore encourage a renewed focus on repatriation initiatives.

Further, in order to incentivise the correct behaviour for all parties, it is vital that the 'no blame' funding mechanism is fair and sustainable. Therefore, key to developing such a funding mechanism will be:

- Incentivisation of <u>all</u> parties with the ability to reduce APP scams to take requisite care (e.g. including on-line market places etc). We believe[2], that a central fund financed solely / directly by PSPs would not provide such an incentive; and
- Customer and firm standards being clear and of a requisite level, as suggested by Nationwide, to help to ensure that parties remain incentivised to take sufficient care.

It must be remembered that APP scams are a crime, the proceeds of which could fund other illegal activities. We perceive there is a risk of a central fund inadvertently serving to perpetuate this crime. This is another reason

[2] Expressed in our January 2018 consultation response

why any central fund should cover a narrow range of 'no blame' situations in which requisite care has been taken rather than in any way incentivising a minimum level of care by parties.

A phased approach to the establishment of any funding model could be taken. For example:

- In the short term, exploring the utilisation of fraud proceeds funds restrained by PSPs to date (i.e. prior to the Code's implementation), where the true owner of the funds has not been identified.
- In the longer term, considering the creation of a mechanism across wider parties with an ability to prevent APP scams from occurring (for example, firms such as telecoms companies, data handlers etc.) through which they pool risk. Or a mechanism could be partially funded by ICO / Data Protection fines in recognition of the impact that large-scale data breaches have (and, to an increasing extent, will have) on the occurrence of APP scams.
- The concept of the voluntary insurance fund at para 4.6 of the Consultation also merits exploration, as this would avoid the burden of 'no blame' funding being passed onto non-victims and equally ensure that those customers, who want such protection, receive it.

Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

We believe the greater the precision of the Code, the simpler it will be for parties to evidence they have met the expectations and followed the standards of the Code (see Annex 1). The Evidential Approach Working Group should consider:

- Evidentiary standard for PSPs with customers: We would encourage that customers are asked to evidence to the greatest extent possible their compliance with the Code in the course of a transaction. For example, through the use of check boxes to acknowledge that they have read effective warnings given based on information they provide during the transaction (for example, on transaction purpose).
- Evidentiary standards for PSPs: We would encourage standardising the approach to demonstrate adherence to the Code and the development of an efficient and consistent mechanism through which the sending PSP can engage the receiving PSP to confirm the latter's compliance without the need for scrutiny of their position. The inter-PSP process followed for cheque fraud could be considered in this context.

Q12 Do you agree with the issues the evidential approach working group will consider?

We would request that the Evidential Approach Working Group have the remit to consider:

- The specifics of the principles in the Code at Sections SF1 & 2 and R and seek to illustrate these in the form of practical guidance (e.g. case studies).
- What 'Gross Negligence' is in an APP scam context and provide further guidance and examples (we do not believe this should be left solely to the FOS, given that it is essentially a new concept for APP scam assessments).
- What evidence would be required for different scam types, potentially developing check lists for use.
- Development of case studies and examples of vulnerable consumers in relation to APP scam scenarios to assess the robustness and practicality of the vulnerable customer definition and rules, and thereby influence the development of clear, sensitive evidentiary standards - including tests to enable the assessment of how vulnerability affected a customer's ability to act on an effective warning or to use CoP etc. Or, in other words, demonstrate how the vulnerability played a part in the decision to transact.
- The level of specificity for measures and minimum standards for receiving firms who are in a strong position to identify and mitigate APP activity through, acting on intelligence appropriately, application vetting and transactional analytics.

We would encourage the provision of case studies and additional guidance to enable micro-enterprises and charities to develop internal payment procedures to avoid falling victim to APP scams (as per R2(1) (e) and noted in our related comments in Annex 1).

Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

As above.

Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

As discussed in our response to Question 5 above, challenges which will need to be considered in the development of evidentiary standards include the difficulty for the sending PSP to:

- Assess vulnerability in some cases, particularly for digital channels, prior to occurrence of a scam; and
- Identify if a vulnerability, particularly one that is dynamic, did impact the customer's susceptibility to an APP scam.

We are concerned that the current definition of vulnerability is so broad it will be difficult to evidence and could make the Code's provisions on vulnerability difficult to operate and prone to false claims. We would ask that this is considered as above in the development of evidentiary codes.

Some potential methods for identifying vulnerability include enabling customers to volunteer information in account opening or ongoing account management scenarios. Not all customers are willing to reveal such details however. Alternatively, they may not regard themselves as 'vulnerable', or sometimes their vulnerability may inhibit them from self-identifying as vulnerable.

Something that could be effective is asking a customer if they have any additional information which they believe should be taken into account when assessing a scam payment.

PSPs should be entitled to ask for further evidence of the events of a reported scam on a case by case basis – whether related to vulnerability or not – and the PSPs should not be limited on the form or extent of such requests.

Q15 Please provide views on which body would be appropriate to govern the code.

We know this is an active debate at the industry level. We have felt the best placed organisation for the governance of the Code could be Pay.UK. As the setter of rules and standards for the UK payments industry, the operator for Faster Payments, governance body for Confirmation of Payee and Transaction Data Analytics this would seem a good fit. However, we have asked Pay.UK about this in open forum and it appears its strategic direction and operational plans do not include such a role. Other payment system operators, notably in the cards space, have evolved mature dispute and arbitration processes and sustain extensive dynamic operating rules. In fairness, these are not completely comparable given their long history and the commercial models underpinning this administration.

However, there are some characteristics we would wish the governance model to feature. These include that it should:

- Continue to take advantage of the financial crime expertise of UK Finance, but not be an integral part of UK Finance operations as this would risk a conflict of interest given that members and their customers can benefit from the trade association remaining independent of the payment systems.

- Have the engagement model to inform and influence public policy where needed – for example, around balancing the tension between access to banking and security and ensuring minimisation of barriers to entry to the market by considering the operational costs and liabilities for some smaller, or new players.

With these points in mind, we will liaise further with UK Finance on its ideas on this topic, which we note include governance being brought within the Home Office led Joint Fraud Taskforce.

Q16 Do you have any feedback on how changes to the code should be made?

This would depend on the governance structure for the model and the size of the change.

We strongly believe that PSP engagement in proposed changes to the Code should extend beyond the current APP Scam Steering Group and would wish involvement in this. This could either be through direct representation on the governance body or indirect representation via constituent representatives to shape the Code.

Again, the delineation of requirements in development in the CRM and new solutions such as Transaction Data Analytics must be completely clear.

Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

The 50:50 apportionment for 'shared blame' has the benefit of a clear apportionment which avoids the need for protracted disputes between PSPs. It could also help to drive the correct behaviour by both the sending and receiving PSP.

However, we would suggest that the implementation of a 50:50 allocation methodology is limited to a set transaction value size and everything above this size should enter (or at least permit one or more of the PSPs involved the option to instigate) a separate ADR process for determining the apportionments based on the circumstances of the case.

Q18 Would the ADR principles as adopted by Open Banking in section 7 of its Dispute

The new Open Banking Disputes Management System is intended to address a range of scenarios which could result from the use of Open Banking from a payment initiation or AISP scenario. Under the CRM, the scope for dispute should be narrower:

- Disputes should only arise between PSPs as customers will have direct redress via the FOS.
- The issues in dispute should relate only to the CRM and, specifically, which PSP was at fault and to what degree.
- Each dispute should relate to an individual APP case and, as a result, the value of the dispute should be more limited.

Taking these CRM-specific factors into account, we would suggest an ADR mechanism for the CRM is correspondingly simpler and more focused. This could take the form of an efficient adjudication process sitting outside of the FOS which allows the PSPs the opportunity to resolve the dispute between themselves based on a standardised process and, failing that, enables them to refer the dispute to a pre-determined and independent adjudication body and calls for a prescribed menu of evidence to be provided by the PSPs.

A decision would need to be taken about how PSPs who do not participate in the Code are linked into this disputes and adjudication process and customer reimbursements more generally. Further, where non-participants are linked in, we believe that their liability should (as far as possible) be determined on a consistent set of standards to the participating PSP. The prospect of non-participating PSPs acting as receiving PSPs under the Code raises several key issues. In particular, where the receiving PSP has not implemented the Code, how

is the sending PSP to engage the receiving PSP to determine whether the receiving PSP is at 'fault' under the Code? Similarly, in that same scenario, if the sending PSP chooses to reimburse the customer on the basis of its determination of the receiving PSP's actions, how will the sending PSP recoup that reimbursement from the receiving PSP?

We believe these are crucial questions that should to be resolved before adoption of the Code. Otherwise there is a risk of a two-tier reimbursement approach, which confuses customers and potentially leads to unnecessary FOS escalations and delays. Particularly if it is not possible to determine if the receiving PSP is at fault.

We would also encourage consideration of the solidity, speed, clarity of responsibilities and timeframes of the disputes management models of the card schemes. These tried and tested scheme rules provide hard specific scenarios where liability is enforced and understood by all. These are good characteristics of disputes management systems and we would encourage their adoption for this ADR mechanism.

Q19 What issues or risks do we need to consider when designing a dispute mechanism

The disputes resolution process should provide for quick resolution between PSPs – and non-participating PSPs - in as many cases as possible without the need for costly and time-consuming adjudication processes (where this can be avoided). We would encourage the consideration of value thresholds with different applicable rules – to avoid a disproportionate amount of time spent on small value transactions but allowing for a more extensive process for large payments.

Apart from proportionality, other features of a disputes management process should be clarity, practicality, efficiency, effectiveness and smoothness of process and over time consideration of automation.

The identity and profile of the adjudication body will be important as will the development of correct evidential standards.

Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

We see among the positive impacts of the CRM to be:

- Greater visibility of scams and potential to increase customer education and awareness to take care. It is not clear however, how customers will know the impact of their actions under the CRM. Consideration will need to be given to this in the implementation of the Code.
- A more consistent experience for consumers who have been scammed and certainty of outcome.
- Continuing focus on methods to tackle APP scams by all parties with a power to influence (depending on the development of an inclusive 'no blame' funding model).

It is possible to envisage negative impacts, such as:

- Customers may expect reimbursement in a wider range of circumstances than reflected in the Code. Customer communication on the parameters of the Code and their need to take requisite care will be important.
- Customers may not want to justify the actions they have taken or disclose vulnerability indicators. Again, customer communication will be key here along with reassurance on privacy etc.
- PSPs may need to limit or restrict some payment services – particularly if customers have been a previous fraud victim.
- There are potential macro level impacts and we must be careful not to create barriers to new PSP competitors entering the market based on a fear that compliance and liabilities may be onerous.
- There may be an uplift in first party fraud which can partially be addressed by clear, defined rules, definitions and clear evidentiary standards.

- Allowing scope for claims management companies activity if the Code is too vague and breeds disputes between customers and PSPs.

As above, the implications for vulnerable consumers should be clearly understood. As recognised in PAS 17271 and the Code these need not always be negative. A possible consequence of the CRM is that Sending PSPs consider whether to offer to withdraw or suspend certain payment facilities from a customer's account where the customer has identified themselves as vulnerable (or has been a previous victim of fraud). But there are other payment facilities which a vulnerable customer could use, such as using debit and credit cards, which are less prone to these forms of abuse due to the features of those payment facilities including dispute and charge-back processes and due diligence of merchants by their acquirer. A Firm may encourage a vulnerable customer to prefer these card payments over Faster Payments and CHAPS.

Any implications on operation of Power of Attorneys – under which either the attorney or the customer could be transacting - should be considered.

Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

The positive elements:

- Greater protection and reimbursement of customers affected by APP scams.
- Clarity for customers on what they reasonably need to do to protect themselves from APP scams and an improved experience for customers who are victims of scams with a clear route through to redress.
- If correctly defined, clarity for sending and receiving PSPs, of what is expected of them to 'prevent', 'detect' and 'recover' as effectively as possible in relation to APP scams.
- A foundation will be laid to build on as further solutions are developed and implemented in the market, including Confirmation of Payee and, later in 2019, cross industry data analysis and collaborations including cross-industry anti money mule solutions.

The possible negative effects for firms from the implication of the Code include:

- Customers expecting reimbursement in all circumstances – leading to a poor customer experience. Very clear customer messaging will be necessary to avoid this.
- Linked to above is the lack of a common understanding / misconceptions on scams and their variations which may result in poor customer messaging. To effectively tackle scams there is a need for stakeholders – including government, regulators, media and consumer groups - to develop a common understanding of scams, scam types and measures to address to enable effective communication and solution implementation. An example of this is CoP, which checks the payee customer account name in advance of a payment, however the payee name will not actually be checked as part of the later transaction processing. This is one of the reasons why it is very important the Code's guidance must be clear to customers and PSPs and must align with solutions such as CoP as they are implemented.
- Whilst it is undoubtedly positive that the collective industry as well as individual firms and solution providers are building defences against APP scams, it is important to understand the limitation of elements such as CoP. With that in mind, we feel the New Payments Architecture being developed by Pay.UK should include transactional security in its scope, levering the potential benefits of ISO 20022 messaging standards and potentially enabling name validation on the actual transactions in flight before funds are available to withdraw.
- Competition and effect on new entrants: The Code could discourage new entrants to the payments market if they view compliance to be uneconomic. The development of third party vendors to meet some requirements could help with this but this should be factored into implementation plans.
- Capacity & Resourcing: The CRM and underlying measures such as CoP are being implemented at the same time as the industry is looking to deliver Open Banking and Secure Customer Authentication. We would ask that the implications of this are considered and we continue to encourage the development of an effective business case for each new measure prior to mandating these going forward.

- Ongoing costs of compliance – including the costs of establishing CoP and other measures and collection and provision of evidence will obviously create an overhead but in the longer term we would hope this may be offset by the improved prevention and detection of scams.
- Awareness of the CRM and underlying measures amongst all PSPs.
- Firms should be able to distinguish reports of APP scams from complaints. This applies in both the treatment of individual cases which may change from a reported APP scam to a complaint if the customer wishes to challenge the PSP's decision, and in the overall regular reporting of scams and complaints that PSPs produce.
- Clarity on status of different measures in the CRM: There is a risk that the status of certain measures are not clear (for example, PAS 17271) and are therefore inappropriately considered by the FOS as relevant in determining liability. The Code must be very clear on issues of status.
- Potential that APP scams are seen to be a victimless crime: If only PSPs fund reimbursements and wider players such as Internet Service Providers and telecommunication companies) do not take seriously the work they can do to address scams this could have a perverse result of an escalation in APP scams.

Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?

- There will be additional friction on push payments which will run counter to previous industry pattern of movement to frictionless payment journeys – although our research shows that customers can prefer some friction in appropriate circumstances. Nevertheless, customer education will be necessary to understand why payments may be challenged or extra information provided, collected and requested.
- Consideration will need to be given to customers' willingness to share additional information, if asked, at the point of instructing a payment, on which a PSP can demonstrate they have taken the requisite level of care.
- PSPs may need to examine their customer offerings of FPS and CHAPS depending on the final shape of the reimbursement model. A fair code which incentivises requisite care by all parties can help mitigate this risk.
- There is potential for first party fraud which can partially be addressed by defined rules and clear evidentiary standards.
- Claims management activity may spring up if the Code is too vague.
- The impact of the eventual funding model for 'no blame' scams would need to be understood.

Q23 How should the effectiveness of the code be measured?

By:

- Measuring the reduction in value and volume of APP scams (indeed we believe this is the most important measure of the Code's effectiveness).
- Its progressive enhancement to include relevant new developments as they emerge e.g. CoP.
- It being effectively managed and governed including the operation of disputes and a minimisation of disputes with customers on reimbursement and between PSPs on liability.

We would encourage the measuring and monitoring of APP scams with unauthorised push payment frauds. The two fraud types are related and monitoring the two together can help identify trends and industry action. For instance, authorised push payment scams occur partially as PSPs and regulation, such as PSD2, are increasing the security so that only the customer can transact.

Annex 1: NATIONWIDE DETAILED COMMENTS ON THE CODE

Party	Provisions in the Draft Code	Nationwide Comments
ALL		
	DS1(2)(b) 'Best Practice Standards (BPS)' (subsequently referenced in SF1(6) & SF2(5))	The BPS do not currently extend to the apportionment of reimbursement costs – we therefore suggest this aspect of the BPS description is removed in DS1(2)(b). Whilst the Society is signed up to the BPS, we believe that SF1(6) and SF2(5) should reflect and seek to accommodate the fact that many PSPs are not. For instance, is the intention that those firms must adhere to the BPS in order to comply with the Code?
	DS1(2)(c) Definition of 'Business Day':	The definition provided makes 'Business Day' dependent on whether the relevant firm is open for business. This is significant as timescales within the Code are defined in Business Days. We would ask for clarity on this as: • Some firms (which are open at weekends, for example) will have less time in which to meet their obligations; and • Payments can be made on any day via online banking and mobile banking. We would suggest adoption of the definition Monday to Friday, with the exception of bank holidays.
	DS1(3) 'Industry Standards' or 'Industry Guidance'	This passage refers to industry standards of guidance "which apply at the time". We would strongly suggest greater clarity and definition as to what will constitute industry standards for the purposes of the Code (given the potential significance of this classification). For example, in what the sense do the standards have to apply, and to whom? If these standards are voluntary, are they to be included in this definition? The references to "a relevant recognised body" should be given more specificity to avoid any future confusion as to which bodies have the remit to influence the Code's requirements.
	DS2(1)(b) First Generation Payments	We note this provision is intended to clarify that the Code applies to '1st generation' payments only. We believe that the second sentence may require clarification in that regard – it seems to provide that the payment out of the recipient account is only out of scope of the Code if the payment is made to a different firm, whereas we suggest that it should provide (more simply) that "The onward transmission of the APP fraud funds *from the* recipient *account into a different account is* out of scope *of the Code*" (with the earlier part of the current sentence being removed).
	GF General Expectations of Firms	We would suggest that this section further clarifies the status of the 'general expectations' and, specifically, whether or not they are intended to influence reimbursement liability under the remaining sections of the Code (our understanding is that they are not, but this is not presently clear from the Code itself).
CUSTOMER		
	R2(1) Assessment of matters in decision to reimburse	*"The assessment of whether these matters can be established should involve consideration of whether they would have had a material effect on preventing the APP fraud that took place."* The phrase 'material' is open to interpretation and dispute. We would suggest the insertion of clearer wording, along the lines of "whether they are more likely than not to have assisted the prevention of".
	R2(1)(a) Customer ignores Effective Warnings given by a	We suggest this section is amended to explicitly require customers to follow and act upon PSP warnings, rather than prohibiting customers from ignoring warnings (i.e. an amendment akin to "*the Customer did not follow (in part or in*

Party	Provisions in the Draft Code	Nationwide Comments
	Firm during Payment Journey	*full) an Effective Warning given by a Firm…*"). This would increase appropriate customer incentivisation, provide more certainty for customers as to what is expected of them and better incentivise PSPs to include clear, simple and practical scam prevention steps in their effective warnings.
	R2(1)(b) Customer must take appropriate actions following a clear negative Confirmation of Payee result	The term "clear negative result" in this passage should be defined. We believe that this should include a 'no' or 'close match', contained within the Pay.UK Confirmation of Payee solution. Clarity on this – and the relative position of the CRM with other verification outcomes - would be valued however to avoid confusion or any conflict in outcomes under the Code and the CoP rules. Subject to the above, we suggest that the Firm warnings which accompany the clear negative CoP responses should constitute effective warnings for the purposes of R2(1)(a) and SF1(2) (save that we do not envisage the CoP warnings needing to be tailored based on payment type, which we believe is already accommodated by the existing words "where possible" in SF1(2)(c)). For clarity, and in view of our suggestion for R2(1)(a), we suggest that the reference to "appropriate actions" in R2(1)(b) be changed to "the suggested actions". The use of "appropriate" in this context leaves room for doubt over what is required, whereas it will be clearer for all parties if customers are expected to carry out the steps recommended by their PSP. To enhance customer incentivisation, we believe the Code should independently require the payer to undertake payee verification steps on a 'no match' and 'maybe' Confirmation of Payee match (with customers being supported in this regard by specific prompts / guidance from the sending firm).
	R2(1)(c) Customer recklessly shares access to their personal security credentials or allows access to their banking system	We believe the clarity and certainty of this provision would be greatly improved by removing the word "recklessly" from this sentence. A specific carve-out could then be added to this provision to permit customers to share access with legally authorised 3rd party providers. We say this because it is unclear what would constitute "recklessly sharing" in this context and this could be interpreted as introducing a different test to gross negligence. This change could then be supported by requiring PSPs to provide guidance to customers on the risks of sharing security details as part of their education and awareness campaigns under GF(1).
	R2(1)(d) Customer must take reasonable steps to satisfy themselves that a payee was the person they were expecting to pay	To ensure the appropriate incentivisation of (and care by) customers, we would suggest that R2(1)(d) should entail a positive and unqualified obligation for the customer to verify that the person they believe has requested the payment of them has indeed made that request, with customers to be supported in this regard by PSP prompts during the payment journey. We believe such an addition would assist in preventing scams arising from impersonation and/or interception.
	R2(1)(e) Where a Microenterprise or Charity, customer must follow its own internal payment procedures	Micro-enterprises & charities should be required to have an internal payment process with safeguards against APP fraud risks. Otherwise, those without a process for approval of payments would be better placed under the CRM than those with a process, because they could not be held to account for failing to follow that process. A positive requirement to have such processes and safeguards would remove that unfairness and incentivise the taking of requisite care by the customer. Additionally, without that change to the Code, it may prove difficult for PSPs to ascertain if a micro-business has such a process or not. The need for, and content of, such processes for microenterprises & charities could form part of the customer awareness programmes referenced at GF(1).

Party	Provisions in the Draft Code	Nationwide Comments
		We would encourage the Evidential Approach Working Group to give of some case studies and additional guidance to enable micro-enterprises and charities to develop such processes. The words at the end of R2(1)(e) ("would have been effective in preventing the APP fraud") duplicate / overlap with R2(1) and, we suggest, are not required.
	R2(1)(f) The customer must deal with their firm openly & honestly	The obligation to act 'openly and honestly' should be extended to require customers to be open and honest with their PSP during the payment journey – including on the initiation of a payment. We recognise the concern expressed at para 3.60 of the Consultation around the effect of such a requirement in cases which entail the customer being coached to lie to their PSP. Nonetheless, we believe a balance needs to be struck here because customer openness and honesty during the payment journey is, in our view, crucial to the operation of the Code and, more generally, scam prevention. If the information provided by the customer at the payment stage is false, this would then distort / prevent the provision of effective warnings by the sending PSP. We therefore believe that the concern expressed at para 3.60 of the Consultation can be tackled by, firstly, ensuring that PSPs' consumer awareness programmes guide consumers to recognise when they may be being coached; secondly, by ensuring that vulnerable customers (who are most likely to be susceptible to coaching) receive additional protection – in our view, that protection is already provided by R2(3).
	R2(2) Impact of Firm acts / omissions	Whilst we understand the intent of R2(2) (in light of the explanation at para 3.63 of the Consultation), we think this provision could be misunderstood or have the potential to over-complicate the reimbursement assessment. We accept that the actions (or omissions) of the sending and receiving PSPs are important overlays. However, the required Firm actions are already set out under the Code. It is therefore unclear to us whether R2(2) is guiding Firms to consider: (a) Its actions beyond the scope of those required in the Code – we do not consider this would be appropriate giving the breadth of those Firm standards and the care and deliberation that has gone into producing them; and/or (b) The causative impact of those actions on the customer – if so, we believe this is already accommodated by R2(1) (see our comments above) and the drafting in R2(1)(a) – (g). For instance, if an Effective Warning did not adhere to SF1(2), then our reading is that the customer would not be in breach of R2(1)(b) if they did not follow it. Any causation qualification beyond that would risk confusing liability outcomes under the Code (which already seek to cater for common blame scenarios), .
	R2(3) Reimbursements to vulnerable consumers	We would suggest the removal or qualification of the wording in R2(3)(a) "the impact of the fraud on that Customer". We do not believe the impact of an APP scam on the customer should influence the assessment of whether it was reasonable for that customer to have taken the requisite care under the Code at the time of the payment. This comment also applies to R2(3)(e). Further, whilst we agree with the principle outlined at para 3.71 (which we understand to be that, for the purposes of R2(3), the vulnerability must have impacted the customer's ability to adhere to the specific standard they failed to adhere to), we do not believe that this principle is clearly reflected in R2(3). We therefore suggest a clear insertion to the main section of R2(3) to reflect this

Party	Provisions in the Draft Code	Nationwide Comments
		principle, in order to avoid any confusion or the need to read across to the Consultation document to interpret this provision. The dynamic nature and broad definition of vulnerability within the Code will make it very difficult for PSPs to proactively identify vulnerability – particularly in certain channels. We believe this must be recognised in the application of SF1(4) and R2(3). We would ask that the Evidential Approach Working Group develop clear, sensitive evidentiary standards – including tests - which inform the assessment of how a vulnerability played a part in a decision to transact. For example, by affecting a customer's ability to act on an effective warning. The development of this could be helped through the production of case studies and examples.
	R3(1)(b) Customer reporting	We understand this provision is intended to refer to the date the Customer reported the APP fraud to the sending firm, and we suggest this is clarified in its wording.
SENDING FIRM		
	SF1 Greater level of protection to customers considered vulnerable to APP fraud	Following the words "Procedures should provide a greater level of protection for Customers who are considered vulnerable to APP fraud", we suggest adding "(where reasonably possible)" to reflect our comment above on the difficulty of reliably identifying dynamic vulnerability and through particular channels. We suggest a similar addition to SF1(4).
	SF1(1): Appropriate action to identify customers and payments with a higher APP fraud risk through transactional data, behavioural analytics and staff training on APP fraud indicators	The Code should include a requirement (as a prevention measure) on a sending firm to refuse the payment where it establishes the customer is acting upon unsolicited contact from the Police or another bank or building society, or indeed commonly impersonated bodies such as HMRC and DVLA, unless it is satisfied by the customer's explanation. This additional requirement is would reflect the high likelihood that a payment in such circumstances will constitute an APP fraud. We therefore struggle to see how it would be appropriate for a sending firm to proceed to make such a payment, even after further enquires of its customer as to the circumstances of the payment request.
	SF1(2): Provide Effective Warnings on APP fraud risks during the Payment Journey	We would suggest the content of the warnings should be standardised across the industry and agreed to the extent possible by the FOS. Standardisation of warnings analogous to "The value of investments can fall, and you may not get back your original investment" would help customer education, awareness and consistency of messaging.
	SF1(3): Implement Confirmation of Payee and provide appropriate guidance to customers to assist their decision to proceed and understanding of the risks	The Code should include practical verification steps to be included in Confirmation of Payee guidance and for this to appear upon both 'no' and 'close' CoP matches.
	SF1(4): Identify and protect vulnerable customers	It will be difficult, if not impossible, to identify vulnerable customers in digital channels. We believe that this should be considered in the application of the obligations in SF1(4) of the Code
	SF1(5): Where an APP fraud concern is held, delay the payment	We suggest the reference to "to the extent possible" is moved to the end of the para, or repeated, to reflect the fact that the PSP may not be able to communicate

Party	Provisions in the Draft Code	Nationwide Comments
	pending investigation through a risk-based approach	with the customer during the investigation due to Proceeds of Crime Act constraints.
RECEIVING FIRM		
	SF2(1): Reasonable steps to prevent accounts from being opened for criminal purposes (including following CDD requirements and using shared intelligence sources / industry databases)	We would request that this provision be clarified to confirm it applies to accounts opened *after* the date of the Code and that it identifies the specific requirements to be complied with (which we suggest should be the JMLSG Guidance) and the shared intelligence sources to be consulted (we suggest FISS & CIFAS).
	* SF2(2)(a) Prohibition of Use of Confirmation of Payee as a means to reduce potential liability	It would be helpful to have additional clarity – potentially through examples - on the intent of SF2(2)(a) - "*Firms should not use Confirmation of Payee as a means to reduce their risk of potential liability for funding the cost of a reimbursement to a Customer in a way that would be likely to prejudice or unduly disrupt legitimate payments*." We would also question whether such a provision should be the sole preserve of the CoP standards (and therefore be removed from the Code altogether) or, alternatively, be moved into Section GF of the Code as a general expectation on the grounds that Firms' adherence to this provision would not be relevant to an individual reimbursement assessment.
	SF2(2): Implement Confirmation of Payee	We would request that the Code requires the receiving firm to act on a clear pattern negative Confirmation of Payee matches, which should trigger a requirement on the receiving PSP to undertake a review of the account and, subject to that investigation, take appropriate action to restrain the account / the funds under SF2(5).
	SF2(3): Take reasonable steps to detect APP mule accounts through transactional data, analytics and staff training	We would request that the Code includes measures and minimum standards for receiving firms who are in a strong position to identify and mitigate APP activity through, acting on intelligence appropriately, application vetting and transactional analytics. The level of specificity should be worked through in the Evidential Approach Working Group. For the longer term, PSPs in collaboration with UK Finance and other stakeholders, including infrastructure providers and other vendors, should continue to support cross industry initiatives with the potential to use network level data to defend against this crime, defining regulatory or legal barriers for escalation where necessary.

Personal Banking
PO Box 1000
Gogarburn
Edinburgh
EH12 1HQ
www.rbs.co.uk

15 November 2018

APP CRM Steering Group
C/o The Payment Systems Regulator
12 Endeavour Square
London
E20 1JN
By e-mail: app_scam-pso-project@psr.org.uk

Dear ,

The Royal Bank of Scotland Group plc ("RBS") welcomes the opportunity to respond to the Consultation Paper. We are also appreciative of the opportunity to provide direct input to the design of the draft Code and the supporting Standards through representation in the APP Scams Steering Group and its expert support groups.

RBS is committed to the many initiatives underway to raise standards of consumer protection across the payments sector. We consider the finalised and agreed Code will first and foremost lead to more consistent PSP service provision to help consumers to be better protected from APP scams, and become more aware of what they can do to help themselves.

To ensure wide adoption by industry, RBS considers that the Code should be set at the level of what is reasonable and proportionate for the majority of PSPs (large or small) to implement and adhere to and also what it is reasonable to expect of an average consumer. In addition, we believe that PSPs should be given adequate time to prioritise their delivery of the standards, which would mean giving the Code time to 'bed in' without substantive change or revision. This period should be at least 12 months.

Developing the draft Code has demanded that its Steering Group balance complex and legal issues. The consultation reflects these, where for PSPs, changes are both procedural and technical and, as such, greater consideration requires to be given to the implementation/adherence timetable proposed. This should factor in the practical implications for PSPs unfamiliar with the Code proposals. New initiatives, such as Confirmation of Payee, will require adaptation to systems and processes, together with testing across industry to ensure customers remain confident of their payment journey.

Although the draft Code centres on the role of PSPs in reducing APP scams and protecting consumers, fraud and scams are enabled through a much broader eco-system including Internet Service Providers, telephone network operators and retailers who hold customer information. We see this industry Code as a catalyst for others in the ecosystem, perhaps recognised by a reinvigorated Home Office - Joint Fraud Task Force, to take parallel and interconnected activity which will also help to tackle this societal issue.

RBS agrees that consumer vulnerability is a significant consideration in the Code and CRM. However, it must be recognised that customer vulnerability should be formally evidenced and established, if we are to prevent consumers from bringing false or inflated claims. This will need to be sensitively and carefully managed.

There are a number of unresolved and complex legal issues arising out of the draft Code which we would urge the Steering Group and Government/Regulators to consider, they include:

- Potential competition and public policy risks on which body issues the final code as well as the fact that a voluntary code can only go so far. For issues around liability in particular, it might be more appropriate for regulation to be put in place to ensure legal certainty and a level playing field across the industry.

- Tension between the draft Code's requirement to slow down or delay payments and requirements under the PSR 2017 to make payments quickly/without friction.

- The lack of a legal vehicle for repatriating suspected proceeds of crime and consequential legal risks on PSPs.

- Regulatory tension between the draft Code requirements to take a precautionary approach to freezing payment accounts and the requirements under the Proceeds of Crime Act.

- Inter PSP refund apportionment and in particular lack of clarity on the position where one PSP is not signed up the Code

Please address any questions on our response to [x] who can be contacted by email at [x]

Q1	Do you agree with the standards set out in the Standards for Firms.

RBS supports the standards in the draft Code in principle. Having been closely involved in the development of the draft Code through the APP Scams Steering Group and the supporting working groups, we consider the standards expected of firms to be both balanced and reasonable. We strongly believe that if implemented well by the majority of PSPs the standards will improve the protection offered to consumers. However, as mentioned in our introduction, challenges of implementation should not be under-estimated, not just for smaller PSPs, but where significant development is required to deliver new initiatives across multiple payment channels in larger PSPs.

The Code should be seen as evolving as new initiatives and standards are delivered with the application of the CRM moving in step. We consider it imperative that a robust and realistic implementation plan and timetable are developed by industry. We believe it equally essential for the PSR to acknowledge these challenges and take on board the views of all PSPs. We want the Code to be a success and do not want to risk a compromised Code being introduced through poor implementation and / or limited take up by PSPs.

The PSR and Steering Group must consider the implications of some, or many, PSPs not adopting the Code and the consequences this could have both for consumers, and other PSPs who have followed the Code. There is a risk that patchy adoption of the Code will add confusion and less certain outcomes for consumers and may lead to a greater caseload for the FOS to manage.

Of the standards, we would pick out the Confirmation of Payee (CoP) service for comment. Whilst we expect this to build customer confidence that they are paying who they are expecting to pay, it remains a solution that will ensure only that the name given matches that for the account held by the payee PSP. It will therefore be more helpful for a customer who enters incorrect account details or is tricked into sending a planned payment to a fraudulent beneficiary (e.g. invoice / payment redirection fraud). It will have limited impact in identifying a fraudulent payee, where both the name and account details are correct.

We note too the PSR's intention to consult on a general direction on participants in Faster Payments to meet specified dates in 2019 to introduce CoP capability. Whilst noting PSR's wish to see early adoption by these PSPs, in our view the PSR and Steering Group members need to be aware that CoP is only one of many delivery programmes which industry has to meet as part of a heavy regulatory agenda. The timing and complexity of certain deliverables, depending on the PSP, are demanding of the same internal specialist and technical resources. Priorities include meeting Open Banking and PSD2 RTS SCA timelines and undertaking Brexit changes. This is alongside emerging activity to prepare for RTGS2 and NPA, in particular ISO20022 adoption, as well as wider changes on FOS reporting,

In addition, CoP should not be seen as a simple delivery for PSPs or industry. In order for it to work well for customers, PSPs will need to ensure limited friction in the customer payment experience, combined with consistent name matching results to retain customer confidence. In addition technical changes to customer channels, development of new procedures and training for impacted staff will all be required. Furthermore, there are Data Protection obligations to be fulfilled and time needed to ensure adequate opt-out for customers that need this.

To enable SF1 (5,a) and SF2 (5) to be as effective as possible, we would welcome regulatory comfort on the ability to slow down payments and/or to freeze the proceeds of fraud (even where the National Crime Agency has granted 'Defence Against Money Laundering ("DAML")' to a Suspicious Activity Report). Whilst we note that Regulators have referred to PSPs relying on their T&Cs in this regard, we believe formal guidance from the FCA/PSR on this issue (or a regulatory framework) making it absolutely clear what is allowed so removing any uncertainty on this issue and making it easier for all PSPs to act and freeze the proceeds of fraud.

In addition, SF2 (5) requires the repatriation of funds to victims and whilst we are fully supportive of this as a desired outcome, there is no legally identifiable vehicle (in the absence of a court order) that allows PSPs to ignore the customer mandate and take money from an account, even that of an alleged fraudster, to return it to another bank to reimburse a victim. Banks do take a risk based approach in returning funds in these circumstances, but in doing so could constitute a breach of contract and could give rise to a claim in damages, if the customer turns out not to be a fraudster or victim.

There may well be unintended consequences with the Code and CRM and there is a possibility that some PSPs will consider that certain customers may pose too great a risk of being a money mule, either intentionally or unintentionally, or becoming a repeat victim of a scam. This may lead to some PSPs de-risking and excluding certain sections of the population from their banking services.

Finally we would suggest that the Code, being voluntary, should clearly explain that the Standards for firms do not create any additional legal liabilities, beyond current law and regulation which could be relied upon by litigants outside the scope of the Code.

Q2	**We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims.**

We interpret this question as inferring that PSPs will not follow the Code fairly with a starting point of trying to find reasons to avoid reimbursing customers. We cannot speak for other firms, but do not accept this inference and confirm our support for the overriding principle that if a consumer has done nothing wrong in falling victim to an APP scam, they should be reimbursed. We also support the principle that if a sending and / or receiving firm has failed to meet the standards, and that failure has contributed to the loss, they reimburse the consumer's loss appropriately. This position is subject to agreeing a clear, workable and fair approach to evidential standards and agreeing a sustainable source of funding to support no blame outcomes.

We consider it essential that a PSP assesses all factors relating to a customer's claim to reach its reimbursement decision. In the event that the majority of PSP standards have been met and the standard missed would not have prevented the scam, then we do not consider it reasonable to expect the PSP to refund the claim. We would expect the PSP to be able to evidence this assessment in the event the case becomes a complaint to the FOS.

In R2 (1) we note the equivalent requirement of firms to consider whether the requisite standards of care, if followed by a consumer, would have had a material effect on preventing the APP scam from taking place. In our opinion these corresponding standards are balanced.

We strongly believe that it is not in any firm's interests to adopt such an approach and would expect the FOS to spot this trend through complaint referrals.

Q3	**We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.**

For the Code to be effective, all PSPs should assess APP scam claims on a case by case basis rather than, for example, apply a principle of finding fault at the earliest stage, i.e. customer compromise and basing their decision on the first point of failure.

We would expect that the majority of PSPs will follow standards effectively and be able to clearly evidence compliance. On this basis "shared blame" cases should be the exception but in the event that blame is shared, reimbursement on an apportioned basis would seem to be the most equitable approach.

We understand the basis for the proposal that PSPs could pay the equivalent amount of the APP scam loss into a central pot as a fine and that the victim would not be refunded, thus supporting the incentive to act with care principle. However we do not consider this is workable. Our view is that if a PSP has an option to help their customer through reimbursement or pay an equivalent "fine" into a central fund to refund other consumers, the PSP will most likely choose to look after its customer. Arguably it is even

more unlikely that a receiving PSP would pay into this central fund. We therefore do not support this proposal.

This is another scenario, where the PSR and / or Steering Group must consider what would happen if one or both PSPs had not adopted the Code, This needs to be considered ahead of the finalised Code being published.

Q4	Do you agree with the steps customers should take to protect themselves?

We agree with the requisite level of care for consumers but regard the draft standards as the minimum that is reasonable to expect of an average consumer. We would not support a proposal to set a lower level of requisite care for consumers and believe that in doing so the PSR's objectives to reduce APP Scams would be at risk.

Fraudsters and scammers directly target consumers who are therefore the "first line of defence" and should be expected to act with caution when asked to make a payment or buy good or services which would appear to the majority of consumers as "too good to be true". Some scams can be complex and very well constructed but there are many scams which are easily detected by the average consumer at the outset.

The requisite level of care (RLC) standards for consumers need to be applicable to all scam types and all consumer groups. This is not easy to achieve in a relatively concise Code however we consider that the RLC for consumers and SMEs offers a solid foundation. However, we would stress the importance of an effective approach to evidential standards and what is reasonable to ask consumers making a claim. An analogy would be consumers providing evidence to support an insurance claim albeit in these circumstances the event is accidental or unintentional. We have to bear in mind that a consumer has authorised a payment which transpires to be an APP scam.

We can foresee difficulties around vulnerability with PSPs having to tread a fine line between investigating a claim, gathering evidence to support a customer's claim of vulnerability and respecting the customer's privacy. There is a risk that PSPs' investigative processes are applied rigorously to identify exaggerated or bogus claims and in doing so put customers who are genuinely vulnerable through the same evidence gathering process.

We are concerned that the concept of Gross Negligence has been included as a measure of customer conduct under R2(1) (g). There is no legal definition of Gross Negligence and whilst it is used as a test to determine liability for unauthorised transactions, we do not believe that the test can be equated in the same way for APP scams. If Gross Negligence is to be included in the code, it is important that the Steering Group determines a reliable and workable definition which is applicable to APP Scams

With respect to R2 (1) (f) and customers acting honestly in their dealings with the PSP, The Bank has a clear legal obligation to act in accordance with its customer's instructions. In certain circumstances, such as in situations where the customer's instructions should put the ordinary prudent banker on inquiry, the law implies a duty of care to question the customer before proceeding with the transaction. If the Bank makes such enquiries and is satisfied with the customer's responses then the Bank has met its duty of care toward the customer (so is not liable for the transaction). We believe the code should reflect the law in these circumstances.

We consider that it will be essential for the PSR, PSPs, consumer bodies and other stakeholders involved in the Code to communicate clearly and consistently on what is expected of consumers in relation to requisite level of care. This needs to be factored into implementation plans and media briefings.

Q5	Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

We take our role and responsibilities in relation to vulnerable customers very seriously. We have policies in place to support early identification of customer vulnerability and we respond appropriately and treat

vulnerable customers fairly. We support the approach set out in the consultation and Code and recognise that vulnerability will be a contributory factor in some situations but not all. We agree with the observations in the consultation that vulnerability does not in itself mean that a consumer will be more susceptible to APP scams and / or certain types of scams, e.g. a customer who is lonely falling prey to a romance scam may not necessarily be more susceptible to a purchase scam. Therefore where vulnerability is considered to be, or claimed to be a factor, a case by case assessment is essential.

It can be very difficult to detect vulnerability with our customers and some customers who are vulnerable may not want to be regarded as such. By its very nature, customers who are vulnerable may not be aware that they are vulnerable and therefore may not declare it to us. Temporary vulnerability caused by life events adds to the difficulty in ascertaining periods of vulnerability.

We are concerned that consumers who are not otherwise considered to be vulnerable may claim to be vulnerable or be directed by third parties to claim that they are vulnerable to increase the possibility of reimbursement from the sending firm. This may lead to customers who are genuinely vulnerable having to go through challenging processes due to the incidence of fabricated claims.

Unintended consequence – the bank may block or delay a genuine payment created by a vulnerable customer. If this is a time critical payment, this could lead to a complaint / litigation.

Q6	**Do you agree with the timeframe for notifying customers on the reimbursement decision?**

The guidance should make it clear that PSPs should aim to complete investigations promptly and provide a clear decision / outcome to the customer as quickly as possible. We would anticipate that the majority of reimbursement decisions will be notified to customers between 1 to 5 days. However we agree that up to 15 working days and in exceptional cases this being extended to 35 days to allow PSPs or Consumers time to investigate / gather appropriate evidence is appropriate.

We can envisage delays arising between sending and receiving banks to evidence that standards have been met, particularly for high value or complex cases where escalation or internal or external legal opinion may be required. We would again note that the Code needs to provide guidance where one of the firms does not subscribe to the Code.

Q7	**Please provide feedback on the measures and tools in the Annex to the code, and whether there are other measures or tools that should be included?**

The list of measures and tools in the Annex to the Code will be useful for PSPs who may not be aware of some of these initiatives. We are already involved in many of the measures noted and as mentioned in our earlier response there is an extensive regulatory programme of changes underway, which PSPs working to meet and need to be borne in mind. It will be important to assess the benefits of each initiative where this is possible and prioritise delivery where the benefit to consumers will be greatest.

Some of the measures and tools are more suited to certain customer delivery channels and it will be sensible for PSPs to consider which initiatives are most appropriate for their business model and customer propositions.

We would hope that the Code and measures will evolve as fraudsters and scammers change approach and consumer preferences in how the make APP payments changes over time. The Code will need to be relatively dynamic to keep pace with these factors.

We are pleased to note that the BSI PAS is included as good practice. We sponsored the production of British Standard Specification in 2016 / 2017 with the aim of helping the sector raise its standards in how we protect customers from fraud and scams. Working with industry leaders, the PAS has been adopted by and incorporated into the Joint Fraud Task Force Victims and Susceptibility work stream and will create a sector benchmark and guidance within the industry.

Q8	**Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?**

Yes as outlined earlier in our response we support the principle that a consumer who can evidence that they have met the requisite level of care as currently described in the draft code, and considered not to be at fault, should be reimbursed. It should not however lead to a prescriptive transfer of liability to a firm who has also met the standards expected of them. The principle is contingent on finding a sustainable funding solution(s) to the "no blame" scenario.

As set out in the introductory section of our response, the Code assesses blame and no blame in relation to the consumer and sending and receiving firms involved in the payment. However, the root cause of the scam and the methods used to execute it can often sit outside of the consumer and PSPs control and responsibilities. Examples include; data compromise of a third party, an ISP being used to host a fake website, social media used to recruit mule accounts or target victims or lax controls with a mobile network operator. These real life examples can all contribute to the scam. We would encourage the PSR and other stakeholders to look beyond the PSPs when funding for No blame cases arises. In our opinion reapportioning fines for data breaches towards a central funding pot would have merit.

There is a risk of first party fraud (i.e. the risk that customers / fraudsters may conspire to send money from one account to another and then the sending party may claim that they have been scammed out of the money, followed warnings, undertaken due diligence etc. and to all intents and purposes met the requisite level of care. The 'victim' will be reimbursed and the beneficiary will retain the original payment (albeit the money will no longer be in the beneficiary account). We have no legal means on sharing data on claims made and settled and using this data positively to protect consumers or to detect potential organised ring frauds. It is recommended that PSPs record and report incidences of first party fraudulent claims and attempted exploitation of the CRM.

Q9	**Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?**

We agree that the sending firm is best placed to support the customer, keep them updated on progress and administer any reimbursement, regardless of funding source. As outlined in our original response to CP17/2 we did not consider that it was appropriate or indeed would support the aims of the APP Scams CRM to apportion liability to a sending and / or receiving firm who had met the standards in a Code.

We have commented earlier in response to Q6 on the difficulties that could arise in complex or high value cases between PSPs, further complicated by the involvement of PSPs who have not signed up to the Voluntary Code. This complication should be considered in respect of administering reimbursement too and its resolution is critical to the viability of the Code.

Q10	**What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?**

We endorse the approach which is being progressed by a sub group of the APP Scams Steering Group to assess the viability of various funding options. These options include PSP funded, customer funded, Government initiative funded and funding options from the wider APP scams eco-system. We are encouraged that the Consultation recognises the difficulties in proposing that PSPs should fund no blame outcomes. We have stated previously that APP scams are a societal problem and require a societal response.

Rather than comment on each proposal in 4.6 we consider it is more appropriate to await the outcome and recommendations from the No Blame Funding Sub Group. However we would stress the importance of any recommended solution being fair for all parties involved, that the source of funding identified is sustainable and that all PSPs who sign up to Voluntary Code can practically support it. For instance we do not consider that imposing a fine on a firm in a shared blame scenario where an equivalent amount to the value of the scam is transferred into a central fund is workable. Furthermore we consider this proposal would only exacerbate a customer's distress in falling victim to a scam.

We would be supportive of proposals which centre on reapportioning funds which are frozen or possibly linked to criminal proceeds, or to reallocate fines incurred by third parties for data breaches which can then be linked to enabling fraud and scams. The legislative changes required to support proposals like these should not be a barrier and we would urge Government though the Joint Fraud Taskforce to

progress this. From a wider perspective it is evident that technologies now deployed by PSPs and across industry to protect consumers have overtaken the relevant legal frameworks which currently hinder funds repatriation and reimbursement. This must be addressed to support optimised operation of the Code.

We urge Government, via the Joint Fraud Taskforce, to review the legal position on repatriating frozen criminal funds, in particular those locked in 2nd/3rd generation beneficiary accounts. The technology on tracing funds is constantly improving, but the law has not developed at the same pace. An established legal and regulatory framework for returning such funds would substantially increase the value of funds recovered and repatriated to victims of fraud.

Q11	How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?

We endorse and are actively supporting the approach which is being progressed by a sub-group of the APP Scams Steering Group to develop effective and fair evidential standards for sending firms, receiving firms and for consumers. Having practical guidance produced and available to all PSPs will help to provide a consistent approach for firms gathering evidence from consumers to support claims and set an expectation with consumers on what is reasonable to provide.

We would anticipate the majority of PSPs would have prescriptive record keeping requirements and audit trails with systems to record and retain what system actions were performed, what customer interactions occurred and what the outcome of these events were. For instance we would expect firms to reproduce records in respect of in the moment warnings across all channels and in due course have clear activity records in relation to confirmation of payee messaging and responses.

Current legislative and regulatory requirements in respect of account opening controls are prescriptive and already subject to stringent assessment and checks.

It is important that the evidential standards provide guidance to PSPs and Consumers in respect of handling cases where vulnerability is evident, or is claimed to be a factor in falling victim to the APP scam. We have expanded on this point in our response to Q14.

It is reasonable for PSPs handling claims to expect customers to share all relevant background and circumstances leading to the APP scam events and be able to evidence the steps they took to check the authenticity of the payee e.g. a purchase scam by evidencing that they checked a trusted source or didn't settle off platform i.e. outside EBay, AirBnB etc.

Q12	Do you agree with the issues the evidential approach working group will consider?

Yes we agree that the issues the evidential working group will consider are appropriate. It is important that the working group not only produce practical guidance for PSPs and consumers but that this is communicated clearly and widely. It is also essential that PSPs who intend to sign up to the Code are given realistic timescales to implement the guidance and adapt their systems and processes accordingly.

This is a positive development for PSPs and for consumers and will set expectations which do not currently exist.

Q13	Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

We suggest that the Steering Group should consider a limitation period for consumers being eligible for reimbursement under the CRM. This will ensure timely reporting by consumers and support recovery efforts as well as valuable intelligence sharing by PSPs with law enforcement. Our suggestion would be that the timelines align with those set out in the PSR 2017, namely 13 months from the date of the scam.

Q14	How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

We consider that this should be undertaken on a case by case basis with an assessment undertaken on a customer's decision making process based on their personal circumstances, for example accessibility issues, cognitive difficulties or life events. In addition to gathering any relevant information that would help the case, depending on the assessment we would recommend making reasonable adjustments for the customer for the future. We would need to make sure that this was in line with our GDPR / privacy and Customers in Vulnerable Situations policies.

Q15	Please provide views on which body would be appropriate to govern the code.

We understand that Pay.UK and the Lending Standards Board are emerging as the front runners to be potential code administrators – each with their own advantages and disadvantages; however it remains important for the Steering Group to consider best practice on voluntary code governance. The UK experience is somewhat limited but other English-speaking countries make greater use of them, and their code governance frameworks offer useful insights. The LSB experience and breadth of managing a range of codes, gives it more maturity as a code administrator and it is supported by an experienced team, which could be supplemented with specialist knowledge as needed. It also has in place a board with extensive expertise. This will be important here where the Code may see as its subscribers any and all of banks, building societies, credit unions and other types of PSP and FinTechs etc.

We believe this Code should have its own advisory committee made up of representatives of key stakeholder groups, which could include trade association representatives on behalf of their members. These will be important to ensure onward communication and awareness raising to their members, and also to monitor subscription levels, as well as where necessary feeding in views of subscribing members to the advisory committee for example, in the event of proposed code changes. In addition, whilst an industry code, the administrator and industry will need to consider whether the advisory group includes consumer body representatives, or other means to seek input on how the code is working.

We consider too that the advisory committee will wish to monitor data on scams and e.g. related complaints to assess if action needs to be taken. It should also produce an annual report and undertake wide engagement ahead of the periodic code reviews, Such a group will ensure the necessary transparency to the code by providing a 'public window' into its progress and outcomes.

We anticipate the first code review will take place after a year to support the annual report, with the advisory committee to determine whether to remain with annual or move to a two or three yearly cycle. Good practice suggests that these committees should themselves be subject to an independent review on a three yearly cycle and we would expect this to coincide with say replacement of say a third of the committee members to ensure continued 'fresh eye' assessment.

We believe that the PSR and/or potentially the FCA may wish to provide an observer to the advisory group.

In respect of Pay.UK, we are aware of its role as administrator to the smaller code for indirect access providers. This is a discrete code whereas the new code of practice will have broader subscription, and whilst specific to PSPs, is less about participation in payment systems and more about customer detriment, fraud mitigation and protection and a well defined reimbursement model. Where any actions from the code of practice are specific to what a PSP that participates in a payment system must do, this may require Pay.UK to be engaged to incorporated appropriate provision into scheme rules. It will also be important for the new code administrator to take on the final code immediately the final code is ready for publication. Pay.UK has a busy portfolio and this is not an essential additional service for it to take on at this time.

We would also call out that we do not consider it appropriate for the Steering Group which drafted the Code for consultation, to issue the final code and/or take it into its launch and implementation phase. There are legal risks both to the Steering Group members and the PSPs represented arising out of any

such approach. This means that in our view, the Code administrator or another interim administrator must be appointed to coincide with the finalised Code being launched.

Q16	Do you have any feedback on how changes to the code should be made?

Changes to the Code should be managed through the appointed Code Administrator with the support of an appropriate specialist advisory body. As stated in our response to Q15, we would recommend that the first code review will take place after 12 months and referenced in the Code Administrator's Annual Report.

Given the wide-ranging and detailed changes that the Code and standards proposes, it will be important that the Code is given time to bed in and at the end of the first year to make only essential clarifying changes.

At all times, the impact of proposed changes will need to be assessed and time given to subscribers to implement them., Where changes impact consumers, every effort must be made to remove complexity. This may confuse and so lead to unintended consequences, which might erode confidence in the Code itself.

We would support annual reviews in Year 1 and Year 2 and consideration after this time to perhaps a review every 3 years after this.

Q17	Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

In the interests of simplicity and expediency a 50:50 reimbursement approach would seem to be the most appropriate solution otherwise we will get into the realms of having to give a weighting to certain aspects of the code, which will be complex and burdensome.

The challenge may arise when there are multiple first generation beneficiaries. For shared blame cases with multiple beneficiaries or where some of the PSPs subscribe to the Code. This is another issue that requires careful consideration by the PSR and / or Steering Group.

We understand in DS2 (1) (b) why scope is limited to first generation accounts but there remains a need to support easier repatriation of scam funds from second generation accounts. It is incongruous that "Bank A" is being held liable to reimburse a customer when "Bank B" may have funds frozen and essentially locked in a second generation beneficiary account. This is an issue that the Joint Fraud Task Force should consider addressing.

In terms of repatriation of funds we consider it would be beneficial if the FCA assessed the legal implications with HMT with a view to issues a letter of comfort and guidance to firms to support victim reparations.

We would expect PSPs to have effective monitoring and reporting in place to track shared blame cases and have appropriate remediation plans in place to address any recurring failings, or factors which may aggravate APP scams.

Q18	Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the code?

A primary principle of the Dispute Management System and Code of Best Practice is for parties to make every effort to ensure that claimants are treated fairly, impartially and receive the best possible outcome. In the context of the CRM, there could be merit in using it as a mechanism for two PSPs involved in a claim to exchange information in order to reach agreement over which party or parties is liable. The DMS is not an arbitration process and there would need to be consideration given to appointing a 3rd party to adjudicate over the dispute with further consideration on how this would be funded.

We note that the DMS has not been properly tested in terms of efficiency, effectiveness and fairness given the gradual roll out of open banking services. Given the volume of APP scams, we would expect

there to be a more significant pipeline of cases, at least early on when principles are still being established. We believe more granular work is required as to how quickly any decisions can be made to avoid creating a backlog of outstanding decisions.

Q19	What issues or risks do we need to consider when designing a dispute mechanism?

The dispute mechanism between PSPs needs to support reaching an outcome for the consumer in a timely manner. This is fundamentally important. The mechanism needs to be transparent to customer and firms involved with clear expectations on the process being set and why.

The mechanism needs to be expedient and economic as there will be a cost attached to dispute referral and resolution. It needs to be clear how the dispute mechanism is funded. It will also need to be clear how the mechanism interacts with established law and regulation as well as how its decisions would affect parties' ability to pursue claims in the civil courts.

Q20	What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

Positives

- If the Code and standards are widely adopted by PSPs, coupled with raised consumer awareness of what constitutes requisite levels of care, there should be a notable decrease in the incidence of APP Scams and a corresponding reduction in funds becoming criminal proceeds.

- Consistency of approach by PSPs leads to consistency of outcomes for consumers with greater clarity and rationale supporting reimbursement and non reimbursement outcomes.

- Greater consumer awareness and education should arise from industry, Consumer groups and positive media coverage on the Code implementation.

- An effective Code can promote greater consumer confidence in payment systems and reassurance from new services in certain circumstances, e.g. Confirmation of Payee.

Negatives

- It is possible that some consumers may over estimate the level of protection the Code and Standards offer and consider there is a greater level of protection and almost guarantee of reimbursement. This impact can be mitigated to an extent through clear, consistent coverage of the Code and communication from all stakeholders.

- As mentioned in our response to other consultation questions some consumers may have difficulty accessing banking services due to PSPs de- risking certain customer groups.

- Customers who are in genuinely vulnerable circumstances may be subject to rigorous investigation, evidence gathering to support a claim. This may be a consequence of other consumers claiming that they are vulnerable to increase the possibility of reimbursement. Consistent guidance on the approach to evidential standards may help PSPs identify genuine vulnerability.

- It is possible that some third parties will offer APP Scam reimbursement services and charge fees to already vulnerable customers.

Q21	What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

Positives

- The Code presents the opportunity for all PSPs to follow a consistent set of improved standards with supporting guidance. The creation of evidential standards will assist PSPs with difficult investigations in sensitive situations i.e. vulnerable customers.

- The Code is designed to provide consistent outcomes to consumers and where reimbursement is not made, consumers can be provided with a clear reason why this decision has been reached.

- PSPs adhering to the standards for Firms and being able to evidence compliance will help PSPs handle complaints consistently and support provision of evidence for FOS referrals.

- The Code's format will allow it to evolve and to develop over time as standards improve consumer behaviour changes and technologies and regulatory changes occur.

Negatives

- There is a risk of false, fabricated and first party fraud claims.

- The Code could have anti competitive consequences in that it could be seen as costly for PSPs and a barrier to entry to the payments market. This could be mitigated with clear guidance from the PSR as to expectations on PSPs around implementation and a reasonable timetable as to expected adherence. In addition, the risks of competition challenged against the PSPs represented at the Steering Group could be mitigated through the final Code being issued by the PSR (rather than the Steering Group).

- The Steering Group's work in developing the Code could be susceptible to challenge by way of Judicial Review on the basis that it (the Steering Group) has exercised a public function in developing the Code. It is not acceptable that Steering Group members should be carrying any legal risk. This risk could be mitigated by the final Code being issued by the PSR or another more appropriate entity (rather than the Steering Group).

- FOS costs and case work increase. When assessing whether to compensate victims, PSPs are required to consider whether the customer's actions would have had a material effect on preventing the APP fraud taking place. PSPs must also asses whether they themselves have complied with the standards set out in the Code. This type of evidence evaluation may be difficult for some PSPs to undertake and is likely to lead to challenge, not only at the FOS but also in the civil courts.

- Lack of certainty for sending PSPs where the receiving PSP is not signed up to the Code, the Code does not appear to provide for this.

- As explained in response to Q1, PSPs will be under increasing risk of breach of mandate and damages claims as a result of freezing and returning funds as required by SF2 (5). This can be mitigated through clear regulatory guidance or an appropriate legal framework for freezing and repatriating funds.

- The Code may create conflict between banks when establishing compliance with the Code and seeking interbank reimbursement.

Q22	**Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?**

- Unintended consequences which may impact consumers have been highlighted through our response to earlier questions. We would envisage that the majority of cases will be investigated quickly and consumers are informed without delay if they will be reimbursed and / or if funds can be recovered on their behalf.

- If some PSPs do not subscribe to the Voluntary Code this could lead to inconsistent outcomes and confusion for consumers in an already complex area. There is a possibility that some PSPs will assess certain customers as too risky either because they are considered to be susceptible to APP scams or

may have the hallmarks of a mule account or likelihood of becoming a mule account. This de-risking effect may lead to some customers struggling to access banking facilities.

- In establishing whether a consumer was vulnerable at the time of the scam, evidential standards may require banks to assess customers rigorously to manage the risk of exaggerated claims or first party fraud claims.

- We must avoid the misconception that the Code and PSPs will protect all customers from scams and provide reimbursement in the event of a scam. The importance of consumers understanding their responsibilities and what requisite level of care means has to be made clear.

Q23	**How should the effectiveness of the code be measured?**

- We consider the effectiveness of the Code should be measured against the aims of reducing the harm caused by APP scams and in doing so the value of funds which become criminal proceeds. There are various quantitative and qualitative measures that should be used to measure the effectiveness including;

- Early and sustained adoption of the Code by PSPs measured by combined payments market share and reassessed after 6 month and 12 months.

- Incidence and value of reported APP scams tracked over time.

- Qualitative feedback from PSPs, Consumer Groups and Consumers

- Trend in APP Scam complaints referred to the FOS - Upheld rates etc.

- Code Administrator annual report, with progress update and list of market participants signed up to Code.

- Code website to be set up to provide effective information on the Code and its management, how its Administrator can be contacted and details of its subscribers

- Monitoring of the effectiveness of specific standards e.g. CoP to determine their impact and contribution

APP Scams Steering Group:

Consultation Paper on the Draft Contingent Reimbursement Model Code

Response from Santander UK plc

Overview

1. Santander UK plc (hereafter 'Santander') is pleased to respond to the APP Scams Steering Group's consultation on the Contingent Reimbursement Model draft code (the 'Draft Code').

2. Santander welcomes greater focus on consumer protection from APP scams and measures that can be taken to minimise and disrupt fraud. We are generally supportive of the proposals in the Draft Code including those related to customer education and awareness which we already place significant emphasis on, and which are central to effective fraud prevention. In addition, we support additional controls such as confirmation of payee and effective warnings which introduce stop and think moments to help customers avoid falling victim of increasingly sophisticated scams.

3. While we understand the focus on PSPs, absent a holistic package of targeted measures addressed to all participants which touch the consumer journey, we believe that the Draft Code will fail to address the root cause of APP scams. Instead the allocation of greater responsibility and liability to PSPs, in the absence of a targeted package of measures across all relevant sectors, is likely to originate fraud risk by not incentivising consumers to be careful, therefore incentivising fraudsters and creating moral hazard.

4. We believe consumers' interests are well served by focusing on reducing opportunity for fraudsters to succeed with APP scams i.e. prevention is inherently better than cure. Santander and other industry participants have pursued a number of initiatives in recent years to address this. In addition to its own education and payment journey initiatives (see below), Santander continues to contribute significantly to industry work such as the project identifying mule networks and 'Take 5 to stop fraud'. We believe these initiatives plus confirmation of payee will better protect consumers in the near future. Santander acknowledges that as a PSP it plays an integral part in preventing APP scams, but advances in payments and communications technology and related infrastructure have created an ecosystem where vulnerabilities are abused by

increasingly sophisticated and organised criminals to perpetuate fraud. Relevant factors include:

a. faster payments: the speed with which payments can be moved around the system means that fraudsters can very quickly move and dissipate the proceeds of crime (including overseas), often prior to the victim report and therefore without effective detection and disruption; and
b. electronic communications and data breaches: fraudsters exploit IT infrastructure vulnerabilities for specific businesses by hacking email and customer information enabling them to use such information to impersonate one of the parties (or third parties) and perpetrate some form of APP fraud.

5. We believe that alongside those measures in the Draft Code that we indicate we support, there is merit in considering enhancement of protections for consumers around the services of internet providers, telecommunication companies, data handlers and relevant online companies and retailers. There is also scope for more protection to be provided by professional firms and businesses (e.g. solicitors, pension and investment firms, car dealerships, etc.) and their regulators and trade associations to mitigate fraud risk. This includes education around how they and their customers can adopt practices and processes to avoid falling victim to APP scams, particularly in respect of invoice and mandate scams. There is also scope in connection with open banking for third party providers and related parties to acknowledge APP scam risk. The desire to remove friction in the payment process should not be at the cost of enabling APP fraud risk. Law enforcement also have an enhanced role to play in detecting, deterring and disrupting APP fraud.

6. We firmly believe that education and customer awareness is fundamental to the prevention of APP scams. Unfortunately there has been a stark increase in the number of young people acting as money mules in recent years and it is often the case that a recipient bank account in an APP scam has been set up by a 'genuine' customer but then used to receive and move the proceeds of crime. We support awareness campaigns in schools and higher education to warn against the dangers and consequences of becoming a money mule. There is also a role for social media, online advertisers and job and recruitment sites to identify and prevent advertisements seeking money mules.

7. The aim of the Draft Code in standardising behaviours by firms is welcomed and Santander feels that it has already in place a number of the prevention and detection measures set out in it. It is working towards others such as confirmation of payee

and it anticipates that this should be in place by June 2019. The PSR is aware that Santander is the first firm to introduce scam warnings in its online payment journey to try and encourage customers (at the point of payment) to reflect on events leading up to that point and the consequence of proceeding with a payment.

8. Santander recognises the importance of protecting vulnerable customers and is pleased to see that the consideration of customer vulnerability is covered in the Draft Code. However, PSPs cannot be expected to accept strict liability for reimbursing vulnerable customers who have fallen victim of an APP scam and further discussion is required around the definition and application of vulnerability in APP scam scenarios. Each case should continue to be assessed on its own facts.

9. Presently PSPs are only liable for authorised payments in very limited circumstances – recognising that PSPs operate on a customer mandate. There is an inherent conflict between existing law and the proposal to make PSPs liable for authorised payments. It is not clear how any code will fit into the existing legal and regulatory framework and how conflict and uncertainty will be resolved – for example where an issue arises between one PSP which has adopted the code and another which has not.

10. We note that a number of questions remain unanswered from the activities of the Steering Group which are to be addressed through further working groups. In particular, the debate around the standard expected of customers is a crucial one and needs careful consideration. Given the significance of these issues, leaving to one side the measures to standardise processes such as confirmation of payee which we believe are capable of being progressed separately (and which Santander is progressing in any event), we query both the overall content and current proposed timing of the introduction of the code.

11. In summary, we support the measures in the Draft Code around standardisation of certain PSP processes to better protect consumers. We believe a more holistic package of measures is required to address roles and responsibilities of all market participants which touch on the customer journey to properly target and disrupt payment fraud, ensuring that its root cause is addressed and unintended consequences are avoided. We firmly believe that any material adjustment to PSP liability is a matter for legislation or regulation after usual government impact assessment taking account of all relevant factors and the ecosystem within which APP fraud is perpetuated and the role of law enforcement.

Q1 Do you agree with the standards set out in the Standards for Firms?

12. Although we believe that further work is required to clearly document the standards, in principle we support the proposals in the Draft Code that are designed to prevent, detect and improve the response to APP fraud. Santander would welcome the standardisation of measures in this regard as it sets a clear behaviour benchmark for all PSPs. The primary focus in tackling APP fraud must remain preventing it in the first place. The creation of an agreed framework to better protect customers is a step in the right direction but needs to apply to all PSPs.

13. Alongside the code, the correct implementation of industry tools such as confirmation of payee could be of significant benefit to customers and PSPs. Such tools would need to be used alongside detailed warnings and changes to the way payments are currently executed by payment users. Santander have already deployed 'scam' warnings on its payment channels and these will undergo continuous improvement. This is particularly so in respect of our digital channels to ensure we protect customers to the best of our ability.

Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims.

14. Should a final code be implemented, a PSP such as Santander would comply with whatever the standards are and this provision is only relevant if controls are entirely absent. Should the standards be clearly articulated and the test for liability be clearly fixed in regulation, then it is difficult to envisage unintended consequences including the example above.

15. Santander considers that emerging payment journeys (such as those through Open Banking) should not take customers away from appropriate warnings and tools, and should avoid allowing customers to submit payment requests without allowing the deposit holder to test the intention behind any payment.

Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

16. The Draft Code is premised on incentivising all parties to reduce the occurrence of APP fraud and on the understanding that customers should be reimbursed where

they have met the requisite level of care. If a customer has not met the requisite level of care and the loss is therefore a result of their initial action (i.e. by initiating the payment), then it follows that the customer should not be reimbursed. The loss has not been caused by the paying or recipient PSP. If, in this situation, the PSP has also not met the requisite level of care, our view is this should not be a PSP liability. We understand there are ongoing discussions around a PSP in such circumstances making some form of contribution to a central fund that may be used to reimburse customers who met the requite standard of care. Santander is willing to be a part of ongoing discussions in this regard.

Q4 Do you agree with the steps customers should take to protect themselves?

17. Santander considers that further work needs to be done in truly understanding the steps customers should take to protect themselves from APP scams and the requisite level of care expected of them. The standard of care expected of customers and how this is evidenced remains of crucial importance. Granular analysis of common scam scenarios needs to be undertaken so that a proper balance between customer and PSP responsibility is struck in relevant scenarios. The discussion needs to recognise that there is a stark difference in customer behaviour in different scam types. For example, a romance scam perpetrated over a prolonged period of time is not comparable to an isolated, one off mandate or invoice scam. As the Draft Code acknowledges, there are a number of APP scam scenarios and one size does not fit all. If this analysis is not properly undertaken and more often than not liability falls to the PSP, this will create moral hazard because it will dis-incentivise customers recognising the need to take appropriate steps to protect themselves.

18. Santander queries whether a *de minimis* threshold should be applied to reimbursements to ensure proportionality and reflect the risk a customer is taking in making a payment. The impact (i.e. financial and emotional) on a customer who may have paid a small / 'non' life changing sum (e.g. a matter of 10s or 100s of pounds for an item on an auction website that has not been delivered) and a customer who may have paid a substantial and possibly life changing sum of money for a large purchase (e,g. a car or house deposit) who has fallen victim of a malicious payment misdirection scam is significant. If customers feel that even smaller purchases are essentially insured by some form of strict liability, meaning they may be able to recover from their PSP, then this is unlikely to encourage prudent behaviour. There is scope also to consider adjustments to the current faster payments framework (including its speed and sum of money permitted to be transferred) to better mitigate associated risk and potentially reduce customer impact.

19. Any reference to customer 'gross negligence' and this term providing some form of test for the standard of care expected of customers in APP scams is inappropriate and cannot form part of any future code. Notwithstanding the fact that the Payment Services Regulation 2017 (the Regulations) only envisage PSP liability for authorised payments in limited circumstances, the term 'gross negligence' is borrowed from regulation 77 of those Regulations and envisages a situation where liability for a payment may be declined by a PSP where the customer has not knowingly consented to a payment instruction and where that customer has also failed to act in accordance with the provisions of regulation 72 of the Regulations (i.e. the obligation of the customer to act in accordance with the terms governing the payment instrument and its personalised security credentials). That test (an objective one in Santander's view) envisages a situation that is entirely different to the case of APP scams where the customer knowingly consents to a payment (and has acted in accordance with the terms governing the payment instrument) and is therefore afforded some opportunity to assess the risk of proceeding with the payment.

20. Ignoring the wider view that other sectors should play their part in preventing APP scams, Santander is concerned that the Draft Code does not strike a fair balance between PSPs and customer responsibility and as drafted is overly weighted in the customer's favour and punishes a PSP for criminal behaviour being third parties that it is not responsible for. As drafted there appears to be a very low threshold for the standard of expected customer behaviour. Whereas a significant proportion of customer claims are likely to be genuine, a low threshold and short timeframe for assessing claims gives rise to serious concerns. A low threshold may not only serve to drive the unintended consequence of customers exercising less caution (and possibly encourage low value but less serious first party fraud) but more importantly it may serve to encourage organised criminality and fraudulent claims. This may in turn lead to PSPs inadvertently funding and encouraging organised criminality including drug or human trafficking and possibly even terrorist financing.

21. Changes to the payment framework in respect of Effective Warnings and confirmation of payee are a positive step and will build necessary friction into the payment process. It will allow PSPs to challenge both customer 'intent' and the 'payment destination'. Santander welcomes this development and has already put in place scam warnings in its payment journeys to assess and challenge customer intent. This is being rolled out across all payment channels and has already had some notable success. In addition to digital channels, Santander has for some time used 'scam

warnings' in branch and it encourages its branch staff to alert customers to the dangers of scams when making large payments or withdrawals.

22. We will endeavour to make our warnings on every channel as robust and relevant as possible. However for Open Banking Non-merchant PIS journeys where we have presented to the Open Banking Implementation Entity (OBIE) our warnings, we have been met with significant challenge, and told by OBIE that these warnings are 'unnecessary additional steps which slow the customer journey'. We do not agree with the OBIE's position, As such, we have requested the OBIE to review and respond to this consultation and consider their view given the current state of the Draft Code.

23. Despite the above, customers are often socially engineered to ignore warnings provided by firms and for example a customer may be asked to lie or deceive their bank in a 'safe account' or similar scams. Even when customers are challenged on a large payment, they may sometimes simply explain that it is for building work or a gift to a family member. The discussion on the standard of care expected by customers must take account of such circumstances and should recognise that despite best intentions, there is a limit to what PSPs can reasonably be expected to do to prevent customers falling victim to scams.

Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

24. The protection of vulnerable customers is extremely important and a responsibility that Santander takes seriously. However, Santander is concerned that the Draft Code in its current form may essentially impose a strict liability for reimbursing all vulnerable customers who have been the victim of a scam. Often a customer's vulnerability may not be known to a PSP until the scam has been successfully perpetrated and this limitation needs to be recognised. In line with the comments in the introductory paragraph, it does not seem right that strict liability attaches to a PSP for reimbursing vulnerable customers in all circumstances. The task of protecting vulnerable individuals is one that falls to all sectors and wider society including those who are close to and may have responsibility for the personal and financial welfare of the vulnerable customer.

25. The assessment of vulnerability is not, and can never be an exact science. Vulnerability can be temporary or permanent and it may be financial, physical or

mental. A customer's vulnerability may not have impacted on his or her decision to proceed with a payment and this ought to be factored into any decision around reimbursement. The Draft Code does not sufficiently define vulnerability and go into detail on how the question of vulnerability ought to be applied in practice in APP scam scenarios.

26. Santander therefore believes that more work needs to be done in respect of defining vulnerability in APP scam scenarios and exploring in what circumstances a PSP may reimburse a vulnerable customer. Careful consideration should be given as to whether an overly onerous imposition of liability on PSPs in respect of vulnerable customers will result in them restricting a customer's ability to make payments. A balance has to be struck between trying to protect vulnerable customers and allowing them access to their monies to carry out their day to day banking and meet their general expenses.

Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?

27. Santander have no specific comments on this timeframe and in principle 15 business day seems adequate for a decision to be made on reimbursement given the current operational processes. The exceptional circumstances of 35 days also seems proportionate given complexities that may arise on certain cases. Aligning to DISP makes sense in this framework and we have no further comments on this section.

28. It should be noted up to 70% volume of cases managed by Santander at present are related to customers making online purchases using push payments and not receiving goods; in such cases, given the warnings in place (or being deployed over the coming months) it is unlikely these cases will require the given 15 days to process.

Q7 Please provide feedback on the measures and tools in this Annex, and whether there any other measures or tools that should be included?

29. The measures and tools in the Annex are good initiatives and will play their part in preventing APP fraud.

30. Customer education and awareness are particularly important. This should include ongoing education through other types of communications with customers (e.g. in

branch, in booklets, material on websites, direct email and SMS warnings and bespoke communications like Santander's recent Scam Avoidance School). As a side point and in line with the comments in the introductory paragraph above, better customer education must be encouraged in other sectors in addition to the work PSPs undertake in this regard.

31. Santander believes an effective warning around scams must come at the point of payment execution. It would be prudent to publish and possibly even standardise warnings each PSP should / could give in relation to each distinct fraud type (for example in the Annex) when making payments for specific reasons. This would enable consistency across the industry and ensure that certain PSPs are not exposing their customers to differing levels of risk.

32. For example, if the Annex was amended to clearly show what the 'call to action' for the payer is when asked to make a payment of that type, and the entire industry was clear on what advice each PSP should offer, this would be a very powerful preventative tool even in isolation. The warnings Santander have deployed (as discussed above) are triggered by a 'payment classification' to assess customer's intent and for each type, so we can give a bespoke warning.

33. We believe the Banking Protocol is an exceptional tool and should be developed further in line with the Draft Code and be supported by all PSPs. As ever, Santander welcomes all enhancements to data sharing and payment network detection tools and will continue to support these as they develop.

34. Lastly, Santander supports the swift deployment by all PSPs of Confirmation of Payee as a key element for some scam types (CEO Email, Invoice Fraud and 'Safe Account' scams), notwithstanding the fact it should also resolve the issue of customers getting account details wrong outside of scam scenarios. We feel that alongside the technical *use* of this tool by the senders and receivers of payments, a guide to how it should be 'configured' in terms of customer warnings where payees don't match, and what fraud types could be most commonly prevented through its use should be explored in future discussions. The introduction of any code should not be before the impact of the introduction of confirmation of payee has been properly assessed.

Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?

35. At any level, it is regrettable that any customer suffers a loss from an APP scam and that this type of criminality is so prevalent in the modern world. This is particularly so where a customer has exercised caution yet still fallen victim to a scam. The question is not about reimbursement but who is responsible for compensating a victim of a crime and in what circumstances. This is the fundamental question which the sector as a whole needs to answer and requires input from all key stakeholders including government and law enforcement.

36. Santander considers that strict liability cannot attach to a PSP and it cannot fall to one sector to essentially insure customers against the risk of a crime. This proposal oversimplifies the issue and does not take account of what may have actually caused the customer to suffer the loss and the extent to which in the usual course of a banking relationship a PSP owes a duty to a customer. We refer to the comments in our introductory paragraph around APP scams being a society wide issue. Santander has no issue in taking responsibility for circumstances where a failure on its behalf may have caused a loss to the customer but losses are often not Santander's fault.

37. If strict liability is imposed against PSPs and the threshold for the standard of care expected of a customer is set too low, then the risk of moral hazard ensues. This is likely to have the unintended consequence of leading customers to be less prudent.

38. This should not be interpreted as apportioning blame on the victim and PSPs seeking to avoid their responsibilities. All parties should agree the fault ultimately lies with the criminal that perpetrated the crime and such actions should be discouraged through law enforcement and prosecution. Rather it is a question around what is fair and how victims ought to be compensated and in what circumstances. In particular discussions around 'no blame' scenarios and a pooled risk fund (similar to that in other sectors) need to continue so that all possible options are fully explored and analysed. Discussions around how other sectors and businesses may also pay into this pot (e.g. those who are the subject of a data breach) should also be explored.

Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?

39. While key discussions around funding options and the reimbursement process continue and any final framework remains unclear, it is premature to say.

40. The issue would need operational assessment; while a firm has the ability to provide a decision and can support the reimbursement (should it ever be required) the accounting mechanisms and processes at Santander are not supported in the same way as card payment schemes. If we were to compare the chargeback or dispute resolution services used elsewhere, they are backed by significant rules, regulations and operational tools.

41. Albeit with lower volumes, our view is that a dedicated and centralised system to control this would be needed and specified before any PSP would be conformable signing up to creating such an accounting risk; the funding mechanism and entities engaged in the funding should be required to design the model so that PSPs can give their feedback and requirements for any integration, shared resolution and allow them to feed in to the technical feasibility of the design.

Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?

42. Losses in this space are a direct result of criminal activity. Accordingly Santander does not believe that the costs of compensation and the expense of dealing with APP scams should be borne by the payment industry alone, particularly when there has been no fault by the PSP and it in no way caused the customer's loss. It therefore encourages constructive discussions around alternative compensation funding options, which include funding by other sectors and government.

43. In particular, Santander is keen to see that criminal monies that have been frozen or restrained are made available to victims of crime as soon as possible. Mechanisms are being put in place to trace fraudulent monies through the payment systems, which may hopefully lead to more assets being seized. This should discourage criminality and make the United Kingdom a safer place to do business. Unfortunately, in practical terms and given the current legal and regulatory framework a firm cannot return monies to a victim in the absence of a Court order and it is often hamstrung in identifying and assisting the original victim. The work in respect of how criminal monies may be used to reimburse and compensate victims needs to be expedited with relevant input from Government. Significant changes and improvements are required to the current legal and regulatory framework, which at present hinders the prospects of victims being reimbursed. This work needs to be undertaken in parallel with work that serves to discourage criminality and tackles the root cause of APP fraud. Prevention must remain the primary focus.

have provided scam awareness education as part of any prior reimbursement). Santander will continue to be part of the evidential working group and feedback our views through this mechanism.

Q12 Do you agree with the issues the evidential approach working group will consider?

55. Yes, please see our other comments above.

Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?

56. We believe the key will be a standardised form of data exchange and the need to prove a wider control mechanism (or a system to allow the sharing of information about a case / customer) which may require focus on specific actions taken by the customer and the PSP. If this is not the case, it may prove impossible for a recipient PSP (i.e. the firm that does not bank the customer) to assess and evidence whether a customer has met the requisite level of care.

57. A customer's previous claim history (if any) ought to be a factor that a PSP can consider in deciding whether a customer has met the requisite standard of care.

Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?

58. Please see the response to 5 above. This requires further discussion and PSPs would be required to agree standardised practices in respect of information they should request, what serves as sufficient evidence of vulnerability and what form of consent would be required from the customer to share it with third parties. The 'TEXAS' model in debt collection practices could be a useful process to amend and build upon.

Q15 Please provide views on which body would be appropriate to govern the code.

59. Of the options presented, we believe the NPSO (now Pay.UK) seems a logical home for centralised body to manage the treatment of payment related dispute issues and oversee the governance of any future code. Pay.UK are currently creating common standards and a new infrastructure, which will be the 'engine' they claim is there to drive excellence and success throughout the industry. Santander does not consider

that the other proposed bodies would have the necessary expertise. The Steering Group is not an appropriate body to govern, particularly in light of recent legal advice around the public policy risks this would pose.

60. As such, Pay.UK seem the logical home for this code to be governed as it is wholly payment based at present. Should the outcome of the code in operational practice start to drive changes to the way customers make payments, or PSPs construct the ability for customers to make / receive them – they are the logical organisation to control this.

61. Pay.UK could also support reporting mechanisms, refund processes and provide the technical infrastructure required to make this a success and work for customers and PSPs alike. This may solve the issues of data exchange and allow a system akin to those used in other payment schemes (such as Visa / Mastercard) to be introduced centrally and monitored, reported on and updated as the code matures. Any future governance should put in place a tool to govern the code and disputes in a manner that moves away from the use of spreadsheets and email. The possibility of using blockchain technology to control processes and support MI demands should be explored and may even help to identify customers who have made previous claims.

Q16 Do you have any feedback on how changes to the code should be made?

62. Should a voluntary code be accepted by PSPs, any final governance structure will inform how changes to the code can be made? The approach detailed seems logical and some flexibility to drive continuous improvements seems sensible. More significant changes may require wider consultation.

63. Santander believes that an impact assessment prior to the introduction of any code would need to be undertaken rather than simply reviewing whether it achieves its overarching objective post implementation.

Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?

64. Given the complexities we have detailed above we are concerned as to how the agreement on shared blame will be reached and communicated operationally – and how this will be tested. The use of a 50:50 weighting in all scenarios seems like a blanket approach which may not be proportionate to the failing on either side, and as

such a weighting based on types of failure would be required if this was to be implemented.

65. We have not seen as yet any detail as to which specific failures would be considered significant or require potential reimbursement, and as such cannot comment meaningfully unless this detail is available. As such, we will follow this through with the Reimbursement Flow Working Group where our approach would be to make this as fair on each party as feasible.

Q18 Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the Code?

66. We would support the use of an open communication mechanism, but would need to review in detail how this would be adapted and configured given the very different type of dispute being discussed for APP fraud.

67. The OB-DMS code provides an example of what can be established for APP Fraud, although the technical deployment would need different skills on either side (sending and receiving banks) and a very different approach given the type of disputes this is intended to manage. In Santander's view, DMS provides a base to work from but one that would need to be amended and improved to some extent. It should be noted that the ADR does not replace the legal and regulatory frameworks.

Q19 What issues or risks do we need to consider when designing a dispute mechanism?

68. Any inter-PSP dispute resolution mechanism would need to mirror those in the open banking dispute management systems. That is, it should promote dialogue that is clear, consistent, transparent and ethical. This will enable disputes to be resolved swiftly and proportionately.

Additional Questions

Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?

69. We refer to our earlier comments and Santander's ultimate view will be formed once the current work streams have been concluded and a draft final code has been circulated for further discussion.

70. In Santander's view, the promotion of tools to try and prevent APP fraud is a key step and there is a great deal in the existing draft code detailing what steps PSPs can take to prevent and minimise the impact of APP fraud. This includes confirmation of payee and proposals around effective warnings.

71. However, much depends on what the final proposed liability model looks like. A code that imposes a strict liability upon PSPs even where its actions cannot be said to have caused a victim's loss would be beneficial to the victim in the sense of them being reimbursed but possibly detrimental to other customers in terms of costs in the banking system passed back to all customers and exacerbated by the moral hazard (see above).

Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?

72. Our comments above in response to other questions have covered this question.

73. As an aside, any form of code gives rise to potential competition issues. This will be broached by the wider industry with the PSR and separately to this response.

Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?

74. We refer to our responses above.

75. One of our key concerns remains around the proliferation of fraudulent claims. Similarly some customers with a higher risk profile may find it difficult to access payment services. There may be more customer challenge by PSPs in respect of payments made in accordance with mandate. This will impact negatively on a customer journey and likely lead to an increase in complaints by customers who want to transfer monies quickly and where it is not in fact a scam and payment is being made to a *bone fide* recipient rather than an account operated by a criminal.

76. We reiterate our concern that consideration must be given to payments where the customer is not directly engaging with their PSP (through various emerging payment journeys). Such payments may become more risky than currently considered, as the PSP is not able to assess customer intent or deliver suitable contextual warnings.

Q23 How should the effectiveness of the code be measured?

77. Metrics relating to the overall number of reported APP Frauds (at a granular level by type) would be beneficial but this cannot be considered in isolation as a yardstick for success. There may be factors that distort such a simple analysis. For example, customers who may otherwise have never reported an APP fraud could be more willing to do so if they feel that PSPs may be liable to reimburse.

78. We feel that on review of the code, there are a number of areas that would lend themselves to new reporting which (given we have a baseline for 2017/18 reporting) could be tracked against. These would include the statistics on the implementation of point of payment warnings across the industry and the take-up of confirmation of payee. Consumer feedback and awareness surveys may also assist.

79. It should be noted that unless a systematic approach (centrally) to manage claims and process the complexities of these situations in terms of liability is established, this may not be easy to do.

END