September 2018

APP Scams Steering Group

Draft Contingent Reimbursement Model Code

CONSULTATION PAPER

Non confidential responses

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 Respondents were asked to clearly mark any confidential information contained in the response which should not be published.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.

44. The suggestion of a contribution mechanism seems logical given the number of parties often involved in APP fraud. Relevant sectors have their role to play.

45. The proposal of a transaction charge is also a good one but it may have its limitations. While such a charge may encourage a customer to better risk assess the consequences of a payment this approach is arguably at odds with how the faster payments scheme is currently constructed, namely as a way of sending funds as a cash / utility payment. To implement a transaction charge would require significant change to the current payment system to make it fair; again we are looking at a comparison to a fee charging / earning system (payment cards for example) which is not in place at present and would need to be developed.

46. The creation of different types of firm accounts offers a potential view of the future of the 'Push Payment scheme' configuration and could be developed into an operating model which solves a number of issues. In conjunction with confirmation of payee this could be the trigger for a fundamentally different platform on which Push Payments are initiated and received (offering different costs and options for payments depending on reason and value, varied by payment destination, sender and if for personal and businesses reasons) and we would be keen for the Pay.UK (NPSO) to review how a model could be developed which considered designing liability, cost, control and risk assessment into a service which at present lacks this.

47. Santander believes that an insurance policy has limitations. We are concerned that selling insurance for a risk customers are widely unaware of, and may never fall victim to if they operate with due care and attention, is not the right thing to propose. The terms of any insurance would be limited and subject to various conditions and limitations which would limit the value of the cover in real terms or create moral hazard. Claims on such a policy could only be viable / applicable in very specific circumstances and we feel this would need to be reviewed in detail by insurance and legal experts. There have been historic issues around the quality of insurance provided alongside other products.

48. Given the ongoing discussions around the liability model generally and what may happen in 'no blame' and 'shared blame' scenarios, it is premature to comment on the fifth proposal. Santander will feed into the future debate on this.

49. It seems sensible to explore the possibility of using dormant funds to fund in part a central compensation fund. However, Santander has initial concerns. The Dormant Account Scheme is used to fund good causes in the United Kingdom and it is

therefore of great benefit to charitable beneficiaries. Santander would not want anything to detract funds away from such good causes and it may be more sensible to use monies that are the proceeds of crime to reimburse victims of crime rather than 'clean' but dormant monies. Fines for control failures in other sectors that serve to increase instances of APP fraud is a discussion that should be continued.

50. The last proposal of a Government-run scheme similar to the Criminal Injuries Compensation scheme seems the most practicable of solutions. Discussions in this regard should continue so that a more detailed model can be put forward for discussion.

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

51. Should a code be adopted, it will require transparency from both the firm and customer.

52. A firm through its regulators ought to be able to demonstrate on an ongoing basis that its systems and controls align with any final code. A firm could for example provide a control and assurance report each 6 months or so to confirm compliance and set out any improvements or work that is planned or has been undertaken. Regulators can then feel assured that efforts to broach the issue of APP fraud continue. Such regulators can exercise their supervisory powers if they feel that an individual firm is not doing enough in this space.

53. A customer cannot of course be audited but they must be encouraged to be as transparent as possible in making an APP claim. In respect of unauthorised payment claims, Santander has unfortunately experienced a reluctance by some customers to provide a full and thorough account of the events that have led to the unauthorised transactions. In authorised payments scenarios (i.e. where the customer consciously authorised the payment), a customer ought to be able to explain in detail events and what led to their decision to make the payment. A lack of transparency and failure to respond fully to a PSP's reasonable queries ought to provide a basis for the PSP to decline a claim.

54. The above serves to demonstrate why the evidential working groups are so important and that setting the standard of care expected by customers at the right level is paramount. In assessing the customer's standard of care, PSPs ought to be able to take account of whether a customer has made prior claims (particularly when firms

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

TransferWise welcomes the Steering Groups aim to provide better standards and expectations for firms, and better protection for consumers, surrounding APP scams. We hope to offer constructive feedback, that would allow all PSPs to be able to implement this code, or work toward incorporating some of its elements, with the ultimate aim to reduce the attractiveness of this type of fraud.

Q1 Do you agree with the standards set out in the Standards for Firms
Effective warnings: Effective warnings described by the Steering Group demonstrate a measured approach to the problem. We wholeheartedly endorse solution driven warnings, and other controls like Confirmation of Payee (CoP) that will educate consumers and drive down the incidence of APP scams. Please see below for small suggestions on specific areas of the code.

Vulnerable customer identification: TransferWise uses multiple factors, like customer behaviour and age, to determine if someone is at a higher risk of falling prey to an APP scam. However, it is not appropriate for PSPs to be given power to assess someone's financial capability and the APP Scams Steering Group (ASSG) risks the possibility of firms either making arbitrary judgements or being forced to use invasive techniques in order to assess, to use the example given in the consultation document, whether a person's mental health is impacting on their ability to make financial decisions. It would be inappropriate for any business to be asked to judge this, and require their customers to disclose this sort of information. A third party, like the FOS, would be better equipped to judge a consumers vulnerability objectively and fairly, and make a decision on their reimbursement status as a result. This would spare consumers the requirement to share intimate information with their PSP, or any financial institution, and remove the possibility that any business would have the power to judge an individual's ability to make financial decisions.

Response times for APP fraud: The proposed 20 day timescale for a beneficiary bank to conduct an investigation into a customer and determine whether or not to freeze funds (as outlined in the Best Practice Standards) is too long. Upon notice from bank or PSP that received funds are potentially the proceeds of a scam, there are no explicit legal blockers for beneficiary banks to freeze those funds while investigating this. If firms were supported to be quicker to freeze funds, scammers would see a huge reduction in profits. This is the one element of the Code that could be hugely strengthened. Even if many smaller PSPs cannot afford to opt in to this voluntary system of reimbursement, all financial institutions should be encouraged to act quicker once they are aware of an APP scam. This would drastically increase customers chances of receiving reimbursement without full industry participation in the voluntary code, and reduce the likelihood of their money staying in the pockets of scammers. I understand that the initial BPS was referring to 20 day repatriation time limit, but some clarification should be given if firms are being directed to that document to establish reasonable timeframes.

There is also a mismatch between the investigation dates in the Best Practice Standards (BPS) and the contingent reimbursement model (CRM). The BPS offer beneficiary banks 20 days to conduct an investigation, while the CRM requires sending firms to decide whether or not to reimburse a consumer in 15 days. These dates must be aligned so firms can understand whether a legitimate APP scam has taken place, before reimbursement.

Recommending card payments: The guidelines must be payment channel neutral, and not require firms to suggest using a competitors service or a more expensive payment method. Many of our consumers will be paying via bank transfer as it was requested by the recipient business. It's expensive for small businesses to accept card, it's expensive for EMIs to allow card top ups to fund accounts, and it's incredibly expensive for PSPs to fund chargebacks for card payments. This suggestion does not contribute to a shift in consumer behaviour towards making safer bank transfers, or incentivise a shift in PSPs behaviour, or therefore, reduce the incidence level of scams. It goes against the guiding principles of the steering group, to mitigate the risk of paying by bank transfer - not disincentivise the payment method.

There are many legitimate reasons a business may require bank transfer. Card payment steering only works in the digital economy, and for payments to businesses big enough to support that card payments. Many small businesses, or micro enterprises will not support such a payment method due to the high cost involved, and it is not uncommon for scammers to explicitly request bank transfer over card payment. Three quarters of our payments processed in the UK are card payments - meaning that bank transfer scammers are, with some probability, already requesting a specific payment channel and consumers (despite many knowing the risks) are happy to oblige. This could be due to the fact many legitimate small businesses could also not afford card functionality. This could mean customers ignore effective warnings about card payments routinely - as they are accustomed to small businesses being unable to accept card, and therefore not be entitled to compensation - or may prevent SMEs receiving legitimate payments.

This approach does not help to reduce scams in the offline world. Customers should be encouraged to conduct due diligence checks rather than chose a different payment channel. This would encourage good practice in the offline world, where the customers payment method is limited to cash only when paying for goods or services. Card payment steering does not help education or awareness, risks disadvantaging businesses that cannot afford to accept card and is expensive for PSPs to facilitate. It also risks excluding customers who would otherwise be eligible for reimbursement, if they pay via bank transfer. Effective Warnings should focus on effective customer due diligence and equipping consumers to avoid scams in every situation -- which is the key driver of much APP fraud.

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

It is a sensible approach. It allows firms to implement risk based guidance for identified customers, rather than forcing all customers through an identical payment flow. For example, a warning to a customer asking them to double check the account owner, will not prevent a loss when the customer has fallen prey to a romance scam. PSPs should not be penalised for recognising the nuanced risk, and implementing the appropriate controls. This is in keeping fraud and money laundering prevention approach, which allows firms to cater their processes to the customer based on their risk level (i.e. requiring additional identity information etc)

It is worth noting that it would be hard to ascertain whether a customer would have been helped by a warning after the fact.

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.
If the customer has been negligent, no refunds should be made. It will be hard to prove negligence during the payment flow, so PSPs will not be incentivised to weaken their warnings or controls based on any insight into the customers due diligence levels. The aim is to incentivise both PSPs and users to implement better controls before putting money in the hands of scammers.

Q4. Do you agree with the steps customers should take to protect themselves?
It is difficult to prove R2 1.e. It would also be tricky to ascertain whether the customer has acted on effective warnings.

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?
The vulnerability criteria bears no relation to the information PSPs have access to. PSPs cannot assess customers health records, any information regarding balances held with other institutions, or personal information such as family situation. The criteria is only helpful for retroactively determining reimbursement eligibility by an independent body to judge a customers vulnerability. Any request for this kind of information after an APP scam by a PSP is invasive in the extreme. This may also mean that any claim to reimbursement on vulnerability grounds would need to be done retroactively (i.e. after the PSP has decided whether or not to reimburse as they cannot judge - unless in extreme circumstances - whether a customer is vulnerable).

As stated in our response to Q14, it is inappropriate for PSPs to make this assessment, we don't have the skills or the training to come to a nuanced and sensitive judgement regarding an individuals vulnerability. An independent body should be involved to make a fair judgement on individual customer vulnerability. The level of detail needed to judge this is invasive in the extreme, and it is completely inappropriate to expect UK citizens to share this level of information with any PSP that requests it.

The example given in the consultation document suggests that it may be left for individual PSPs to judge whether a person's mental health, for example, is impacting their capability to make appropriate financial decisions. This is an inappropriate level of responsibility for a financial institution and it would be an intrusive process for any customer to undergo. This must be assessed by an independent body.

Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?
Best Practice Standards suggest a 20 day time period for the beneficiary bank to investigate the scam claims and decide whether or not to freeze funds. Yet Recommendation 3 (1) requires firms to make a decision on whether to reimburse in 15 Business days. The final code should correct this oversight, as

the sending PSP should not be required to make a decision on reimbursement before receiving findings about whether the beneficiary bank thinks the transfer is a scam, or simply a disputed trade transaction etc.

As stated before, the 20 day period for beneficiary banks to inform the sending PSP of the outcome of an investigations or freeze funds. It is possible to freeze funds while they undergo investigations for fraud and money laundering, and firms should be incentivised to freeze funds quickly.

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?
N/A

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, but if the ASSG is looking to secure as many PSPS as possible to sign up to the code, they should acknowledge that many of the potential funding sources identified in no blame scenarios, the PSP will be paying to reimburse victims. It is not possible for smaller PSPs or challenger banks to absorb this cost, when there is no fault.

Should PSPs be required to reimburse all victims, even if they have behaved with due care and diligence, the consequence of this would be a lack of competition in the market, an overall price rise for all consumers, most likely indirectly or as a result of a lack of competition in the market, is a reasonable outcome, or identify another source of funds e.g. a government funded scheme or an optional consumer insurance scheme.

Of course, in the case of vulnerable individuals, we must take steps to ensure they benefit from increased protections regardless of funding sources.

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?
Yes but there needs to be a prompt time frame to decide blame apportionment and timely refunding for the sending PSPs if they are not to blame.

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 Q8.

Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?
The code can rely on self assessment, but if arbitration is required, the FOS needs to be supported to expand their capacity to judge this. Assessing a firm's compliance with the AML regs, and the efficacy of internal controls in general is a time consuming activity, and requires specialist skills. The FCA , for example,already has this capacity.

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

Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?
No.

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

It is inappropriate for PSPs to make this assessment, we don't have the skills or the training to come to a nuanced and sensitive judgement regarding an individuals vulnerability. An independent body should be involved to make a fair judgement on individual customer vulnerability, so as not to arbitrarily discriminate. The level of detail needed to judge this is invasive in the extreme, and it is completely inappropriate to expect UK citizens to share this level of information with any PSP that requests it.

The example given in the consultation document suggests that it may be left for individual PSPs to judge whether a person's mental health, for example, is impacting their capability to make appropriate financial decisions. This is an inappropriate level of responsibility for a financial institution and it would be an intrusive process for any customer to undergo. This must be assessed by an independent body.

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

Q16 Do you have any feedback on how changes to the code should be made?
If the steering group wants to include all PSPs, they must facilitate an opportunity for all of financial institutions, not just those who have opted into the code, to feedback on it.

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

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?
N/A

Q19 What issues or risks do we need to consider when designing a dispute mechanism? Additional Questions
N/A

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?
N/A

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?
N/A

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

Q23 How should the effectiveness of the code be measured?
N/A

Transpact – Response to APP scams Steering Group consultation

Dear Authorised Push Payment Scams (APP) Steering Group,

I am writing on behalf of my firm in response to the Consultation on the industry code for Authorised Push Payment Scams.
The points below in response are not in any particular order (although the first point is by far the most important).

1) The draft code is seriously deficient in respect to reimbursement of APP fraud where payment is made into what turns out to be a mule bank account.

   Nearly all APP fraud takes place either through a bank account opened with fake ID, or through a mule account.
   So banks need to take strong active steps to ensure that neither can accounts be easily opened with fake ID, nor can their customers use their legitimate bank accounts as mule accounts.

   So half the battle against APP fraud is down to banks educating their customers not to use their bank accounts as mule accounts.
   However, the problem is currently actually far more significant than that.

   Due to banks' unacceptable inaction, we currently live in a society where account mules can get away with the crime of account muling without significant sanction.
   The problem is this – when account muling takes place, the mule is always immediately caught by the Police, because they are easily and immediately identified – the crime of muling makes no attempt to hide the identity of the mule.
   So the Police forward the mule to the Courts for prosecution.
   But the Courts find that the mule pleads that they were unaware of the criminal nature of their actions, due to no bank education, and the Courts are forced to award no custodial sentence, and no real punishment with a deterrent effect.
   Given that the Police then know that Courts will not pass any strong sentence on a mule worth speaking of, the Police have stopped referring many mules to the Courts – the Police simply do not have the very large amount of time necessary to see mules through Court system in which they end up with no real punishment.

   So we now have a situation, due to bank inaction and lack of bank education, where a mule will be caught by the Police, but face no real prosecution or sanction for their muling crime !

   Why is this a bank problem ? Because the banks are clearly laundering the proceeds of the mules' crimes, and the banks are mandated by law to prevent such money movements. But the banks have failed dramatically to do so.

   The answer is simple and clear, and will greatly improve the UK fraud landscape.
   Banks must provide an educational regime to their customers so that it is clear to their customers that if they act as an account mule, they are acting illegally and can expect a custodial sentence.
   Such a customer education campaign by banks is not difficulty, and is absolutely necessary (although it will not be cheap, as it will require each bank to write to each of its customers with educational literature that will require response).
   Once the banks have educated their customers, the Courts will not have to accept that mules acted out of ignorance, and will start jailing account mules.
   And once Courts start jailing account mules, Police will start referring all account mules

caught to Court – which will be anyone acting as an account mule.
And once mules see that all account mules when caught (and they will always be caught) face a custodial sentence, then no one will act as an account mule anymore, as they will see the inevitability of their action leading to jail – and what today is an easy crime rewarded with significant financial reimbursement and little sanction, will dry up entirely.

The key to this process is banks clearly educating their customers that account muling is illegal – something banks are mandated by law to do in order to prevent the banks from money laundering – but something the banks have abjectly failed to do until now.
(Network level transaction data analytics is not a replacement for such a step, and by itself will only have a limited impact on the problem).

The draft code needs emphatically to reflect the above issue.
So if a customer loses money in an APP fraud, and the customer made payment to a mule account at a bank which did not educate its customers sufficiently that mule accounting was illegal, then the customer should experience at least partial reimbursement through the CRM due to that bank's failure to meet the code and its responsibilities.
At present, the draft code only mentions customer education about account muling in GF1(a) in its General Expectations, but not at all in R1 to R4 'Reimbursement of Customer following an APP fraud'.

The way the code is written at present, R2(1) states that no reimbursement need be made if the customer is found to have transgressed one of seven (a) to (g) events.
So if a customer fails in events (a) to (g) of R2(1), and their money is lost, even if it is lost through a mule account where the bank did not take steps to educate the mule that their muling was illegal, the customer would still bear the loss, and the bank would currently be allowed not to be penalised for its dereliction in customer education.

This is offset somewhat by R2(2), that states that the bank should consider whether the bank's failure impeded the customer's ability to avoid falling victim to APP fraud.
But this is very ambiguous language, and is open to all sorts of interpretation.
It seems to say (or can certainly be interpreted as such), that if the bank's failure did not impact directly on the factors (a) to (g) of R2(1), then the bank can bear no liability.
This is due to the phrasing of '*the Customer's ability'* in the draft code in R2(2). Since the bank's failure to educate the mule concerning the illegality of muling had no relation to the victim customer's ability to avoid loss through APP fraud, the draft code will allow the banks to avoid any loss due to failure to educate account mules.

This is also due to the phrasing '*to meet the Standards for Firms*' in R2(2). Standards for Firms does not include education against account muling – so the draft code lets the banks off scot free for this offence.
Instead the phrasing of R2(2) should be changed '*to meet the Standards for Firms and the General Expectations for Firms'*. (It is the General Expectations for Firms that includes the banks' duty to educate against account muling).

These are two core failures of the draft code as currently drafted.

To mitigate against this, instead R2(2) should be redrafted somewhere along the following lines:

'The exclusions of R2(1) above will not wholly apply where an act or omission of a Firm to meet the Standards and General Expectations for Firms contributed to the Customer's falling victim to the APP fraud. In such a situation, appropriate partial or full reimbursement reasonable basis will be made.'

Even if nothing else in the code changes, the above changes bringing liability to a bank if it does not educate its customers concerning account muling, is a must and mirrors the CRM first Core Principle.

2) This next point I make does not relate to the draft code directly, but is a plea to the Authorised Push Payment Scams (APP) Steering Group.
The other vector that enables APP fraud apart from account muling is bank accounts opened with false ID.
The vast majority of documents used to open bank accounts in the UK are UK documents – mostly UK passports and UK driving licences.

   But the UK Government will not provide an API to banks with which the banks can check whether any one UK passport or UK driving licence has been reported as lost or revoked.

   As a result, a UK bank is forced to accept forged or stolen UK passports and UK driving licences as evidence of identity, allowing criminals to open bank accounts using false ID.

   It would be simple for the UK Government to instruct the UK Passport Office and DVLA to provide an API to authorised UK banks only, whereby a passport/driving-licence number and name could be entered, and a Yes/No response could be returned back stating whether the passport/licence existed and was currently valid.

   Until such a step is carried out, false bank account opening in the UK will remain rampant.

   The banks and UK Finance (their trade body) should be strongly pushing for such a step – especially in the face of the new CRM reimbursement scheme.
In fact, OP1(1) of the code instructs that firms should act in a way to reduce APP Fraud, so all Firms should be taking active steps to call for this change.
The Government's reluctance to such a step (based on false security-service considerations) will quickly be overcome if Firms and industry bodies add their weight to this demand.
We ask you, the Authorised Push Payment Scams (APP) Steering Group, to add your name to such a demand to Government, as the scale of APP fraud demands such a response.

3) Code OP1 should have an additional item added before the third point (3), stating that the Code should also increase confidence in the Customer Journey and reduce customer error.
This is because a bank (or PSP) which subscribes to the code should use Confirmation of Payee to eliminate mistaken customer payment misdirection (where the customer mistakenly types in the wrong payee bank account number or sortcode) – this is not APP Fraud, but should be covered by the Code to ensure that such mistakes are eliminated.
At present, the code only allows for cases where the payer was intentionally deceived.
But in a case where there was no deception of the payer, but the payer makes an input mistake, the CRM should offer reimbursement to the payer if Confirmation of Payee was not offered correctly to the payer – and this is not currently captured by the Code, and needs to be.

4) We strongly believe that DS1(2)(a)(ii) has no place within the CRM.
It can never be a bank's (or PSP's) role to take on the burden of checking that the underlying transaction for which payment is being made is legitimate or not.
To do so will cause the UK payment infrastructure to seize up, as banks (and PSPs) become super cautious about whether any payment can take place.
To prevent bank (and PSP) liability, many genuine customers will not be allowed to access payment systems, and widespread disruption and damage to UK business will result as businesses and customers are 'derisked'.

We appreciate that payment analytics and transactional data analysis may sometimes help a bank in identifying customers and bank accounts used for fraud, but making the payer or payee's bank liable for loss in all situations involving Romance Scams or Investment Scams or Purchase Scams or Advance Fee Scams must be outside the scope of the CRM.

The needless chaos which will result if DS1(2)(a)(ii) remains within the draft code should be avoided by limiting the CRM to cases where the customer believes they are paying one party, but are tricked into paying another (cases dealt with under DS1(2)(a)(i)).

We fully appreciate that DS2(2)(b) excludes commercial disputes from the code, but there can never be a clear demarcation between service non-delivery and fraudulent delivery – and it cannot and must not be the bank's (or PSP's) responsibility to police this area.

A customer must retain full liability for making a payment to a known party – as in DS1(2)(a)(ii).

It may seem constructive and helpful to include DS1(2)(a)(ii) within the CRM, but it will have catastrophic effects on the UK, disrupt the UK economy, and lead to widespread disruption and loss.
This clause must be withdrawn.

5) The Best Practice Standards (BPS) mentioned in DS1(2)(b) do not seem to be publicly available, and were not included as an annex to the code – so it is impossible to comment on them, or take their details into account.
If possible, please supply for comment.

6) Code DS1(2)(e)(ii) mentions only Microenterprises.
The FCA and FOS are currently changing their rules so that both Microenterprises and SMEs will be covered by the FOS.
It will be confusing, inconsistent and possibly wrong for SMEs to be excluded from the CRM, but included for FOS participation. So DS1(2)(e)(ii) should be expanded to include SMEs in the same way the FCA and FOS are currently doing so.

7) The first sentence in SF should be amended from *'These provisions set out the standards that Firms should meet.'* to '*These provisions (including the General Expectations for Firms above) set out the standards that Firms should meet.'*

8) Code SF1 first and second sentences should add at the end '*and from customer payee-details entry error'*. See 3) above.

9) Code SF4(c) – If BSI PAS 17271 is referenced in the CRM, it should be publicly available without charge.
It is unacceptable for a consumer considering bringing a claim under the CRM to have to pay £75 (the current price) to discover what SBI PAS 17271 says, to understand whether the consumer will be protected and reimbursed by the CRM or not. If BSI PAS 17271 cannot be made available free of charge, an alternate but similar standard which can be freely obtained must be developed.

10) Code R1 – An additional sentence should be added stating: 'A customer should also be reimbursed if due to customer error the customer entered the wrong payee bank account number or sortcode, and Confirmation of Payee was not properly implemented.' See 3) above.

11) Code R2(1) – The wording currently states that if any of R2(1) (a) to (g) apply, then no reimbursement will be made if (a) to (g) would have had a 'material effect' on preventing the APP fraud.
A 'material effect' could mean that it would, say, make the APP fraud 20% less likely.

So under the current wording, even if a bank did not meet the code and would otherwise be liable, under R2(1) if it can show that any of (a) to (g) is present and would have lessened the chance of fraud even somewhat, then no liability will remain with the bank.

This does not seem fair.
Instead, where (a) to (g) are present and where the bank is also liable due to not elsewhere meeting the code, the reimbursement should be made, but at a reasonably reduced rate to take into account the customer failing of (a) to (g).
The wording of R2(1) needs to be changed to reflect this.

12) Code R2(1) & R2(2) – See answer to 1) above.

13) Code R(2)(3) – We strongly disagree that customers should be treated differently if they are regarded as vulnerable, and certainly if the bank (or PSP) could not easily identify them as such.
Whilst this is a noble sentiment, it means that a bank (or PSP) having a customer who is in any way vulnerable now faces unlimited liability, as the steps necessary to protect that vulnerable customer are ambiguous and unknown from the Code.
As such, it is no longer commercially worthwhile for banks (and PSPs) to service such customers, and categories of such customers will be targeted for account closure by means of favouring other customers with positive discrimination to vulnerable customer's exclusion.

There is an alternative. Charitable bodies should work with banks to categorise and identify certain types of vulnerable customers, and give precise guidance for the special care each category of vulnerability requires.
And such customers should then self-identify their category to banks (and PSPs) in advance, so those special measures can be applied before APP fraud takes place.

Otherwise, vulnerable customers will find themselves debanked through surreptitious means.

14) Consultation - Page 4 - Figure 1
We do not understand why a bank (or PSP) should be liable to a customer if the bank has met its obligations and levels of care, just because the customer also met their level of care.
In doing so, the CRM is creating an open-ended liability for banks for handling customers' payments, even where the bank acts properly and correctly and to best effect in every way.

No bank can function economically in this way – especially where the revenue from handling any one payment of a client is miniscule (in the realm of pennies).

To act in this way will mean that the UK payment system seizes up, and stops functioning, due to bank derisking, and other consequential steps. It will be catastrophic.
Where a bank (or PSP) has met its obligations and levels of care, it must have no liability under the CRM. This is necessary if the UK payment system is to continue to operate.

15) Core Principle 2 – Consistency of Outcomes
As this is the first opportunity presented to comment on the CRM's core and operating principles, I will take the opportunity to do so.

Almost nowhere else in law is there a concept of consistency of outcomes.
The members of the CRM are trying to rewrite English law to upturn the law of the land.
Whilst this may have good intentions, and produce fair and equitable outcomes for customers, the repercussions and costs of doing so would be so damaging that the net effect would be disastrous.

If a rich visitor comes into your home and negligently broke a very expensive vase, you would expect a different outcome from a similar case where a poor visitor came into your home and did exactly the same thing.
In the first case, full recompense is available to you, and in the second case, it is likely that no recompense will be available (as the visitor does not have the funds to reimburse).
So different outcomes for you for the same event.
Unfair outcomes are a fact of life, and necessary for a fair and well-functioning society.

Where tax and Government regulation can build protection for such cases to iron out unequal outcomes and protect the disadvantaged, it is good to do so. But the great cost of doing so will first need to be recognised, and costed for, and taxation laid to pay for such a measure.
In the case of the CRM, a new tax on the public is trying to be laid, to fund reimbursement of unequal outcomes, and without any consultation or preparation.
Not only is this not right, but this is a role for the Government to undertake through Parliament, and not via the CRM Steering Group.

Principle 2 of the CRM is admirable, but wrong and damaging, and needs to be rethought out.

16) Core Principle 4 – All PSPs
Core Principal 4 is not within the CRMs remit, and is plain wrong.

Whilst the CRM may well be appropriate for the big 5 banks, or even the largest eight banks (who transact by far most of the payments in the UK), as it is currently written the CRM cannot be appropriate for the vast majority of PSPs (who are by number the vast majority of PSPs).

This is because the Competition and Marketing Authority recognise that the large 5 banks have in effect semi-monopolistic powers and earnings in the UK, and can fund donations to the CRM out of their other activities.
And it may be appropriate for them to do so.

But the vast majority of PSPs earn only a revenue of a few pennies from each payment they handle – and this is their entire income stream.
The CRM, as currently written, creates an open liability of thousands of pounds from handling any one payment.
For example, handling a payment of £6,000 to fit a kitchen will result in a liability of £7,500 to a PSP once FOS costs are taken into account. That liability will exist to the PSP even if it pursues only best practice and correct actions. No PSP can exist in a market where any one transaction can earn it a few pennies but may costs it through no-fault thousands of pounds in reimbursement under the CRM.
This would be a totally anti-competitive step, and force the majority of PSPs out of business.

Further, not all PSPs are classical bank like organisations.
For example, our firm is Europe's leading escrow service, set up to prevent and protect against fraud.

And yet we are a PSP, as we conditionally remit payment. Applying the CRM as it is currently written to our PSP firm would actually prevent us from providing our anti-fraud escrow service.
And yet, Core Principal 4 as it is written would do just that.

So Core Principal 4 is totally wrong. PSPs must act to prevent APP scams – that is correct. But for all PSPs to apply the code would actually increase APP scams.
The code needs to recognise this, and Core Principal 4 must be rewritten to acknowledge that whilst it is appropriate to apply the code to the big 5 banks, and maybe some others, there are many PSPs and the Code as currently constituted is not suitable for them all (if, for example, it hampers PSPs who are effective in preventing fraud).

17) Core Principal 5 – No contingency on recovery of funds
See comments above on Core Principal 2 !

18) Paragraph 4.4 of the consultation document talks about consistent outcomes for firms, and the establishment of a working group to identify the source of funds for reimbursement in cases where no firm was at fault. It states that the working group will be co-chaired by an industry representative and a consumer representative.
This makes it seem that an industry representative can fairly represent the whole industry in taking this forward.
However, the industry is made of firms with very different experiences and situations, and what is good for one firm will be bad for another. In particular, what is appropriate for a large bank will be completely inappropriate for a SME PSP. The setting up of the working group with these two co-chairs is extremely naïve and wrong in this respect..

19) Paragraph 4.17 of the consultation document asks for comments on which body would be appropriate to govern the code.
One suggestion is the current steering group.
As the point above makes clear, the current steering group does not have representation from the large number of PSPs who are not large banks. So the make-up of the current steering group, made up of large banks and consumer organisations, can steer part of the liability of the CRM to other PSPs who are not represented. This is of course unacceptable.
We believe that the CRM is linked inextricably with the Financial Ombudsman Service (FOS), and the FOS should be the governing body of the code.

I am happy to provide any further explanation or clarification if required.

Best Regards,

Transpact.com

Creu Cymru oed gyfeillgar
Creating an age friendly Wales

15 November 2018

APP Scams Steering Group Consultation
c/o Payment Systems Regulator
12 Endeavour Square,
Stratford
London
E20 1JN

Dear Sir,

Age Cymru is the leading charity working to improve the lives of all older people in Wales. We believe older people should be able to lead healthy and fulfilled lives, have adequate income, access to high quality services and the opportunity to shape their own future. We seek to provide a strong voice for all older people in Wales and to raise awareness of the issues of importance to them. We work in partnership with colleagues in Age UK, Age Scotland and Age NI.

Ensuring that older people are protected from scams is a key area of work for us. It is vital because fraud or scams can destroy people's life savings, health and independence.

People of all ages and circumstances ages fall victim to various types of fraud and, in that sense, are vulnerable to fraud. However, older people are at higher risk of particular fraud types, e.g. pension and investment fraud, doorstep rogue traders, postal mass marketing fraud, romance fraud, courier fraud, impersonation scams and phone scams such as computer repair fraud. In some cases, this is because fraudsters deliberately target older people. Anecdotal evidence from Trading Standards services suggests doorstep rogue traders offering services such as building, gardening or energy efficiency services target older people living alone. Fraudsters used customer data following major data breaches to target older people with various phone scams.

At the same time, we do not consider that 'older' people are by definition vulnerable. Ageing, however, often brings circumstances and challenges that can make people vulnerable in the sense of being less able to protect themselves, e.g. cognitive impairment, health conditions, bereavement, loneliness and isolation. Indeed, we particularly want to highlight cognitive impairment, social isolation and loneliness (as well as previously being a victim) as key causes of vulnerability.

Llawr Isaf
Tŷ Mariners
Llys Trident
Heol East Moors
Caerdydd CF24 5TD

Ground Floor
Mariners House
Trident Court
East Moors Road
Cardiff CF24 5TD

ff/t 029 2043 1555
ff/f 029 2047 1418
e/e enquiries@agecymru.org.uk
www.agecymru.org.uk

FRSB FundRaising Standards Board

Creu Cymru oed gyfeillgar
Creating an age friendly Wales

We believe that banks have a unique and central role to play in protecting their customers from fraud. They can: educate and warn customers; spot and challenge suspicious payments and patterns; deny scammers access to a bank account and spot accounts being used by scammers; and support customers who become victims.

We believe that the banking industry has a reasonable level of protection and compensation in place for victims of fraud where the fraudster acts without the victim's involvement. However, we are increasingly concerned about fraud where fraudsters trick the victims into making a payment or giving out their personal or financial information.

We welcome the recognition in the consultation that

where a customer has met its requisite level of care, they should get their money back – one of the important principles of our work has been that customers in the same circumstances have consistent outcomes

However, we are uncomfortable with the suggestions at 4.6 that would lead to consumers funding the cost of reimbursement. We believe that the responsibility should lay with the organisations involved. They are by far in the best position to develop the mechanisms and protections to protect consumers from fraud or scams.

Yours sincerely

Llawr Isaf
Tŷ Mariners
Llys Trident
Heol East Moors
Caerdydd CF24 5TD

Ground Floor
Mariners House
Trident Court
East Moors Road
Cardiff CF24 5TD

ff/t 029 2043 1555
ff/f 029 2047 1418
e/e enquiries@agecymru.org.uk
www.agecymru.org.uk

Consultation

APP Scams Steering Group: Draft Contingent Reimbursement Model Code

November 2018 Ref:

Policy@ageuk.org.uk

Age UK
Tavis House
1-6 Tavistock Square
London WC1H 9NA
T 0800 169 80 80 **F** 020 3033 1000
E policy@ageuk.org.uk
www.ageuk.org.uk

Age UK is a charitable company limited by guarantee and registered in England (registered charity number 1128267 and registered company number 6825798). The registered address is Tavis House 1-6 Tavistock Square, London WC1H 9NA.

About Age UK

Age UK is a national charity that works with a network of partners, including Age Scotland, Age Cymru, Age NI and local Age UKs across England, to help everyone make the most of later life, whatever their circumstances.

In the UK, the Charity helps more than seven million older people each year by providing advice and support. It also researches and campaigns on the issues that matter most to older people. Its work focuses on ensuring that older people: have enough money; enjoy life and feel well; receive high quality health and care; are comfortable, safe and secure at home; and feel valued and able to participate.

About this consultation

This consultation asks for responses to a draft contingent reimbursement code (the **Code**) developed by a steering group of industry and consumer representatives. The aim of the steering group was to develop a contingent reimbursement model. The Code will be a voluntary code with the aims of reducing the occurrence of APP scams from happening in the first place, and lessening the impact these crimes have on consumers, microenterprises and small charities The steering group was established by the Payment Systems Regulator (**PSR**) following a consultation prompted by a super-complaint made by Which? about how firms dealt with authorised push payment fraud (**APP fraud).** An employee of Age UK has been a consumer representative member of the steering group. In this response we set out Age UK's views on the consultation. In this response we have used the words 'fraud' and 'scam' interchangeably. Where we use the capitalised word 'Firm' we refer to a payment service provider which has signed up to the Code.

Key points

- We warmly welcome the publication of the draft code and of this consultation and recognise its potential value in increasing consistency across the industry, securing protection for some of the most vulnerable victims of APP fraud and establishing a mechanism through which good practice can continue to be developed and shared.

- We are disappointed by the relatively modest standard of care required of Firms. Much of this reflects existing requirements or codes or are heavily qualified and on this level the draft code is a missed opportunity to raise standards.

- Some provisions of the Code fundamentally undermine the approach and must be either deleted or amended if the code is to be acceptable:

    - R2(1)(c) must be clarified to ensure that it is clear how it applies to authorised payments and that it does not inadvertently bring payments currently treated as unauthorised into the Code; and

- R2(1)(d) should be removed or amended so that it is clear that it only applies to purchase fraud. It should be further amended so that the exact steps a customer is expected to take are spelt out.

- We fully support the approach taken to describing and protecting vulnerable customers.

- It is essential that customers who have met their level of care are reimbursed.

- APP fraud must always involve either failures in account opening or mis-use of existing accounts in such a way that can never be the fault of the victim. It is therefore completely unacceptable that customers who have met the relevant level of care should be expected to fund reimbursement, whether through a charge on payments, insurance or other cost paid for directly by customers.

- Getting the governance arrangements right is vital for the longer-term success of the Code. We think that the Lending Standards Board, possibly working with Pay.UK, would be best placed to take on governance. Whichever organisation is responsible must:
  - Have adequate consumer, payments and fraud expertise
  - Be seen to be independent
  - Have experience of governing voluntary codes or similar

- There is a significant lack of research providing reliable evidence of how APP fraud works and how customers respond to both warnings and the frauds themselves. It will be important for the governance body or some other organisation to start to fill this gap so that the Code can continue to be developed in a way which places realistic expectations on customers and enables Firms and others to find more effective ways to help customers protect themselves.

- We understand that as this is a voluntary code the PSR cannot be involved in its governance but we would expect the PSR to be monitoring its effectiveness. If the Code is not meeting its objectives then we would expect that the PSR would put in place compulsory measures to reduce APP fraud and increase consumer protection.

Age UK Response

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

We had hoped to see clearer, higher standards for firms. We recognise the value in the current code as a starting point and also the need to bring standards up across the industry. Given the level of responsibility expected of Firms currently set out in the Code we would expect to see the standard raised as we learn more about what Firms are able

to do and see more good practice develop, especially as regards the receiving Firm. We return to this in the questions on governance.

The adequacy of the standard for firms will hinge on decisions around re-imbursement in a no blame/no blame scenario. If a consumer is reimbursed through Firm contributions in this situation then the exact standards on Firms are less critical for consumers – as Firms should in any case be incentivised to take steps to reduce APP fraud. If, however, consumers who have met their requisite level of care can still be left unprotected or are expected to fund no blame cases then it would be necessary to look at the standards for firms much more carefully.

Sending Firm – specific comments

SF1(1) (a) – It is unclear how good these analytics need to be. Also, how will it be determined whether it is 'appropriate' to incorporate the use of fraud data and typologies? As the Code is used more, detail on the standard of this analytics should be developed. It would be helpful for the Code to provide some signal to make clear that these should be of a high standard. Although we assume that most Firms will be working hard to improve their analytics we are aware of cases in the past that suggest more could be done e.g.

- In some cases, fraudsters gain access to a customer's account and move money between different accounts, making it look like money has 'appeared' from somewhere else, and then pressure the customer to 'repay' it. Firms' analytics and/or warnings must spot where this is happening (combined with other risk indicators) and ensure the customer is aware of potential fraudulent activity. This could alert the customer to suspicious behaviour and prevent them from making a payment.

- In other cases account names are changed to something like 'frozen' to persuade the customer to make a payment. Again, Firms should spot this and alert the customer to the fact. In both this case and the one above, if the customer has genuinely moved money or changed the account name they shouldn't mind being made aware of it but if they haven't, this could alert them to prevent fraud taking place.

- We are aware of cases where a customer has been persuaded into making multiple payments of unusually large amounts to a new payee they have set up very recently. Firms' analytics must capture this highly suspicious activity.

SF1(1)(b) – It should be made clear that Firms must train all relevant employees, not just fraud specialists, including frontline staff but also those staff who design other relevant systems and customer communications.

SF1(2) – This should apply 'Where Firms identify, *or ought reasonably have identified*, APP fraud risk….'. The current provision could inadvertently incentivise Firms NOT to identify an APP fraud risk. If this provision is not changed then it is even more important that SF1(1)(a) is clarified.

SF1(2)(b) - Should be amended to read 'where the Firm identifies, *or ought reasonably have identified*, an APP fraud risk.

SF1(2)(c) – Should be amended to read 'any specific APP fraud types identified, *or which should have reasonably been identified*'.

We strongly support much of the approach taken to defining an 'Effective Warning'. In particular we underline how important it is that warnings are intelligently designed to ensure that real world consumers can understand them. If a consumer is not capable of understanding the warning given then that consumer cannot be expected to 'protect themselves'. We understand that the shift towards increasing automation may create both challenges and opportunities in improving warnings. Challenges, because it may be easier for branch staff to tailor a message to an individual they can see and talk to, and who they may even know, than for a system to tailor a message to someone using online or mobile banking. Opportunities, because as Firms gather more and more data about their customers it may become easier to test and tailor different messages and to learn about what works.

It is vital that Firms are able to demonstrate how they know that their warnings are effective as defined in the Code. For some aspects of the definition this will require Firms to be able to demonstrate that the relevant customer could understand the warning and for other aspects it will require evidence of high quality testing of the impact of the warning more generally.

SF1(2) Prevention

Some bank impersonation frauds involve fraudsters phoning a victim and appearing legitimate in the phone's caller display or message trail. Some banks have introduced caller verification apps, which is a valuable development. However, given that some customers – including some older people or people with disabilities – are unable to use apps and others may not yet trust them, offering these services to customers who then do not use them should not be an excuse for Firms to discharge liability.

We are aware that there has been inconsistency and a lack of clarity regarding Firms' security instructions to customers. For example, Firms frequently advise customers to

verify contact details elsewhere before contacting them, and to never click links in an email yet we understand that Firms sometimes send emails or texts to customers that contain valid web links or contact details for customer to use. Similarly, while Firms often tell customers never to disclose their security credentials to a caller, Firms do make genuine calls to customers and ask customers to verify themselves by sharing *selected* security credentials. These messages and practices are inconsistent and insufficiently clear to customers.

If Firms improved their practices in this area, ideally on an industry-wide basis, then this could have a very significant impact on a customer's ability to protect themselves from impersonation frauds. This should be recognised somewhere in the Code. If it is not possible to include in the Code itself then perhaps it could be referenced in an annex as best practice, or otherwise recognised as an important factor in how the Firm's practices affect the customer' s ability to protect themselves.

SF1(4)(a) - Should be amended to read 'Firms should take *all reasonable* steps to identify customers….'
Firms should be required to take steps appropriate to their size and the nature of the business they conduct.

SF1(4)(b) – Should be amended to read 'Firms must implement *appropriate/all reasonable* measures and other tools….'
Firms should be required to take steps appropriate to their size and the nature of the business they conduct.

SF1(5) – Should be amended to read 'Where a Firm has, *or should have*, sufficient concern that a payment may be an APP fraud….'
There is a risk that the current wording provides an inadvertent incentive for firms not to develop concerns.

It would also be helpful to establish what might constitute 'sufficient concern'. We have heard firms express significantly differing views on what this might be. We have also heard firms speak of cases where they are 99% certain it is an APP fraud but still feel unable to do anything to delay or stop the payment. It would therefore be useful for the steering group or the PSR as appropriate to publish any work available on relevant laws and regulation. If current laws really do inhibit Firms' ability to protect customers then these should be reviewed. Although we recognise that this is beyond the scope of the steering group's work it would be helpful if somewhere in the response to this consultation it was stated how this will be taken forward.

Receiving Firm
Our response to this section depends on what is considered 'reasonable', as most of the steps required for the receiving Firm are qualified in this way. It is difficult for us to comment on this without a much greater understanding of how it is possible for a fraudster to gain access to the banking system.

However, we note that SF2 largely reflects existing law and regulation. As we assume that Firms are largely complying with these longstanding requirements and yet fraudsters still gain access to the banking system there is clearly more that needs to be done by receiving Firms to reduce fraud. Indeed, we are aware that there is a significant range of good practice within the industry that is not included in SF2.

Given that the receiving account is the lifeblood of APP fraud and that its existence must always involve either failures in account opening or mis-use of existing accounts in such a way that can never be the fault of the victim we see a strong argument to raise expectations of Firms in this area. We suggest that if it is not possible for SF2 to be significantly improved prior to publication of the final code then this should be a priority area for review by the governance body.

SF2(3) – Same comments as for SF1(1)(a) and (b).

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.
Whilst we understand the desire for a provision along these lines in order to assist in apportioning responsibility between Firms we are concerned that there may be some unintended consequences from the current position and wording of the provision.

"*The assessment of whether a Firm has met a standard or not should involve consideration of whether compliance with that standard would have had a material effect on preventing the APP fraud that took place."*

A prime objective of the Code is to provide an incentive for Firms to take steps to reduce APP fraud generally, as well as to protect individual customers. Therefore, Firms should be held to account for compliance with the standard whether or not the breach was considered to be material in the individual case.

As a minimum this should be re-drafted so that it operates as a potential exemption to re-imbursement not compliance. A Firm should only be treated as having met the standard if

they have taken the steps set out in the standard, not on the basis of hypothetical assumptions. This may be important in terms of governance and reporting and will also be important in terms of communication to customers.

We assume that, unless the case is taken to the Financial Ombudsman Service (**FOS**), the organisation making the assessment will be the Firm itself. This poses clear potential problems. If a Firm determines that it did not fully comply with the Code but that the non-compliance was not material then it should inform the customer of this decision, not that 'the Firm has met the required standard'.

The provision is very wide and yet the circumstances in which non-compliance of part of the standard could be immaterial to the success of the fraud seem limited. this provision should therefore be more narrowly drawn and clearer about the harm it is seeking to prevent.

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?
We are confused by this question as the provisions seem to operate by assuming that the Sending Firm has met its level of care. If it has not, then on our reading of the Code R2(1)(a) and (b) would not be relevant.

We would be concerned if this question implied a different interpretation of the Code. If there is an intention to include additional requirements on Customers who have not received Effective Warnings/received a clear negative Confirmation of Payee result compliant with SF1(3) or SF2(2) then these should be set out clearly as separate requirements. We cannot think of any additional requirements it would be appropriate to include here.

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

We agree that the steps set out are desirable but we disagree that it is reasonable to expect consumers to take all of them before they can be reimbursed. Some of the steps should be deleted or clarified. If the Code is to be fair it must be based on reliable evidence of what consumers can currently reasonably be expected to do to protect themselves, and of how people behave in the real world, not what Firms think consumers 'ought to do'. Behavioural theory tells us that it is unlikely that the Code itself will have a significant impact on how consumers behave when faced with a scam.

We fully support work to raise awareness and help consumers protect themselves - no one wants to be a victim of an APP fraud, even if they do get reimbursed at the end of the

experience. Older people can suffer severe, in some cases life-changing, financial and health impacts. There are cases of people losing their life savings, which they may not have time to rebuild if they have retired from work. Some people lose their home or go bankrupt as a result. Older people's physical health can deteriorate quickly after being a victim of crime, and they can suffer severe psychological health impacts such as stress and depression. They may also lose their independence as a result.

Even a Customer who would not usually be considered vulnerable may well fall for an APP fraud where sophisticated grooming or other well-developed techniques are employed by the fraudster, especially in scams such as impersonation scams. Despite the work of the Take Five campaign and other individual bank campaigns as well as other programmes including those run by charities such as Age UK, there are still many people who have very low awareness of scams and what they should do to protect themselves. Indeed it may be that even those of us who think we can look after ourselves haven't yet absorbed even the basic 'Take Five' messages:

> '80% of people surveyed say they could confidently identify a fraudulent approach. Yet, in a separate test of over 63,000 people only 9% who completed the Take Five Too Smart To Be Scammed? quiz scored full marks'[1].

This means that what we can reasonably expect a customer to do when they are faced with a scam is generally limited.

It may be helpful for the governance body to consider tracking consumer awareness of fraud and conducting research to understand how well consumers are able to protect themselves. This would need to include both an understanding of what consumers know about fraud prevention and also how well consumers are able to apply this knowledge when faced with realistic fraud scenarios.

The other side of this is that a simpler approach to the Customer standard would make it much easier to communicate with Customers and raise their ability to protect themselves from scams. There are multiple awareness raising campaigns aimed at individuals every year (not just scams but also health, other money, legal changes) and for messages to stick they need to ensure that Customers know exactly what to do next.

There are a number of provisions in the Code which are open to interpretation e.g. will a Customer be treated as having 'ignored' a warning if they didn't read it because they get so many messages from the Firm (and in other online journeys) that they assumed it was 'spam'. We know that consumers are always looking to 'click through' to the next stage.

[1] file://agepdcppro03.uk.age.local/vdi_profiles$/Phil.Mawhinney/Downloads/too-smart-to-be-scammed.pdf

Will a Customer have 'ignored' a warning if they read it, understood it but believed the fraudster in an impersonation scam rather than the bank's message? In the same provision and in respect of Confirmation of Payee, it is not completely clear what 'appropriate action in response to an Effective Warning' will be. It will be important that the governance process reviews how Firms are interpreting these provisions and whether this interpretation is consistent, both between Firms and most importantly with the spirit of the Code.

Based on the cases we see and have seen via other consumer groups and our understanding of risk compensation theory we do not think the Code is likely to mean that consumers take less care. We would be very interested to see examples of cases where Firms believe that the consumer should have done more and was too careless. The focus must be on understanding how consumers really behave when faced with fraud and how we can practically help protective behaviour. As discussed above this will require further research.

We have some concerns about the expectations placed on Confirmation of Payee as a fraud reduction tool. While it is sure to be useful, we understand that it was designed less to prevent fraud and more to help customers avoid inadvertent mistakes. The consequences of using it as a fraud prevention tool and of linking to it in this Code will need to be monitored. If consumers receive too many negative matches, even when they are sure that the payment is correctly addressed, it is likely that Confirmation of Payee related messages will cease to be impactful and it may not be reasonable to expect Customers to take additional action as a result of receiving them. Given that Confirmation of Payee is not yet available to Customers and we have yet to see how it will work in practice, we suggest that provisions related to it in the Code do not take effect until Confirmation of Payee is stable and evidence is available on how customers understand and use it. Depending on how Confirmation of Payee works in practice and how we see Customers responding, it may be appropriate for the governance body to review this provision before it becomes effective.

R2(1)(c) We question what place this provision has in a code which applies only to APP fraud rather than unauthorised payments made as a result of credential theft/sharing. This clause should be removed or amended.

This provision also makes us question whether the definition of 'authorised' is sufficiently clear. Surely a fraud in which the fraudster has gained access to an online banking site and moved money between customer accounts and then convinced the customer to transfer money to an account in another person's name is a consequence of unauthorised access to online banking. It would be helpful for this to be clarified. The Code overall must not result in any reduction of consumer protection i.e. frauds that are currently protected as unauthorised starting to be treated as authorised.

R2(1)(d) needs to be removed or clarified so that it does not apply to impersonation scams. The description of the intention of this provision in the consultation document does not match our reading of what the provision says in the context of the Code. If it remains as it is we are extremely concerned that it would completely undermine the relevance of the Code to impersonation fraud.

Even in relation to purchase fraud, it is not clear to us what it is reasonable to expect consumers to do in these circumstances. The test of 'reasonable steps' is much more onerous than the other provisions in the customer level of care and would therefore potentially undo much of the balance provided in R2(1). If R2(1)(d) remains it should specify exactly what constitutes reasonable steps as this is not clear to most customers or most customer representatives.

R2(1)(f) should be deleted. We completely agree that customers should behave in this way and also concur with the intention expressed in the consultation paper. However we do not see how this is relevant to the question of whether the customer should be treated as having met their standard of care or be reimbursed.

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 support the approach taken to customers vulnerable to APP fraud. In particular we agree that reimbursement must be assessed on a case by case basis and cannot be treated as a tick box exercise. Although the definition is different from the current FCA definition we agree that this is appropriate, because of the additional factor of the impact of the actions of the fraudster.

Given that a case by case approach necessarily requires more interpretation and therefore potential variance it will important to review how these provisions are being interpreted and we hope that as the Code progresses it will be possible to share additional best practice.

In discussions on vulnerability in other financial services policy questions we have heard firms express concern that extra protections for vulnerable consumers could reduce the incentives for firms to serve them at all. Firms have also in the past suggested that additional protections will mean that some customers will only be able to receive a 'dumbed down' version of a product or service in order to allow firms to manage the perceived risk of serving these clients. Whilst it is possible that firms could respond to the Code's approach to vulnerability in this way we think it is unlikely to occur because of the

universality of the need to access payments and the risk that not serving certain customer groups could breach equalities legislation. More positively we think that increasing understanding of vulnerability will, in conjunction with strong and clear requirements such as the Code provision, result in firms finding better ways to support vulnerable customers and so reduce risk and cost to all parties.

We recognise that this may be a difficult area for Firms and that identifying vulnerability is often challenging, however these are challenges that it is essential for Firms to meet. The question of how Firms treat those who are most in need of support and who are also those often most severely impacted by fraud will be a key litmus test for the success of the Code and one which Age UK will monitor carefully.

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

We do not support the timeframe currently set out. We understand why Firms might regard requests for help with APP Fraud as not falling within the definition of a complaint. However we think that the timelines should operate as if the Firm did receive the notification as a complaint. This is because (i) Customers should not receive different treatments just because they frame their calls in different ways; (ii) we see no compelling reason why an APP fraud case dealt with by a Firm under this code would need to go through a full and separate complaints procedure. If this is not changed it will make sense for all consumers to be advised to express their requests for help as complaints.

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. We strongly agree with this because the principles of consistency and fairness require that customers are reimbursed if they have met their requisite level of care.

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 should administer reimbursement but the question of when it is liable for or required to contribute to the cost of the refund should be dealt with separately. It should be the responsibility of the sending firm to recover any contribution to the cost of funding from the receiving bank or from such other fund as may be established to cover the cost. This approach is consistent with other banking law, such as credit card fraud.

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?

Customers should not be expected to directly pay for the cost of reimbursement. This would seriously limit the incentives on firms to reduce fraud. Reasons for this include:

- Firms are better placed than customers to spot and stop fraud and also to absorb the losses (e.g. through insurance)
- Ultimately the Firms are, by way of business, providing customers with an infrastructure which is fundamentally, if understandably in some cases, insecure
- The payments landscape is increasingly driving customers towards faster payments, increasing the likelihood that customers will be at risk of APP fraud

Customers receive protection in the card and direct debit space without additional cost direct to themselves and it would make no sense for them to have to pay when using faster payments. Whilst we understand that organisations other than payment firms have an impact on APP fraud we do not accept that this is a reason to leave customers unprotected or ultimately make customers pay.

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

Customers should be expected to cooperate with a Firm's enquiries to establish whether they are entitled to reimbursement but we note that the code currently places the requirement to demonstrate evidence on the Firm. We fully agree with this approach.

Q12 Do you 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 broadly agree with the issues set out in the consultation. In particular we think it is important that the evidential approach does not in any way seek to change the standards required by the back door. There are a number of provisions we have noted in our response where the standard itself is potentially ambiguous. We do not think that it would be appropriate for this to be addressed through evidential standards. If it is possible to provide clarification this should be done on the face of the Code.

We hope that the evidential approach will continue to be developed as the Code develops.

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

Respect and sensitivity during the information gathering and assessment phase will be vital in ensuring that evidence of vulnerability is collected in a way that does not create

further harm. Indeed, the way that information is gathered and checked may be as important as the information that is requested. We would expect Firms to use best practice developed in other areas, such as debt and credit to help develop best practice for the code.

Firms will at times need to proactively investigate whether a customer may be vulnerable (in the meaning given in the code) even if the customer has not explicitly stated that they think they are vulnerable. 'Vulnerable' is not a term many people would use to describe themselves, perhaps especially some of those most at risk. We know that many people who have been scammed blame themselves and feel stupid when reporting, even when no-one could have expected them to be able to spot the scam. In these circumstances they are often in a position to provide a list of reasons why they should get additional protection and the Firm will need to check for indicators in the way they would with other areas of vulnerability. For example, the Firm should take into account anything that it already knows about a customer's personal circumstances and the level of sophistication of the fraud in question; indeed even ignoring a warning that is usually very effective may indicate some level of vulnerability (e.g. arising from mental health problems).

There may be specific issues that need to be addressed if claims management firms or other similar businesses become active in this area, however we suggest this should be dealt with by regulation of these firms rather than through the vulnerability provisions of this Code.

Q15 Please provide views on which body would be appropriate to govern the code.
It is important that the body which governs the Code has both payments and consumer expertise and experience in code governance. It must also be independent and trusted as such. It is difficult to see a single body perfectly suited to the role. Whichever organisation takes on the code is likely to incur some costs in developing areas in which they currently have less resource. In particular, we would expect that the organisation which governs the Code will need to both take on additional consumer expertise and regularly commission research, some of which has been mentioned already in this response, to understand what it is reasonable to expect of consumers and keep track of how this may change over time.

We would suggest that currently the Lending Standards Board would be best placed to govern the code, but we also think that Pay.UK could have a useful role.

We envisage that Code governance must include more than just refreshing the Code. There must also be some function which checks how well Firms which have signed up to the code are complying with it. This is important because relatively few cases are likely to reach the FOS and because there must also be a mechanism for reporting on compliance

and ultimately requiring Firms to leave the Code if they have signed but not complied. Consumers should be able to choose to bank with Firms who have signed up to the Code and this advantage will be limited without effective governance.

Q16 Do you have any feedback on how changes to the code should be made?
We strongly agree with the suggestion that there should be a full review after a year and also that changes should be permitted on an ad hoc basis.

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?
The impacts of fraud can be shattering. Some older people lose their life savings, which they worked decades for and which were meant to provide for their retirement. Even relatively small losses can be devastating to the victim. In our polling, around 1 in 8 of those who lost money (13%) lost more than £1,000, while a quarter (23%) lost less than £100. In the case of older people in vulnerable circumstances, the impacts can go beyond money, affecting their physical and mental health too. This can even mean that someone who was living at home independently is no longer able to. On top of the personal harm caused, this increases demand on under-pressure public services like the NHS and social care. People defrauded in their own homes are 2.5 times more likely either to die or go into residential care within a year.[2] Any progress the Code makes towards reducing the incidence and impact of APP fraud is therefore extremely welcome.

We hope that the Code will also drive an increased understanding of how APP fraud operates and what can be done to help customers to protect themselves.

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 expect that Firms will also benefit from a reduced incidence of fraud. If the Code is introduced and implemented well then we would expect to see a significant increase in trust in Firms, particularly those that fully embrace it and provide notably improved protection for their customers. We expect that Firms may also benefit from development of the Effective Warning system to improve communications with their Customers in other areas.

Q23 How should the effectiveness of the code be measured?

[2] https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/safe-at-home/rb_mar18_applying_the_brakes.pdf

We expect that it will be necessary to use several measures of effectiveness which could include:

- Change in the amount of reported APP fraud
- APP fraud prevented (e.g. dropped payments following warning)
- Amount reimbursed to customers
- Number of cases in which Customers are reimbursed, broken down by fraud type
- Over time we would expect to see a decrease in the number of cases going to the Financial Ombudsman Service, but initially a rise may be a sign of success
- Case reviews showing consistent application of the code
- Case reviews show that expectations on customers are reasonable when applied to real life fraud and real life customers
- Evidence that customers know what they need to do to protect themselves from APP fraud

We note that these measures taken out of context could be misleading e.g. there could be an increase in APP fraud, however the Code could still be successful as it could have been less of an increase than we would have seen without the Code.

We understand that as this is a voluntary code the PSR cannot be involved in its governance but we would expect the PSR to be monitoring its effectiveness. If the Code is not meeting its objectives then we would expect that the PSR would put in place compulsory measures to reduce APP fraud and increase consumer protection.

Consultation Response to Authorised Push Payments (APP) Scams Steering Group Draft Contingent Reimbursement Model Code

15 November 2018

1. Introduction

1.1 The Consumer Council is a non-departmental public body established through the General Consumer Council (Northern Ireland) Order 1984. Our principal statutory duty is to promote and safeguard the interests of consumers in Northern Ireland.

1.2 The Consumer Council welcomes the opportunity to contribute to the Authorised Push Payments[1] Scams Steering Group Draft Contingent Reimbursement Model Code. (APPS/CRM). The Consumer Council believes it is uniquely placed to assist in the development of this code from a Northern Ireland consumer perspective. This is because of our daily interaction with consumers, alongside outreach, empowerment work and research which examines consumers' financial behaviours and trends.

1.3 It is of great importance to consumer well-being in Northern Ireland that regional differences are recognised by regulators and policy makers alike, whatever the subject matter. This sometimes means that UK wide approaches need to be tailored or completely rethought where necessary. This is because, as this response will show, Northern Ireland represents a very different consumer environment to comparable parts of the UK.

2. Background data on Northern Ireland

2.1 Northern Ireland wages are almost 10% lower than that of the UK, with average incomes of £21,254 and £23,474 respectively.[2] Alongside a lower level of income, Northern Ireland's level of vulnerable consumers has been placed at 56% opposed to 50% within the UK[3] with 21%[4] of the population being disabled or sufferers of a long term illness.

2.2 Research[5] commissioned by The Consumer Council shows that a third of all adults in Northern Ireland have been targeted by a scam of some kind in the past three years, with the young and old most likely to have been targeted (40% of 16-34s and 38% of 65+s). The most common method of targeting was via e-mail, followed by telephone and fake websites. One in seven of those targeted fell victim to the scam, with the young and middle-aged more likely to have fallen victim (19% of 16-34s and 22% of 35-50s); those with disabilities were also more likely to have fallen victim (23%).

---

[1] '*Push payments are payments where a customer instructs their bank to transfer money from. their account to someone else's account.*' https://www.psr.org.uk/sites/default/files/media/PDF/PSO-%20APP-scams-final-ToR.pdf

[2] The Consumer Council – Consumer Outlook Survey February 2018

[3] FCA Financial Lives: https://www.fca.org.uk/publication/research/financial-lives-consumers-across-uk.pdf

[4] The Consumer Council – Vulnerable Consumers 2017

[5] Consumer Insight Survey 2018 Summary Report http://www.consumercouncil.org.uk/sites/default/files/2018

2.3 Of all those targeted by a scam 14% became victims. Within this cohort, there are some groups who appear more likely to have fallen victim to a scam. These were consumers in socio economic groups C2DE (17%, n=127) and those residing in Derry City and Strabane District Council (38%, n=19).

2.4 Promoting and galvanising consumer rights has always been The Consumer Council's 'rasion d'etre'. Part of our role is also to educate consumers on their rights, and on how to get the best deals across various markets. Our complaints role focuses heavily on driving policy changes and delivering consumer redress. In the latest complaints report[6], £278,863 was returned to the pockets of consumers in Northern Ireland. Whilst campaigning strongly for consumer rights, we also feel it crucial that consumers take as much responsibility for their own decisions as possible.

2.5 Unfortunately there are factors such as vulnerability (whether fleeting or permanent), personal experience and expertise which may severely hamper some consumers' ability to:

- Stay safe when making financial decisions, and;
- Effectively protect themselves against financial scams.

It is within these vulnerable groups that payment providers hold a duty of care to ensure additional protective measures are in place.

3. Main body of response to questions

3.1 The following is our response to some of the questions posed in this review.
We have supplied evidence only where we have the necessary expertise and data upon which to rely. We therefore are unable to respond to any specific questions on base rates for instance as we consider this a matter for industry and regulators.

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

3.2 The Consumer Council welcomes the industry best practice guidelines set out for APP claim reporting standards, namely that:

Banks will have 24-hour, 7-day dedicated staff trained in scam management to deal with and process APP scam complaints.
The customer will only have to deal with their own bank/ account provider. The victim's bank will act as sole intermediary between the victim and the beneficiary bank.
Banks have agreed on a set of necessary information, to be collated by the victim's bank following APP scam complaints.

[6] http://www.consumercouncil.org.uk/sites/default/files/original/Complaints_Report_2016-17.pdf

The victim's bank will collate/provide this information to the beneficiary bank who will investigate the alleged scam.
The beneficiary bank will investigate, recovering funds where possible/ appropriate, and return funds to the victim.
Banks will collaborate more widely with each other on information to support investigations and protect victims.

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

3.3 Some may argue that the balance is already heavily weighted towards the banks and against the consumer. This is because banks often refuse to refund scammed customers on the basis that they made the payment voluntarily. In October 2015, the Royal Bank of Scotland group revealed that 70% of its customers who had fallen victim to a scam did not get a single penny back.[7]

3.4 The Consumer Council was contacted by a consumer who lost £77,000 when she mistakenly responded to a fake email purporting to be from her conveyancing solicitor. Despite attempts to recover the amount, including contacting the Financial Ombudsman she was ultimately unable to recoup the loss. She told the Belfast Telegraph:

'*I have just been sick ever since. Everyone is telling me my money is gone and no one is responsible but me.'*[8]

3.5 Consumers should not be penalised for being scammed. Whilst a basic level of care and attention can be reasonably expected from customers, providers should take other elements into account. A wide range of factors are often at play and a holistic approach will capture these and temper any response accordingly.

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

3.5 The recommendation of 15 business days seems fair in that providers may reasonably require due time to investigate any fraudulent activity. From the consumer perspective, of course, any length of wait at all will seem endless.

[7] BBC News October 2015- 'Most scam victims recover nothing, says RBS 'https://www.bbc.co.uk/news/business-34654400

[8] Belfast Telegraph article,17 November 2015 https://www.belfasttelegraph.co.uk/news/northern-ireland/mum-swindled-out-of-77000-in-house-sale-scam-finally-gets-a-new-home-but-her-worries-are-far-from-over-34206822.html

3.6 As in the example given of the consumer[9] mentioned earlier, the loss of such a vast sum impacted very dramatically on her life and that of her children. She was unable to proceed with a house purchase because the proceeds of her own house sale were stolen.
Timeliness is therefore of utmost importance and the sooner firms can come to a decision the better. That said, decisions should not be unduly rushed where many factors need to be reviewed and fairly considered.

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

3.7 As previously asserted The Consumer Council does not believe that consumers should be doubly penalised by providers, following a fraud by effectively being blamed for their own misfortune. If consumers can be seen to have acted in good faith and as the consultation paper says , they '*act prudently to protect their own interests*[10]' and taken all sensible protective steps to protect themselves, then natural justice dictates that reimbursement should be due.

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

3.8 In responding to any consultation, The Consumer Council considers to what degree the following consumer principles are met: Access, choice, safety, information, fairness, representation, redress and education. The aim behind these is to encourage education and to embed financial resilience. The Consumer Council therefore agrees that customers should have transparent systems in place when reporting a scam. Further we believe that the processes should be both fair and consistent in order to deliver the fairest outcomes.

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

3.9 According to the findings of our 2018 research, 14% of those targeted by a scam became a victim. Of those, there are some groups who appear more at risk - those more likely to have fallen victim to a scam were consumers in socio economic groups C2DE (17%, n=127) and those residing in Derry City and Strabane District Council (38%, n=19)[11].

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

3.10 The Consumer Council agrees that the code should be periodically reviewed as it develops. Furthermore, cases should be recorded to a standard and in a format that the FCA would normally require.
The effectiveness of the code could potentially be measured by customer Metrics/feedback. Anonymised case summaries could be produced, similar to those published by the Financial Ombudsman Service (FOS).

---

[9] Belfast Telegraph article,17 November 2015 https://www.belfasttelegraph.co.uk/news/northern-ireland/mum-swindled-out-of-77000-in-house-sale-scam-finally-gets-a-new-home-but-her-worries-are-far-from-over-34206822.html

[10] https://appcrmsteeringgroup.uk/wp-content/uploads/2018/09/APP-scams-Steering-Group-CRM-Consultation-paper-FINAL.pdf

[11] Note that the sample size for the sub groups is <100 in some cases. This means the findings in the sub groups are indicative only and should be used with caution.

4. Other issues

4.1 Cross Border payments

The Consumer Council notes that this code does not relate to international payments or payments in other currencies. We are curious to know if the Steering group (or other body) will be giving any thought to how to protect consumers in Northern Ireland who may fall victim to scams in cross border payments or in euros.

4.2 Small to Medium sized Enterprises (SMEs)

The Consumer Council agrees with Open Banking's customer experience guidelines in that:

'Security is vital for both consumers and SMEs, but it is especially critical for SMEs, due to the nature and scale of the transactions involved. SMEs are more likely to be making more payments of higher value, and their businesses may depend on these being made securely. There may also be reputation considerations involved. '[12]

4.3 The need to protect SMEs was recently bolstered when the Financial Conduct Authority (FCA) confirmed its plans to extend access to the Financial Ombudsman Service (FOS) to SMEs.[13]Many of our consumer contacts in Northern Ireland are small businesses and hence it is important that the risks to this group are fully considered whilst developing the code on push payment scams.

5. Conclusion

5.1 With the growth of Faster Payments,[14]allowing transactions to clear in under two hours, thousands can be moved with a few taps of a keyboard. The worrying aspect especially for less savvy consumers is that safeguards have not always kept pace with evolving technology.

5.2 Despite the risks faced by consumers, an investigation by Which? found that between April 2015 and February 2017, Barclays wrongly rejected 36% of customers who disputed transactions on their accounts.

Santander wrongly denied 33% of customers' compensation; Nationwide, RBS and NatWest refused to reimburse almost a third of customers who were victims of fraud. The Financial

[12] Open Banking Customer Experience Guidelines https://www.openbanking.org.uk/wp-content/uploads/Customer-Experience-Guidelines-V1-01.pdf
[13] ESAN Newsletter- October 2018
[14] Faster Payments; How faster payments works http://www.fasterpayments.org.uk/how-faster-payments-works

Ombudsman Service later decided all of these decisions were unfair and ruled in favour of all four banks compensating their customers.[15]

5.3 Northern Ireland consumers lack confidence and are somewhat '*downbeat*' about financial capability according to the FCA report 'Financial Lives'.[16] Given the national higher vulnerability ratings [16]coupled with lower levels of financial capability within Northern Ireland the Consumer Council believes that the following statement from Which? best sums up our position:

"It's simply unacceptable that in cases where banks claim they could not have done anything more, it will still be the victim who is left to bear the cost - often with devastating consequences."[17]

5.4 Thank you for giving us the opportunity to respond to this call for evidence. The Consumer Council consents to this response being reproduced in its entirity by the Steering Group. [✂]

Yours sincerely

[✂]

[15] The Telegraph: '*How does your bank score when dealing with fraud?*' May 2017 https://www.telegraph.co.uk/personal-banking/savings/does-bank-score-dealing-fraud/

[16] FCA Financial Lives: https://www.fca.org.uk/publication/research/financial-lives-consumers-across-uk.pdf

[16] FCA Financial Lives: https://www.fca.org.uk/publication/research/financial-lives-consumers-across-uk.pdf

[17] BBC Business -28 September 2018 '*Refund hopes rise for push payment scam victims*' Refund hopes rise for push payment scam victims https://www.bbc.co.uk/news/business-45664980

Floor 3
Seatem House
28-32 Alfred Street
Belfast
BT2 8EN

Freephone:	0800 121 6022
Switchboard:	028 9025 1600
Fax:	028 9025 1663
E-mail:	info@consumercouncil.org.uk
Website:	www.consumercouncil.org.uk

Financial Services Consumer Panel
AN INDEPENDENT VOICE FOR CONSUMERS OF FINANCIAL SERVICES

Telephone: 020 7066 9346
Email: enquiries@fs-cp.org.uk

APP Scams Steering Group Consultation
c/o Payments Systems Regulator
12 Endeavour Square
Stratford
London E20 1JN

13 November 2018

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

Dear Sir / Madam

Financial Services Consumer Panel response to the APP Scams Steering Group Draft Contingent Reimbursement Model Code Consultation Paper

The Financial Services Consumer Panel is an independent statutory body. We represent the interests of individual and small business consumers in the development of policy and regulation of financial services in the UK.

The Panel welcomes the opportunity to respond to the APP Scams Steering Group Draft Contingent Reimbursement Model Code Consultation Paper. Our main points are:

- Everyone is vulnerable to fraud, as the consultation paper makes clear. Although some people have more capacity to protect themselves than others, a division of customers into vulnerable and non-vulnerable will not work in practice. The Code should make clear that everyone is vulnerable and all customers should receive protection.
- The Code should explicitly address the risk of APP fraud to SMEs, and confirm that it applies to SMEs.
- There should be a presumption that the receiving bank is at fault where there has been an APP scam.
- Consumers should be reimbursed if they are victims of an APP fraud unless they have been grossly negligent. This is the standard applied to card payments and it should apply to faster payments as well.

The Panel's responses to the questions posed in the consultation document are set out below.

Yours faithfully,

Financial Services Consumer Panel

ANSWERS TO CONSULTATION QUESTIONS

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

To stop scams, or allow money to be returned to consumers more easily, information needs to flow as quickly as money. The technology exists to enable this, but the current legal and regulatory framework does not permit it. This needs to be carefully considered, and may require intervention from Government to bring it about.

The Panel's comments on the standards are divided between those which apply to 'sending' firms and 'receiving' firms.

For 'sending' firms:

The standards for 'sending' firms look broadly acceptable. However, the Panel has four reservations:

1. All consumers are vulnerable to APP scams. Attempting to identify consumers who are likely to be particularly vulnerable does not make sense.
2. SMEs are also at risk and the Code is silent here. This is a gap which should be addressed.
3. The 'sending' firm is only required to notify the receiving bank if it is a UK bank. While the Code does not cover the actions of a receiving bank in another country, we understand that such contact can result in voluntary and prompt action. The 'sending' firm should be required to notify the receiving bank wherever they are so consumers making international payments receive effective warnings and prompt responses if they have fallen victim to scams.
4. Sending banks should offer customers a 24-hour delay for all payments. Where Payment Service Providers (PSPs) warn customers about an APP scam risk, they should remind them that card payments offer significantly more protection, particularly in relation to chargeback.

For 'receiving' firms:

There should be a presumption that the receiving bank is at fault where there has been an APP scam.

The receiving bank has facilitated a financial crime by allowing the fraudster to open an account, or by failing to detect that an account is being used as a money mule account. Under the present system, the receiving bank has no incentive to detect fraudulent payments as they bear no risk. Under the proposed Code the receiving bank has to take 'reasonable steps' to prevent and respond to APP fraud. This is not clear enough. If the receiving bank fails to detect and prevent fraud, it should be liable for losses suffered by the sending customer. Only then will firms have sufficient incentive to put in place robust fraud prevention systems

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 find it difficult to envisage circumstances where this might apply.

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.

The Panel is unable to envisage situations in which these provisions would apply. If the sending bank and receiving bank have both failed, then whatever happens the customer can't be held liable under R2 (1) (a) and (b) and should receive reimbursement. Where all parties have not met their level of care we would expect the provisions of R2 (2) to apply and firms to reimburse consumers as their acts or omissions have "impeded the Customer's ability to avoid falling victim to the APP fraud".

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

Customers should take reasonable care, but are entitled to expect that the bank will have systems and processes in place to protect them, and to help them recover their funds. We believe that all consumers should be reimbursed unless they have been grossly negligent (i.e. R2 (1)(g) only). This is the standard applied to card payments and we believe it should apply to push payments as well. The other standards should not be assumed to define 'gross negligence'. Gross negligence involves conscious and intentional disregard or care. Ignoring a negative Confirmation of Payee (CoP) response (perhaps because CoP is not sufficiently reliable) may be rational and cannot constitute 'gross negligence'.

Consumers are entitled under PSD2 to share their credentials with authorised third parties. R2 (1)(c) is therefore not relevant to authorised push payment fraud but unauthorised push payment fraud. It should be removed.

There is insufficient detail for R2 (1) (d): "Failing to take reasonable steps to satisfy themselves that a payee was the person the Customer was expecting to pay". It is not clear what exact steps customers are supposed to take beyond using the Confirmation of Payee system once it is operational. If the Code cannot provide absolute clarity on this point (e.g. consumers should speak with the recipient in person to confirm the account details and sort Code in advance of making the payment), then R2 (1) (d) should be removed.

We recommend removing R2 (1) (f) from the Code altogether. Where consumers are coached by fraudsters to 'lie' to their bank, they are caught in the scam and cannot therefore be judged against the provisions in the Code. Consumers who are actively involved in fraud are not covered by the Code in any case.

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?

The consultation document states that all consumers are vulnerable to APP scams. We agree. However, the Code should also make this clear. Identifying consumers who are likely to be particularly vulnerable does not make sense. A momentary distraction like a child crying, problems at work, or a short-term illness all make people particularly vulnerable to APP scams. It is not possible to codify and anticipate these events. This section of the Code, as currently drafted, is not workable in practice. The approach should be to assume that everyone is vulnerable, and protect them accordingly.

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

Yes. However, consumers should be able to go to the Financial Ombudsman Service (FOS) immediately if they are unhappy with the reimbursement decision. Firms should

not be able to delay reimbursement or consumers' access to FOS. The easiest way to accomplish this is for the FCA to define a report of an APP scam as a complaint and to turn on the complaints forwarding rules for all complaints about APP scams so that the sending bank has to pass on the complaint to the receiving bank.

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?

Better transaction analytics are likely to be forthcoming if the banks, rather than customers, bear the risk of APP fraud. Banks are more likely to develop analytics to protect themselves than they are to protect their customers.

Confirmation of Payee only provides partial protection, especially where a fraudster sets up an account in a name resembling that of the intended payee. For example, if the payer intends to pay Norman Archer and the fraudster sets up an account in the name of NM Archer, Confirmation of Payee will not return "no match". In addition, Confirmation of Payee which relies on checking firms' names with Companies House does not provide adequate protection since the process for registering a company is simple, and liable to be abused by those perpetrating scams.

Banks should offer all customers payment deferral, not just those they identify as vulnerable. This would be much simpler to administer and at least one High Street bank already does it, so it is technically possible.

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. We believe they should be reimbursed unless they have been grossly negligent, to bring the protection offered by push payments into line with cards.

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?

The sending firm has the relationship with the sending customer and it therefore makes sense for them to administer the reimbursement. As we have said above, we think the presumption should be that the receiving bank is liable unless the sending bank has failed to meet the Code's standard of care.

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 are strongly opposed to an insurance fund or government sponsored fund. This would create a moral hazard, and sharply reduce the incentive for banks to develop systems to protect themselves and their customers from fraudsters.

Under card scheme rules the cardholder's bank is responsible for reimbursing the customer in the event of fraud. Banks do this as part of the cost of scheme membership because they make money from every card transaction.

Faster Payments are free to individual consumers, although SMEs usually have to pay. Banks do not therefore see them as a revenue stream, but as a cost. In reality, Faster Payments enable banks to cut their operating costs by getting the consumer to do the work rather than bank staff, and by reducing the need for branches to handle payments. Banks prefer that consumers use Faster Payments than write cheques or make transactions in cash. They do not offer alternatives to consumers wishing to make

payments directly from their bank (for instance a slower type of payment). The banks themselves benefit from this. It is therefore in the banks' interest to maintain trust in Faster Payments (and Chaps), as they do with cards.

It would be possible to charge individual customers for making push payments. As lower value payments (say less than £5,000) are rarely attractive to fraudsters the charge could be levied only on payments above the threshold. Consumers already pay for larger payments via CHAPS. Incentivising banks by associating Faster Payments with a revenue stream would help to promote usage, and therefore trust.

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

As we have said above, we believe customers should be reimbursed unless they have been grossly negligent, as with cards. The card schemes have a lot of experience of defining what is and what is not gross negligence.

Q12 Do you 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?

Yes. We have no recommendations for other issues.

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

Everyone is vulnerable to fraud. Some people will – in that moment – have more capacity to protect themselves than others. As we have said above, it is not possibly to codify and anticipate who will be vulnerable at the point at which they are scammed. A division of customers into vulnerable and non-vulnerable categories will not work in practice.

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

Pay.UK (formerly the New Payment System Operator) is the obvious body to govern the Code. It is the analogous body to card schemes and should be responsible for taking the lead in ensuring that the payments systems it runs are trustworthy.

The body responsible for governing the Code must have the resources, powers and responsibility to collate or gather data on APP scams, conduct compliance assessments and to share best practice. It should also maintain a register of firms which have signed up to the Code. The governing body would need to have a memorandum of understanding with the FOS and receive all of the FOS decisions made about firms with regard to APP scams and compliance with the Code. We would also expect the FOS to draw the governing body's attention to any systemic issues about how firms were complying with the Code. The governing body should also have the power to name firms which are failing to comply with the Code.

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

Pay.UK should lead and work jointly with consumer groups and UK Finance, with input from the Payment Systems Regulator. These bodies should consult regularly with consumer bodies to discuss the Code's effectiveness or changes and improvements.

The Code also needs proper oversight, monitoring and enforcement. Pay.UK could usefully learn from the Lending Standards Board, or commission their support for auditing individual firm's compliance with the Code.

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

As we have said above, the receiving bank should be presumed to be at fault unless the sending bank has contributed.

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?

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

Consumers affected by APP scams need a clear and simple means of registering a complaint, and they should have to do this only once. Under no circumstances should the consumer have to make separate complaints to both the sending and receiving banks. This would add unnecessary duplication and complexity, and raise the prospect that a consumer seeking redress will be passed back and forth between banks, with neither taking overall responsibility.

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

No comment.

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?

The biggest benefit is that more victims should get their money back.

We anticipate that consumers with less formal means of proving their identity will struggle to open bank accounts, exacerbating financial exclusion. There might also be more forced account closures.

Some consumers may also become irritated or frustrated at the imposition of more friction into payments.

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?

There might be some payment delays (e.g. to solicitors) and processes will need to be adjusted to take account of these.

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

As we state in our answer to Q20, the Code may increase levels of financial exclusion, since consumers with less formal identification documents may struggle to open bank accounts.

Q23 How should the effectiveness of the Code be measured?

Key measures to determine the effectiveness of the Code should be the reduction in the number of APP scams and reduction in the level of losses incurred.

Code signatories should be required to report key statistics to the governance body on a regular basis. The governance body should be responsible for monitoring firms' adherence to the Code, and be able to 'name and shame' firms that do not adhere to the Code. Otherwise, the Code will be of little use, other than to provide some guidance on acceptable practice to the FOS. In cases where consumers do not complain or take their concerns to the FOS, they will be worse off.

15 November 2018

Contingent Reimbursement Model Consultation Response

Victim Support is the leading charity supporting victims of crime in England and Wales. In 2017/18 more than 38,000 victims of fraud were referred to our sevices for information and help.

We welcome a code that seeks to reduce the likelihood of people becoming victims of authorised push payment fraud, and to reimburse them if they do fall victim

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

Yes. However SF 1 (1) requires further explanation of of what 'identifying Customers [at risk]' means, as the focus on SF1 (1) (a) and (b) is on analytics and transactions, rather than on knowing and understanding their customers

SF 1 (2) (e) (iii) Impactful should be a measurable outcome. If a firm is to rely on its claim that its warnings are effective in a given situation in order to not reimburse a customer, then it is our view that this requires a demonstrable evidence base on which to stand.

SF 1 (2) (e) (v) should be tailored not only to the customer 'type' but to the individual customer, where the firm holds information that a customer has specific needs or characteristics.

SF 1 (5) We welcome the intention to delay a payment to investigate prospective fraud. Fraud victims tell us that they have realised shortly after a transaction that they were being scammed, and so would benefit from a reflective period where fraud is suspected

SF 2 (3) (b) Firms should also train their employees on understanding and identifying vulnerability amongst their customers and how scams are perpetrated, with the implication that if firms have not done so then they may be liable to reimburse

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

Yes it might have negative unintended consequences for customer reimbursement. The purpose of the code surely is to set standards that firms must meet in order to prevent, detect and reimburse customers. If they do not meet the standards and a

customer is defrauded, then the firm should reimburse the customer. Incentivisation of of firms to reduce then occurrence of fraud is one of the Overarching Provisions

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.

Our view is that, if the firm has not met its standard of care and a customer has been defrauded, then the firm should reimburse.

We know from the fraud victims we support that scammers use sophisticated techniques to engage the confidence of customers (eg by pretending to be from banks, broadband providers or the police) and so scammers will try to convince customers to ignore warnings. The issue therefore of a warning that a customer ignores should not necessarily mean that a customer should not be reimbursed

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

Yes, however we suggest that gross negligence on the part of the customer should be the overarching test for whether a customer gets reimbursed, rather than it being only one consideration out of many.

As discussed in our response to Q3 above, a customer failure to take a particular step (eg by ignoring an Effective Warning) should not necessarily prohibit them from being reimbursed, as consideration of the recklessness of this needs to be evaluated within the constext of the specific scam.

Also we know that people may be subject to coercion or control within their intimate relationships, and so where a customer appears to have been reckless within the terms of R2 (1) (c) then examination of this must take place and a decision made on the specific circumstances of each case

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?

Yes, this is a sound approach. Vulnerability is not necessarily a fixed or readily identifiable characteristic and so this approach directs firms to examine the ability of that particular customer to protect themselves, at that time, from that particular fraud.

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

15 business days seems ample for an investigation and decision. 35 business days seems excessive, and places the customer at a significant disadvantage when (as is common in fraud investigation) bank and other accounts are frozen and customer access to funds is limited

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?

Consumer education and awareness: significantly more than these measures can done to develop customer awareness. E-learning can be directed to individual online

banking accounts, whether for new customers or existing, to demonstrate the range of scams and how to avoid them. Tailored messages and news bulletins which would allow firms to communicate details of up-to-date scams to their customers, as they emerge

We know from our work that many scams go unreported to firms or the police. There is scope for firms to identify independent, confidential sources to their customers so that people can seek support if they have been scammed.

Also where custsomers do report fraud, as part of their customer care package firms should be ensuring that each customer is either signposted or referred to appropriate sources of support, to help people get over the immediate aftermath of the scam but also to build personal resilience and vigilance so that repeat scams are less likely in the 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?

Yes, surely that is the purpose of the code. If the customer has done all that is required of them, but the firm has allowed the loss of their funds, why would the customer have to bear the cost of this?

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?

It is our view that the sending firm should reimburse at the earliest opportunity to minimise customer distress and inconvenience. The sending and receiving firm can then agree on liability between themselves.

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?

It is our view that customers should not bear the cost of reimbursement through transaction fees, insurance or other charges.

Firms should instead contribute from their profits a levy to a central scheme which can reimburse fraud victims in the 'no blame' scenario, whilst firms reimburse directly where they (senders or receivers) have not met the requisite standards of care or where there is a 'shared blame' scenario

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?

It will be a positive outcome for customers to be reimbursed quickly and without contention where they have been scammed but it was through no fault of theirs.

It will also be a positive outcome for customers to be reimbursed where the firm is at fault, or where there is shared responsibility.

It will be a positive outcome for customers to be treated fairly and with consistency by firms, and for there to be common guidance for customers on the circumstances under which the may or may not be reimbursed

It wil be a positive outcome for customers to have a pathway to the Financial Ombudsman Service in the event of dissatisfaction with a firm

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

The code should be explicit on the requirement to evaluate not just the level of care deonstrated by the customer but also the standard of care demonstrated by the firm **in every case.** Otherwise firms may simply examine the behaviour of the customer, and then decide against reimbursement the basis of that alone, without examining their own standards of care and whether they have met the required standards for firms

Which?, 2 Marylebone Road, London, NW1 4DF
Date: 15 November 2018
Response to: APP Scams Steering Group Draft contingent reimbursement model code

Consultation Response

Authorised Push Payment Scams Steering Group consultation: Draft contingent reimbursement model code

Summary

- Which? broadly agrees with the Authorised Push Payment (APP) Scams Steering Group's draft contingent reimbursement model code. The draft code is a step towards a system that is fairer to victims of APP scams and it will provide some incentives for those best placed to reduce APP scams to do so, two key aims of Which?'s 2016 super-complaint[1] on this issue.

- We strongly support the principle that all victims meeting their requisite level of care should be reimbursed, regardless of the actions of the sending and receiving payment service providers.[2] We also agree with the requirements on both sending and receiving firms to identify and mitigate the risk of scams, and for sending firms to administer any reimbursement to the victim. However, the code should set out that any report of an APP scam should be treated as a complaint by both the sending and receiving firms.

- The steering group now needs to urgently agree how to fund the reimbursement of victims in 'no blame' cases, where the victim has met the required standard and both the sending and receiving firms have met their obligations under the code, and who will govern the code once it is in force. Choosing the right governance body is fundamentally important for ensuring that all firms involved in push payments sign up to the voluntary code and adhere to it, and for ensuring that the code, and any associated rules, keep pace with how scams evolve.

- Victims in no blame cases should be reimbursed from a central fund that is collectively funded by a transaction charge on sending firms using Faster Payments. Of the seven options proposed by the steering group, a transaction charge, if levied on firms rather than consumers, is one of only two options that could incentivise firms involved in push payments to individually and collectively reduce the risk of APP scams, above and beyond the minimum requirements set out in the code. We are concerned that the other option, a wider contribution mechanism covering firms beyond payment service providers, will be difficult to define and agree in time for the launch of the code in early 2019.

[1] Which? (2016), *Which? super-complaint: Consumer safeguards in the market for push payments*
[2] We use the terms 'sending firms' and 'receiving firms' throughout the rest of this submission in place of 'sending payment service providers' and 'receiving payment service providers'

- We propose that the transaction charge should be paid by the sending firm to the Faster Payments scheme, since it is the sending firm that chooses to use Faster Payments, and its customers benefit from any protections against scams offered by Faster Payments. The Faster Payments scheme should then use this funding to offer a new protection guarantee for customers similar to the Direct Debit Guarantee.

- If a funding mechanism for no blame cases is not ready in time for the launch of the code in early 2019, then the sending firm involved in each case should reimburse the victim.

- The contingent reimbursement model code should be governed by Pay.UK. Unlike other payment schemes, Pay.UK's Faster Payments scheme lacks rules or policies related to consumer protection against fraud. Pay.UK should perform a number of functions, including translating the key principles and requirements of the code into its scheme rules for Faster Payments, which all firms that use the scheme must follow.

Which? broadly agrees with the draft contingent reimbursement model code

Which? welcomes the opportunity to respond to the APP Scams Steering Group's consultation on the draft contingent reimbursement model code. We welcome the work that the Payment Systems Regulator and industry have done since our super-complaint in September 2016 to improve the detection, prevention, and response to APP scams. The contingent reimbursement model draft code is another step towards a fairer and more effective system.

One of the consumer representatives on the steering group is a Which? employee. Here we set out Which?'s views on the draft code.

The current system leaves victims facing losses of potentially life-changing amounts of money to fraudsters whose methods are constantly evolving. Whether a victim is reimbursed after a scam is dependent on the goodwill of their bank, or the success of attempts at repatriation, so most victims are not reimbursed unless the sending and/or receiving firm decides it is at fault. Of the £92.9m lost by consumers from 31,510 cases of APP fraud in the first half of 2018, just £15.4m (16.6%) was returned to consumers.[3]

Which? strongly agrees with the two main aims of the draft code: to reduce the occurrence of APP scams, and to reduce the impact of these crimes. These two aims were at the heart of Which?'s 2016 super-complaint on this issue. The code should be judged principally by how well it achieves both of these aims.

Consumers have important roles to play in preventing APP scams. We support the principles in the code that consumers meeting a requisite level of care should be reimbursed, regardless of the actions of the sending and receiving firms, and that consumers who are vulnerable to APP

[3] UK Finance (2018), *2018 half year fraud update*, p.19

scams should not be held to the same level of care as other consumers. We also support the code's approach to the requisite level of care for consumers, including the requirements for consumers to be open and honest in their dealings with firms.

Which? agrees with the principle that the code should provide incentives for those with the ability to prevent APP scams to do so. Consumers already have extremely strong incentives to avoid being scammed, as they stand to lose significant, sometimes life-changing sums of money, as well as potentially experiencing distress, fear and embarrassment. However the firms involved in making push payments currently lack the financial incentives to reduce APP scams.

This is unlike other payment methods, whereby firms have arrangements for appropriately allocating between themselves the liability for losses due to fraud. Sending and receiving firms, and the operators of the payment schemes, therefore have strong financial incentives to develop effective systems and approaches for reducing the risk of other types of fraud, and have introduced a range of protections and policies.

The code therefore rightly sets out a range of requirements on both the sending and receiving firms. If either firm does not meet these standards, and the consumer has met their requisite level of care, then the firm/s will be required to reimburse the victim. This will therefore provide financial incentives on firms to meet these industry standards. Crucially the code makes clear that both the sending and receiving firms have a responsibility to identify and mitigate the risks of scams, above and beyond administering the payment. We particularly support the requirements on sending firms to:

- provide effective warnings to their customers, which should be understandable, clear, impactful, timely and specific;
- intervene on a risk-based approach to delay execution of a payment authorisation; and
- provide a greater level of protection for customers who are considered vulnerable to APP fraud.

Equally, the code makes clear that receiving firms have a responsibility to mitigate the risks of APP scams, since fraudsters directly, or indirectly, use accounts with them. We therefore strongly support the requirements on receiving firms, including to:

- screen customer accounts to identify accounts at higher risk of being used by criminals;
- use transactional data and customer behaviour analytics to identify payments that are at higher risk of being an APP fraud; and
- train their employees on how to identify indicators of circumstances around, and leading to, transactions that are at higher risk of facilitating APP fraud.

We also support requirements for both the sending and receiving firms to introduce Confirmation of Payee. This measure is urgently required to tackle APP scams, and it is disappointing that voluntary action to introduce Confirmation of Payee has not resulted in swifter implementation. Payments made via Faster Payments are currently processed without checking whether the account name matches the account number. Confirmation of Payee will verify the name of the company or individual connected to that account before any money is

transferred. If this provides consumers with clear and reliable information and warnings, this measure could be particularly effective at tackling redirection scams, where the victim thinks they are paying a legitimate payee but are tricked into paying a malicious payee. Consumers lost £43.7m to these scams in the first half of 2018.[4]

While we support the key principles and requirements in the code, whether the code meets its stated aims will depend on how the code is put into practice by signatories to the code, and how they are held to account. Crucially, the code should not place unrealistic expectations on victims. Firms should be required to show clear evidence that their warnings are effective, both that their systems are designed to be effective for different groups of consumers and that these warnings were effective in individual cases. If they are unable to evidence this, then consumers who have met their requisite level of care should be reimbursed.

The code needs to be updated to keep pace with fraudsters' rapidly evolving methods. There is a risk that many firms will be able to meet the proposed minimum standards, particularly those that relate to their general systems and processes, but that the number and value of APP scams will continue to rise. A strong governance body is required that has the ability to introduce new measures to combat scams that are adopted across the sector. Furthermore, the steering group needs to agree a funding mechanism for no blame cases that provides a financial incentive on firms to work individually and collectively to go above and beyond the code. We set out our proposals below on why Pay.UK, the operator of Faster Payments, should be the governance body, and for Pay.UK to introduce a transaction charge on its member firms to fund no blame cases.

The code should also lead to a system that is not onerous for consumers to report APP fraud and pursue their claim for reimbursement. Consumers should not be expected to understand each firm's role in the push payment, and how this relates to industry standards. Nor should they have to deal with the receiving firm, since they are not a customer of that firm. We therefore support the code's requirement for the sending firm to administer any reimbursement, and to make this reimbursement swiftly, even if the sending and receiving firms have yet to agree on how to apportion these costs.

However, the code currently states that where a customer reports that they have been a victim of an APP scam, this report may not meet the definition of a complaint. This is not in line with the FCA's definition of a complaint as 'any oral or written expression of dissatisfaction, whether justified or not… which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience'.[5] When a consumer reports an APP fraud, both the sending and receiving firms should automatically count this as a complaint since it is not reasonable to expect consumers to know which firm might potentially have failed to meet their obligations. This would ensure that the FCA's time periods for resolving complaints are always

[4] UK Finance (2018), *2018 half year fraud update: Annexe*

[5] The full definition is: 'Any oral or written expression of dissatisfaction, whether justified or not, from, or on behalf of, a person about the provision of, or failure to provide, a financial service or a redress determination, which alleges that the complainant has suffered (or may suffer) financial loss, material distress or material inconvenience.'
https://www.handbook.fca.org.uk/handbook/glossary/G197.html

triggered as soon as a consumer reports an APP fraud, and that consumers are not required to wait for an initial response to then have to submit a complaint, before then potentially taking their complaint to the Financial Ombudsman Service.[6]

The steering group urgently needs to agree how to fund the reimbursement of victims in no blame cases, and who will govern the code

The steering group has not been able to agree so far on how to fund the reimbursement of victims in no blame cases, where both the victim and the firms involved have met their obligations under the code, and on who will govern the code. Both issues are fundamentally important for the success of the scheme and need to be urgently addressed in time for the launch of the scheme in early 2019.

Without a funding solution for no blame cases, many victims that have met the code's requisite level of care may not be reimbursed, despite this being a key principle of the code. As well as failing to address the detriment experienced by these victims, this could severely undermine public trust in the scheme.

As well as finding a solution to reimburse victims, the funding mechanism for no blame cases should be designed to provide continuing financial incentives for sending and receiving firms to go above and beyond the code's industry standards to adapt to fraudsters' changing methods. This can be challenging given that:

- firms are reliant on the actions of other firms to reduce the likelihood of their customers being scammed as the fraudster may bank with someone else; and
- the majority of the benefit from a firm guarding against its customers being fraudsters is likely to go to customers of other banks, who would otherwise have lost money to fraud.

This means that industry measures to combat scams often require collective action, which can be difficult to achieve. Such industry-wide measures will only be adopted if there are strong incentives on all firms and the relevant payment scheme to bear down on APP scams.

For example, plans by Pay.UK and members of Faster Payments to introduce Confirmation of Payee would arguably have been introduced sooner had there been stronger incentives on Faster Payments and its member firms to reduce scams since Faster Payments launched in 2008. Confirmation of Payee was considered at least as early as 2011 by the then Payments Council,[7] and later in 2015 by Payments UK, which is now part of UK Finance.[8] But progress has been slow, especially as it became unclear whether all firms would offer the service, and when those that chose to offer it would make it available. The Payment Systems Regulator has been

[6] Separately, Which? has welcomed the Financial Conduct Authority's (FCA) proposals to require receiving firms to follow the FCA's complaints handling rules, and to enable consumers to appeal to the Financial Ombudsman Service (FOS) if they are not happy with how their complaint is handled. See Which? (2018), *Response to FCA consultation on 'Authorised push payment fraud – extending the jurisdiction of the Financial Ombudsman Service'*

[7] Payments Council (2011), *National Payments Plan*

[8] Payments UK (2015), *World Class Payments in the UK*

forced to step in. It recently announced plans to consult on using its regulatory powers to give a 'general direction' to banks and payment service providers to implement Confirmation of Payee.[9] Which? strongly supports the Payment Systems Regulator's proposals.

Choosing the right governance body is also fundamentally important for the success of the code. The governance body should be accountable for achieving the aims of the code. It should therefore have strong incentives to encourage new industry-wide protections against scams that go above and beyond the existing code. But unless it is in a position to lead the development and implementation of these measures, it will be difficult for any progress to be made. Choosing the right governance body can also help to:

- encourage all firms involved in push payments to sign up to the voluntary code;
- evidence that firms are adhering to the code, both in their systems and in individual cases;
- resolve disputes between firms regarding reimbursement decisions; and
- continuously update the code, and any associated rules, to keep pace with how APP scams evolve.

The steering group has also not been able to decide what should happen when the victim and either or both firms have not met their obligations under the code. So a sending or receiving firm, or both, could fail to meet the standards in the code but face no penalty for doing so. For the code to be effective there should be strong financial incentives on firms to meet the code's standards, regardless of the actions of victims.

Victims in no blame cases should be reimbursed from a central fund collectively funded by a transaction charge on sending firms

If firms involved in push payments were to collectively fund no blame scenarios, this would provide incentives for sending and receiving firms to work individually and collectively to reduce the risk of APP scams, including by putting pressure on Pay.UK to require all of its members to introduce new protections against scams, such as Confirmation of Payee. In turn, this would reduce the cost to firms.

Only two of the steering group's proposals could potentially require firms involved in push payments to collectively fund no blame scenarios:

- creating a contribution mechanism across all parties with an ability to prevent APP scams from occurring (for example, firms, telecoms companies, data handlers etc); and
- a transaction charge on higher risk and higher value payments to be directed into a fund.

Some stakeholders have proposed that the transaction charge option above could be paid directly by consumers. However, this would not provide any incentive on firms involved in push

[9] The Payment Systems Regulator has proposed deadlines of 1 April 2019 for responding to Confirmation of Payee requests and 1 July 2019 for sending Confirmation of Payee requests and presenting results to their customers. https://www.psr.org.uk/psr-publications/news-announcements/PSR-welcomes-industry-code-to-protect-against-app-scams

payments or Faster Payments to reduce APP scams. It could also act as a barrier to consumers making transactions or lead them to use other less well-suited or riskier payment methods (e.g cash for large transactions). The transaction charge should therefore be levied on firms rather than consumers.

Similarly, most of the steering group's other proposed funding options would provide no incentives on firms involved in push payments to collectively reduce APP scams. Some, such as unlocking dormant funds, involve funding sources with no link to where the risks of APP scams can be mitigated. Some of these proposed options, such as consumers taking out insurance products, would also add barriers to consumers when making payments.

Of the two options above, we are concerned that the contribution mechanism across all parties will be difficult to define and agree in time for the launch of the code in early 2019. In contrast, Pay.UK already collects funding from members of Faster Payments, so a transaction charge levied just on its members firms could form part of this funding. The APP Scams Steering Group also has representatives from banks, the Electronic Money Association and UK Finance, whereas firms from other sectors are not currently represented.

We propose that the transaction charge should be paid by the sending firm to the Faster Payments scheme. This is because it is the sending firm that chooses the payment options for its customers. Its customers then benefit from any protections offered by those payment methods. It therefore has strong incentives to push for greater protections for its customers. The sending firm can also choose to offer its customers alternative methods of push payments, such as Visa Direct and Mastercard Send which launched recently, or to recommend that customers use other payment methods, such as card payments or PayPal.

We propose that this levy should form part of a new Faster Payments guarantee for consumers, similar to the Direct Debit Guarantee and card payment chargeback rules. The Faster Payments guarantee would make clear to consumers that they will always be reimbursed if they have met their requisite level of care when making a payment via Faster Payments.

Furthermore, we propose that Pay.UK should also levy an additional charge on firms that do not meet the standards of the code in cases where the victim has not met their requisite level of care. This would ensure that firms always have strong financial incentives to meet the code's standards. We do not think that these charges are likely to be sufficient to fund no blame cases, so this funding would be in addition to our proposed transaction charge on sending firms.

However, if our proposed funding mechanism for no blame cases is not ready in time for the launch of the code in early 2019, then the sending firm in each case should reimburse the victim until the funding mechanism launches. This is the simplest and most practical option to ensure that the code delivers on the principles agreed by the steering group until a longer term funding mechanism is agreed and implemented for no blame cases.

The contingent reimbursement model code should be governed by Pay.UK

At the heart of all APP scams is the relevant payment system. The draft code applies to three payment systems:

- the Faster Payments scheme, which is operated by Pay.UK;
- the CHAPS payment system, which is operated by the Bank of England; and
- internal book transfers, which involve payments made to and from the customer of the same payment service provider.

The code does not currently place any requirements on the operators of these schemes, Pay.UK and the Bank of England. This is despite the Payment Systems Regulator concluding in response to our super-complaint that neither the Faster Payments scheme nor the CHAPs scheme have any rules, policies or procedures related to consumer protection against scams.[10]

Other payment schemes have rules that protect consumers against fraudulent payments, including mechanisms for payments to be challenged and reversed. For example:

- Card schemes provide the interbank challenge and reversal process referred to as chargeback. The chargeback rules are highly detailed, and are updated on a frequent basis to take into account constantly changing fraud and behaviour patterns. For example, Mastercard's current Chargeback Guide is more than 400 pages.[11]
- Direct debits, which are operated by Pay.UK, are covered by the Direct Debit Guarantee. The paying firm is responsible for making any refunds immediately if an error is made in the payment of a direct debit. If the recipient has made the error then the sending firm must raise an indemnity claim to obtain the money back. If the recipient no longer exists, the receiving firm will settle the indemnity claim.

Chargeback and similar arrangements provide not only a means of reimbursing consumers, but also of shifting costs onto the receiving bank if they are at fault (or the merchant acquirer in a card scheme). So these interbank processes provide for liability to be passed to the receiving firm where the fraudster holds or operates an account. Liability is therefore allocated to those who are best able to manage the risk of fraudsters using bank accounts and payment systems to facilitate their scam.

Both the Faster Payments and CHAPs schemes should incorporate the principles of the code into their detailed scheme rules. Pay.UK should lead the governance of the contingent reimbursement model code due to the prevalence of APP scams on its system. Our analysis of UK Finance figures shows that in the first half of 2018, 96.2% (47,520) of APP payments where scams were reported, excluding international payments which are not covered by the code,

[10] The Payment Systems Regulator concluded: 'The operators of the Faster Payments Scheme (FPS) and CHAPS payment systems, the two payment systems which consumers might use when falling foul of APP scams, do not have any rules, policies or procedures in place related to consumer protection against fraud or scams. Operators of these systems view it as outside their remit to intervene in what they view as private contractual matters between PSPs and their customers.' Payment Systems Regulator (2016), *Which? authorised push payments super-complaint: PSR response*, p.5

[11] Mastercard (2018), *Chargeback Guide*

were made via Faster Payments. Just 0.7% (355) were payments made via CHAPs and 1.9% (921) via internal bank transfers.[12] All members of Faster Payments are required to follow its scheme rules, so this would ensure that the code is adopted across the industry. Pay.UK is also independent of its members firms, as required by the Bank of England's governance code of practice.

Pay.UK should:

- translate the key principles and requirements of the code into its scheme rules for Faster Payments, which all firms that use the scheme must follow;
- audit member firms' systems to evidence whether these meet the standards in the code, including whether warnings provided to consumers are effective;
- levy our proposed transaction charge on firms making payments via Faster Payments, which should be used to fund a new protection guarantee for consumers that meet their requisite level of care when making a payment, as well as to fund the governance and implementation of the code, such as new central systems or infrastructure;
- introduce a dispute mechanism for disputes between members of Faster Payments regarding APP scams;
- ensure that its wider governance structure, and any specific governance for the code, is independent of its member firms, and has strong consumer representation; and
- report regularly on the effectiveness of the code, and consult on changes to update the code and any associated rules.

About Which?

Which? is the largest consumer organisation in the UK with more than 1.3 million members and supporters. We operate as an independent, a-political, social enterprise working for all consumers. We are funded solely by our commercial ventures and receive no government money, public donations, or other fundraising income. Which?'s mission is to make individuals as powerful as the organisations they have to deal with in their daily lives, by empowering them to make informed decisions and by campaigning to make people's lives fairer, simpler and safer.

For more information, contact

November 2018

[12] Note, UK Finance also reports figures for BACS payments (568) and standing orders (29). UK Finance (2018), *2018 half year fraud update: Annexe*

Response from Buster Jack at ActionScam

1. IDEA: Introduction of a mandatory three-tier withdrawal curfew on authorised push payment transfers

1. 12 hour withdrawal curfew on transfers above £3,000 and below £10,000
2. 24 hour withdrawal curfew on transfers above £10,000 and below £20,000
3. 72 hour withdrawal curfew on transfers above £20,000

If the money-sender alerts his/her own bank of suspected fraud within 12 hours of the transfer, the sending bank should become liable for that loss in full if it allows the withdrawal of those funds within that period. While it's true that 12 hours is sufficient for a fraudster to withdraw the funds at the receiving end, a 12-hour curfew on withdrawals applicable to transfers of above (say) £3,000 would at least give potential victims a chance to put a block on the receiving account before the withdrawal is made. So the outward transfer itself would be near-instant as is the case now, but the recipient, while able to see that the funds have been received, will have to wait 12 hours before making a withdrawal of those specific funds. It's a compromise rather than a solution, but it would prevent fraud from being completed in a significant number of cases. The longer the withdrawal curfew, the higher the chances of preventing fraud. If the recipient refuses to accept these conditions, the sender would need to notify his/her bank (to unlock the withdrawal curfew) who would be obliged to advise their customer of the potential risks in doing so.

This would not be a refund in the literal sense, as the receiving bank would simply be reversing the transaction at little or no cost to itself. In a way it would replace FPS with SPS - Faster replaced with slower.

This could be expanded to longer withdrawal curfews for higher transfers, e.g. 72 hours for transfers above £20,000

This should be of particular benefit to would-be victims of telephone spoofing, which often requires targets to transfer money to what they are given to believe is their own ('new') bank account. The caller/fraudster should have no objection to a 72-hour withdrawal curfew because the funds are, it's assumed, being sent by the sender to himself or herself. It also gives the bank 72 hours to contact its customer to check that the transfer was not fraudulent, and if it was, the funds can be requested from the recipient bank at no cost (or at least negligible cost) to either bank or the victim. The only loser in such a system would be the fraudster.

Another source of substantial losses to APPF is conveyancing fraud, when large sums are transferred to non-existent solicitors. Again, 72 hours to reverse any transaction over £20,000. A withdrawal curfew could deter several fraudsters from trying this in the future, for fear of "losing" a large sum of money that they had invested a considerable amount of time in over weeks or even months. 72 hours for the victim to realise that their solicitors have received nothing at all, and to take remedial action at negligible cost to any party other than the fraudster.

2. IDEA: Make receiving banks owe a Duty of Care to non-customers who pay into other banks

At present, beneficiary banks do not owe a Duty of Care to anyone making an authorised push payment transfer into a bank of which they are not a customer.
This urgently needs to change.

- *(that's the short version)*

Longer Version - but please read.

If a fraudster steals money from the victim's account by means of either an unauthorised transaction or an authorised push payment fraud, then the money in the fraudster's account is still the victim's money.

The Law Reports (Appeal Cases)
URL: http://www.bailii.org/uk/cases/UKHL/1990/2.html
Cite as: [1990] 2 AC 605, [1990] 1 All ER 568, [1990] UKHL 2

Caparo Industries Plc. Respondents and Dickman and Others Appellants

(As reported in BAILII)

What emerges is that, in addition to the foreseeability of damage, necessary ingredients in any situation giving rise to a **duty of care** are that there should exist between the party owing the duty and the party to whom it is owed a relationship characterised by the law as one of "proximity" or "neighbourhood" and that the situation should be one in which the court considers it fair, just and reasonable that the law should impose a duty of a given scope upon the one party for the benefit of the other. But it is implicit in the passages referred to that the concepts of proximity and fairness embodied in these additional ingredients are not susceptible to any such precise definition as would be necessary to give them utility as practical tests, but amount in effect to little more than convenient labels to attach to the features of different specific situations which, on a detailed examination of all the circumstances, the law recognises pragmatically as giving rise to a duty of care of a given scope.

from which I draw three phrases:-

1. foreseeability of damage

2. proximity or neighbourhood of the relationship

3. fair, just and reasonable

Determining if there is a Duty of Care

The judge said that these three labels: "amount in effect to little more than convenient labels to attach to the features of different specific situations which, on a detailed examination of all the circumstances, the law recognises pragmatically as giving rise to a duty of care of a given scope".

So we need to examine each label in the specific scope of the Receiving Bank holding an account into which money is transferred as a result of a fraud.

I suggest that at this stage we do not ask whether the receiving account was opened in accordance with Money Laundering (AML) and Payment Services Regulations (PSR). These will be questions that are asked when we consider whether or not the bank has fulfilled its Duty of Care. At this stage we are only concerned with the question of 'does the bank have a Duty of Care?'

Q1. Was there a 'foreseeability of damage' to the victim if the receiving account was opened without compliance to AML and PSR?

Yes. If a bank opens or operates an account through a process or processes that are not complaint with AML and PSR then it is clearly foreseeable that that account will be used for fraudulent purposes and cause harm to the Victim of the fraudulent activity.

Q2. Is there an appropriate 'proximity or neighbourhood of the relationship' between the Receiving Bank and the Victim?

Yes. The receiving bank is now holding money that is the legal property of the Victim. I believe that this creates an appropriate proximity of relationship.

Q3. Is it 'fair, just and reasonable' to establish a **Duty of Care** from the Receiving Bank to the Victim.

Yes. The Receiving Bank is a large commercial organisation with wide ranging responsibilities for the conduct of its business for which it requires the trust and confidence of the whole community that it serves. If a person transfers money into an account held by the Bank it must be reasonable for that person to expect the Bank to be fulfilling it regulatory obligations.

Ergo, the receiving bank owes a Duty of Care to a victim of fraud whose funds still belonged to them when those funds - procured by fraud - were allowed to be withdrawn by the receiving bank

- *end of longer version*

Thank you for reading this in full.

https://www.fca.org.uk/publications/discussion-papers/dp18-5-duty-care-and-potential-alternative-approaches

DP18/5: a duty of care and potential alternative ...

www.fca.org.uk

On 17 July 2018, alongside our Approach to Consumers, we published a Discussion Paper on a duty of care and potential alternative approaches.

The above mini-thesis is presented with the collaboration of recognised APPF specialist [✂] of 4Keys International.

3. IDEA: Beneficiary Banks in APP Fraud to provide all account creation documents to victims (or the FOS)

At the present time, the significant majority of APP Fraud victims have only one option when trying to recover their losses, and that is to demonstrate that the beneficiary account had been created using forged ID and documents. In most cases, fraudulently opened accounts are used at the primary stage, so obtaining evidence is a crucial factor. However this is very difficult to do. First of all, the only credible source of such evidence is the police, and apart from the fact that the police can be reluctant to share this information - even with direct victims - a significant proportion of reports to ActionFraud do not proceed any further than that anyway, because many crimes are not disseminated by ActionFraud to an appointed police force. So victims often have no chance of a police report because there is no police investigation at all.

While this is likely to cause conflicts with Data Protection regulations, it nevertheless offers victims genuine hope of recovering their losses. Most banks, when presented with evidence that the receiving account had been created using forged ID and other documents will make gesture-of-goodwill settlements while denying liability. All victims given such offers will accept them. By obliging banks to provide victims with all documents used in the creation of the account used to receive stolen funds, police resources - already under strain to breaking point - will be free to concentrate only on the criminal investigation. The civil element, which is the one victims are far more interested in anyway, can then be handled by the victim's appointed legal counsel or other intermediary, whose task will be to establish whether the account was opened fraudulently or not.

Perhaps the best solution to the problem of DP conflict would be to out-source such work to the Financial Ombudsman Service, which is in any case not subject to data protection restrictions in the way a member of the public would be. First of all, the remit of the FOS would need to be changed in one simple but essential way: Victims of APP Fraud would be able to refer complaints of this kind to the Financial Ombudsman Service, something that is usually denied at the present time because complaints against banks of which the complainant is not a customer are classified as ineligible. So step one would be to remove this ridiculous rule, and create a dedicated group within the FOS whose remit would be to establish whether a given bank account has been opened in breach of MLD4 (4th Money Laundering Directive). If it is confirmed that forged documents had been used to create the beneficiary account, the complaint should be upheld in favour of the APP Fraud victim. This is how the system should work with an ombudsman service that is fair, reasonable, neutral and independent - words currently used by the FOS on a regular basis to describe itself - but in reality most APP Fraud victims are shunned not only by ActionFraud, but by the Financial Ombudsman Service as well. It is small wonder that almost every APP Fraud victim ends up believing that nobody cares and that the system is skewed in the banks' favour. This needs to change, and fast.

I would be more than willing to help up set up and run such a dedicated group within the Financial Ombudsman Service.

4. Further comment:

It's the morning after the night before and I'm really keen to press home what I believe are the 'everybody wins' benefits of my 3rd Idea, the one involving the Financial Ombudsman Service. In the last half-hour I have received an email from a couple who lost £16,000 in an APPF, here is ActionFraud's reaction to their report:-

==========
[✂]

==========

THIS IS THE REALITY. They were conned into giving away £16,000, and the police won't even investigate it because they haven't been instructed to by NFIB/City of London Police. Thousands of people get messages like this every month. It's just not right.

My idea would solve this. To set up a new division within the Financial Ombudsman Service so that people like this would not care if the police investigated or not. Instead, while they would still report the crime to ActionFraud, they would then serve the receiving bank with a complaint (I would suggest that ActionFraud advise them of this in the acknowledgement letter that everyone receives).

1. Victim complains to the beneficiary bank
2. Victim refers the complaint to the Financial Ombudsman Service
3. FOS direct such a complaint to its new RBFC unit (receiving bank fraud complaints)
4. FOS serves bank with a Production Order
5. Bank responds with copies of ID and docs used to open the account
6. FOS sends these to fraud specialist divisions at Immigration Office and utility companies
7. Responses received, stating whether ID card and utility bill were authentic or not
8. If forged, FOS uphold the complaint (based on AML breaches by the bank)

9. If authentic, FOS rule in favour of the bank, complaint rejected, case closed (subject to appeal)

It's not that complicated, and the benefits would be significant. As soon as banks find themselves refunding more APPF victims than they currently do, they won't wait for legislation or regulatory amendments - they'll make internal changes of their own volition as a matter of urgency. I refer mainly to the robustness of compliance with AML regulations. Banks will do their utmost to make sure that all ID and documents presented at the account-opening stage are 100% authentic. That's what should be happening now, but plainly it's not. For the first time, banks will "take fraud seriously".

Within a year, APPF volumes will have fallen drastically, because the banks will have made sure that account applications are water-tight clean and authentic.

I cannot think of a valid reason why this could not be implemented. Obviously the banks would strongly resist all this, but does the dog wag the tail, or the tail the dog? What purpose does banking regulation serve unless it regulates the banks?

Sincerely

APP Scams Steering Group – Draft Contingent Reimbursement Model Code – BRC Response

1. The British Retail Consortium represents the retail industry, including retailers both large and small amongst our members. Our membership comprises over 5,000 businesses responsible for £180bn of sales and employing over one and half million employees. Our members are active in the fight against fraud, and may also be significant victims in their own right. Amongst other things, we are members of the Joint Fraud Taskforce.

2. We welcome the opportunity to respond to the consultation, and for the steps which partner organisations have attempted to take to provide a degree of certainty, reassurance and protection to users of payment systems.

3. We are, however, concerned about two areas of the proposals in general terms, which we think may give rise to considerable unfairness, lead to unfortunate outcomes and do not flow from the foregoing work or contextual material Our most significant concern is over scope, a factor the adequacy of which has been impossible to determine without the new material in this latest consultation.

4. In addition, we have some suggestions about some points of drafting within the proposed code.

5. We have, where possible, sought to brigade our concerns under relevant questions, but we trust that the full range of our views will be considered in the spirit of finding consensus.

Scope of Code

6. As well as a free-standing point, please consider this a response to Questions 1, 2, 20, 21 and 22.

7. As the consultation document(s) set out, the drive to create such a scheme came from a super-complaint by Which? in September 2016. That super-complaint argued that reform was necessary to alter financial institutions' behaviour and protect users of their services from harm. No distinctions are drawn in that document by size of organisation. Applying the new scheme to some, but not all, consumers risks perpetuating or even exacerbating (by creating new unhelpful incentives for fraudsters and others) the current market failures.

8. In particular, we are concerned by the approach to scope in DS2 and DS1(2)(e) of the proposed code to limit the protection of the code to consumers, microenterprises [sic.] and charities. Potentially important preliminary drafting points to note include that i) the term used and defined in Part 1 of the Payment Service Regulations 2017 ('PSR') is "micro-enterprise" and not "microenterprise", so technically as drafted the definition might be read to exclude all businesses; and ii) those terms derive from EC Recommendation 2003/361/EC of May 2003, not the PSR (as the PSR makes clear).

9. But our main point is a wider one – which is that an arbitrary size-based threshold should not be applied to scope where the victim happens to be a business. The Consultation provides

very little thinking on the rationale for that approach, only noting that it derives from the PSR response to the earlier, February 2018, response.[1] In that earlier response the only reasoning given is to ensure alignment with the PSR. Notably, there is no reasoning based around the affordability of the scheme (or not) in the response, which cannot therefore have been part of the rationale for the decision.

10. This consultation is the first opportunity to comment on the decision to take the approach in that earlier response in the light of the proposed protections for those in and out of scope, which we wish to take and ask for a reconsideration.

11. In that earlier response, at paragraph 3.82, the reasoning for the approach to scope as expressed is flawed and leads to unfair and perverse outcomes in a number of ways, including:

    a. as the earlier response makes clear, the scope was changed from the previous consultation (to which it responded) without any expressed reasoning. The earlier term used was "small businesses", which in the response had become "micro-enterprises". That is clearly a significant shift in scope and emphasis away from other common terms which might be used to denote "small businesses", including those used in EC Recommendation 2003/361/EC;

    b. as set out above, in the earlier report the sole (and highly limited) rationale applied is the approach taken in the PSR, and in particular the need to ensure consistency with "many of the rights and obligations in relation to the provision of payment services set out in the [PSR]" within it.

       But that is an incorrect reading of the PSR. A simple textual search of the PSR shows that there are only 6 references in the 144 pages of text to "micro". The first two of which are definitional (section 2), the final a reference to an existing section in another regulation (Part 3). So none of those three are relevant to the "rights and obligations".

       The remaining three references only come from Parts 6 and 7 of the PSR, out of a total of 11 Parts – very far from "many". More importantly, it is clear that the parallel drawn to the approach taken in the later consultation is highly flawed. The first and second of the substantive references (ss. 40(7) and 63(5)) allow all micro-enterprises (and others) to **agree that certain of the provisions do not apply** – that is **permits** them to do so. That is very different to *excluding as a matter of rule* other organisations from provisions the benefit of which they would otherwise have.

       The final reference (in s. 88(a)) is also quite different, in that it provides for a different time period for funds to be available post-transfer. Praying that in aid for the proposed approach in this code would only be valid where very slightly different timeframes (immediately after receipt vs. end of next business day) were required for recompense to defrauded consumers.

       So it is clear that the parallel drawn between the two sets of provisions to justify the more limited scope here is flawed. If the other provisions were to give micro-enterprises and others the ability to opt out of the proposed scheme then the parallel

[1] 'APP Scams Steering Group: Draft Contingent Reimbursement Model Code – Consultation Paper' (September 2018) at para 3.13.

might be rational and legitimate. That was a possibility (and we do not now express a position on the desirability of it) which has not been followed.

Indeed, there is a very credible argument that the approach to scope taken actually moves the scope of the code further away from the PSR's than if there were no limits on scope by size. The approach taken delivers the opposite of the expressed reasoning for it.

Given the approach set out in the remainder of the paper, a reconsideration of scope is certainly required. We would go further and argue that, in order to not breach the principles on which the scheme as proposed is intended to run, there should be no curbs on the types of consumer which should attract protections;

c. taking the approach to scope in the consultation would create a two-tier system for victims of fraud based around an objectively indefensible distinction. A company with 51 employees which is a victim is not necessarily less deserving of recompense than a company with 49, and in our view there is no need to draw a line as suggested on the published arguments and reasoning. That is particularly as in both cases the victim may have acted entirely properly, and in-line with the proposed standards, whilst the financial institution did not. Further, the proposed approach creates a clear incentive for businesses to focus the level of protection they offer at customers who are given protection by the scheme and not at others, which may actually increase fraud; and

d. flowing from the above points, and as an exercise in moral hazard, the approach to scope as applied to the proposed design of the scheme carries a clear risk that it will breach several of the core principles the group has identified, including:

   - *incentives for those with the ability to effectively prevent APP scams and reduce their impact* – financial institutions will not be incentivised to offer the same level of protection and mitigation to out-of-scope consumers;

   - *consistency of outcomes for those with the same characteristics* – the only characteristic applied in scope for business victims is a red line on size and turnover, meaning that essentially the same consumers can be treated very differently; and

   - *no adverse ability on commercial development of further protections* – by keeping larger victims out of scope the incentive to develop additional protections will be significantly reduced, affecting the market for developing such products.

12. Given the above, there is a clear case that the proposed scope and model will have very strongly negative effects in response to questions 1,2, 20, 21 and 22. The way to resolve those issues is to remove the barrier to protecting and mitigating the harm to certain consumers by abolishing the current line on scope by size; we would be happy to discuss alternatives.

13. Consequent drafting changes might also be required elsewhere in the Code.

Standards for Firms

14. Please consider this a further response to Questions 1 and 2.

15. Section 'SF' of the draft code sets out the standards for 'firms', that is the financial institutions engaged in executing the fraudulent payment. We welcome many areas, but also think there are places which could be strengthened to better meet the principles for this work:

    a. it is not clear how compliance with the 'General Expectations of Firms' are to be incentivised and managed. Non-compliance by a firm with GF(1)-(3) might not be read as a possible trigger for repayment in the first section of SF ("These provisions set….that took place");

    b. when giving evidence to the House of Commons' Treasury Committee, Stephen Jones, Chief Executive Officer of UK Finance, spoke compellingly on Push Payment fraud (see from Q.285 to Q.289 here). At Q. 285 Mr. Jones identified the key issue around push payment fraud as "…. in the vast majority of cases, [receiving] accounts are opened through perfectly well-undertaken KYC processes….. They open their account perfectly legitimately and are then compromised". Whilst the Code makes reference at SF2 to detecting accounts being used to received funds, it would be sensible to make specific reference also to accounts which have been compromised in the way Mr Jones described;

    c. as drafted there is a risk that, in conjunction with the structure of R1 and R2, the requirement for Effective Warnings to be given can be met by simply providing the same boiler-plate text for every transaction, which over time would undermine the impact of the warning and cease to be effective. This risk could be mitigated by strengthening the drafting in SF1, SF1(2)(c) and SF1(2)(e)(v) to be entirely clear that to be effective a warning has to be worded specifically around the risk analysis with the nature of the warnings and the severity of the risk described explicitly related to that risk, perhaps with some kind of tiering system;

    d. the link between repayment and a failure to meet the standards being 'material' is of concern, and does not meet the approach described in para 3.49 of the consultation paper.

       First, it adds an extra layer of complexity and the potential for argument which many victims may be unable to meet, certainly it creates the potential for an inequality of arms as against a well-resourced financial institution. Second, It may also cause financial institutions to simply not protect certain customers, perhaps those with learning disabilities, on the basis that they may not have responded to a warning if provided or would be less able to challenge a decision not to recompense them. Third, the customer might not have received the requisite level of care but not be reimbursed. Such outcomes would be extremely harmful, and should be avoided by removing the requirement; and

    e. the requirements upon a sending firm under SF 1(4) may (as drafted) be met by including relevant systems in general terms, including where those systems failed with regard to a particular Customer. For example, firms may take steps to identify Customers who are vulnerable to push fraud, and even if they fail to identify a specific customer through those steps, and that customer then becomes a victim having not received additional protection measures, then the requirements of SF1(4) could be argued to have been met because systems had been put in place.

Other points

16. Whilst we have considered the draft code from a policy position, and not undertaken a close scrutiny of the drafting, there are a few areas where we believe some further clarification of the drafting and intention might be helpful, including:

    a. ***DS1(2)(a)(i)*** – "another" is otiose and unclear, and might seek to exclude from scope situations where a victim intends to transfer funds from one to another of their accounts but is deceived and instead transfers the funds to a fraudster's account;

    b. ***DS1(2)(a)(ii)*** – consideration should be given to whether this is drawn too widely in that it captures situations where the transfer was entirely legitimate but at some future point the money is used for fraudulent purposes; and

    c. ***DS2(2)(b)*** – the term "commercial disputes" is not actually defined here, and given that this is a potentially key point for scope that is quite a serious issue. Providing examples is helpful, but a proper definition is also required.

[✂]
British Retail Consortium.
November 2018.

APP Scams steering group - Draft Contingent Reimbursement Model Code

Response from the Building Societies Association

09 November 2018

Building Societies Association

Set out below is the response from the Building Societies Association (BSA) to the draft APP Fraud Contingent Reimbursement Model Code and accompanying consultation published in September 2018 by the APP Scams Steering group / Contingent Reimbursement Model (CRM) Working Party.

The Building Societies Association (BSA) represents all 43 UK building societies. Building societies have total assets of over £396 billion and, together with their subsidiaries, hold residential mortgages of over £312 billion, 23% of the total outstanding in the UK. They hold over £276 billion of retail deposits, accounting for 18% of all such deposits in the UK. Building societies account for 37% of all cash ISA balances. They employ approximately 40,000 full and part-time staff and operate through approximately 1,550 branches.

Summary

- The objectives behind the draft CRM Code are sensible and desirable and have the building society sector's full support. Authorised push payment fraud (APP fraud) is a significant threat to consumers, firms and confidence in UK financial services that all stakeholders must work together to minimise.
- However, the Code's objectives have already been undermined by a dislocation between APP fraud policy and APP fraud infrastructure development that will create a 2 tier APP fraud protection environment for UK banks, building societies and their customers:
    - Tier 1 will consist of firms with full access to Confirmation of Payee from its implementation and full access to the infrastructure supporting the UK Finance APP fraud best practice principles.
    - Tier 2 will be those building societies, challenger banks and credit unions that will not have this access. Their customers (c.6.5 million building society customers) will be less well-protected against APP fraud.
    - Providing the wider infrastructure that tier 2 firms need access to in order to comply with the code is not a feasible option in the short term.
    - Tier 2 firms will be more likely to be targeted by criminals for laundering the proceeds of APP fraud once it is clear that they have fewer defences than tier 1 firms. The firms also still carry the reputational risk of public expectation to provide the same level of protection as tier 1 firms.
    - 2 tier APP fraud protection will also have consequences for the Financial Ombudsman service in determining what is fair in APP fraud complaints.
- This is obviously not what the Code intends but tier 2 firms would be immediately non-compliant through no fault of their own if they signed up to the CRM code in current form. There is a significant risk of a large number of tier 2 firms not signing up to the Code because of their disadvantaged position (and a public explanation of why they did not sign up) undermining the launch of the Code as an effective solution to tackling APP fraud.
- The dislocation between policy and infrastructure development that has led to the situation of two tier APP fraud protection is due to the absence of representatives of firms outside of the clearing banks on the CRM Working Group and related APP fraud prevention infrastructure development programmes.

- We strongly recommend that this state of affairs is addressed for the next stage of development and would like the Payment services regulator to take the lead in re-balancing representation.
- The APP Scams Steering Group needs to undertake an urgent review as to how the code can be adapted to operate within this unintended environment. The BSA and BSA members commit to working with the Steering Group and other APP fraud prevention programmes to make the CRM Code workable under the two tier APP fraud protection environment that consumers and firms will have to live with.

The position of building societies

As the code and related infrastructure delivery plans stand at the moment, most building societies would find themselves as tier 2 firms in terms of the APP fraud protection they can offer c.6.5 million customers.

Building societies certainly fit the target profile for the CRM code of "firms involved in making or receiving APP-associated payments between UK bank accounts who have control over preventing and responding to APP scams" and their customers are already being targeted for APP fraud. Our sector fully supports the objectives of the contingent reimbursement model to reduce the occurrence of APP fraud, increase customer-protection from the impact of APP fraud and minimise disruption to legitimate payment journeys. BSA Members will commit to adopting the CRM code's requirements in respect of fraud education, targeted fraud warnings and supporting fraud victims as best practice for their products and services.

However, the majority of building societies have a banking model that differs from that of a full payment services provider:

- They have no direct access to CHAPS, SWIFT and Faster Payments and use a clearing bank providing agency banking services to undertake transfers to other banks from their customers' accounts on their behalf.
- Some societies do allow transfers from internet–based savings accounts to the customer's current account but that account has to be nominated in advance and cannot be varied by the customer.
- Under current plans, firms using this banking model would not have access to the UK Finance-provided portal to report APP fraud to receiving banks or be able to offer their customers the Confirmation of Payee check – both are prerequisites for compliance with the proposed code.

Our members are considering carefully whether they should sign up for a voluntary code that they will be unable to implement in full. They are mindful of significant concerns about the customer service and reputational implications of not signing up – it is unlikely that consumer groups and other advocates of the code will be interested in reasons why some firms have to offer a lower level of APP fraud protection. They are also conscious of the implications for consumer confidence of the new code failing to meet its objectives at launch.

The position that the majority of BSA members now find themselves in is best summarised by feedback on this consultation from a BSA member:

"We along with other Building Societies are at an immediate disadvantage compared to larger banking organisations because:

- *Currently we are unable to fully participate with the Best Practice Standards as we do not have access to the UK Finance online portal (and therefore contacts) to submit APP fraud orders to the receiving banks*
- *As we do not have access to the portal we cannot receive the APP fraud notifications from the victim bank - UK Finance need to enable smaller organisations access to this facility to enable full participation.*
- *At this time, as a Building Society requiring a clearing bank, we are unaware whether we will be able to participate with the Confirmation of the Payee facility.*

We are prepared to re-evaluate our position as and when further clarification to the above points are released and we are able to fully participate with the Best Practice Standards and Confirmation of the Payee."

Current misalignment of policy and infrastructure

UK Finance online portal

Currently, access to the UK Finance online portal for reporting APP fraud to a receiving bank is only available for a certain level of UK Finance membership, which is above the needs of most BSA members who are also UK Finance members. It is not open to non-UK finances member such as BSA members who do not also have UK Finance membership. The result is that 41 out of 43 building societies currently do not have access to this portal and therefore could not fulfil their obligations under the proposed CRM code in full.

There is no suggestion that UK Finance have engineered this situation deliberately or that their intention is to act anti-competitively or leverage access to this portal to increase membership revenue.

The BSA is engaged with UK Finance on providing this wider access but there are significant development issues to sort out in respect of providing controlled access to their member-only website for non-members, building capacity for the portal to handle the extra capacity and the business case for this development compared to other development requirements on the UK Finance website. As of now, it is not possible to give guarantees as to when wider access will be available.

Confirmation of Payee

Confirmation of Payee is a banking infrastructure project running alongside but not co-ordinated with the CRM Working Party. Its target is that all payment service providers that are participants in Faster Payments be capable of sending confirmation of payee requests and presenting the response showing the name of the account that the payment is to be made to. their customers by July 2019.

For July 2019, "Customers" – will not include agency banking customers such as building societies and there is no commitment to provide Confirmation of Payee to them other than a vague intention to address this in a "phase 2". We hope that imminent consultation by the PSR on Confirmation of Payee will provide fuller commitment.

Delivering Confirmation of Payee is a significant technical development programme and - even if the promise of delivery in phase 2 was confirmed - it will be some time before banks could put this facility in place for building societies and other agency customers. However, it is important that the needs of agency banking customers are locked into Confirmation of Payee delivery now.

Development going forward

The CRM Working Group needs to undertake an urgent review as to how the CRM code can be adapted to operate within an (unintended) two tier APP fraud protection environment – as the code is written now it would be impossible for tier 2 firms to be able to comply.

The dislocation between policy and infrastructure development that has led to the situation of two tier APP fraud protection has been created by a lack of consideration of the role of banks and building societies outside of the major clearing banks in preventing APP fraud created by the absence of representatives of firms outside of the clearing banks on the CRM Working Group and related APP fraud prevention infrastructure development programmes.

We strongly recommend that this state of affairs is addressed for the next stage of development, led by the Payment Services Regulator.

The BSA and its members will commit to working closely the CRM Working Group and other programmes from now on - if invited to do so - to make sure that the CRM Code is made workable for the two tier APP fraud protection environment that firms and consumers will have to live with and to close the infrastructure gap between the two tiers.

Other aspects of the draft CRM Code:

- We support general duties for firms to provide fraud education, targeted warning and victim-support for customers. BSA members will commit to adopting these as best practice in their products and services.
- We also support the proposed duties for customers and firms where firms have the necessary capability to comply – though it may be helpful for customers to understand their duties in respect of APP fraud if they were written in plainer, less legalistic language with examples provided.
- The Code's current approach to vulnerability is too wide and may have unintended consequences. In particular, the Code's proposed introduction of assessments for vulnerability to fraud risks undermines one of the basic principles of supporting consumer vulnerability in that you support customers in vulnerable circumstances without judging how they got there. Case by case assessment of whether individual victims had vulnerable circumstances which would entitle them to automatic reimbursement will make maintaining that customer's trust and willingness to highlight difficult personal circumstances much more difficult by introducing a judgemental element around their circumstances.
- We agree with the working group's position on reimbursement for no fault cases that this is a good objective in principle but there will need to be a sustainable source of funding in place back up the principle with available funds before it can be delivered on. Our preference on funding would be a contribution mechanism across all parties with an ability to prevent APP scams from occurring including 3rd parties outside of

financial services, including redirection of fines by the ICO and other regulators for data loss, control weaknesses, failed cyber defences etc. which have led to APP fraud and recovered proceeds of crime from APP fraud.

- The Payment Services Regulator is the body most appropriate to take on supervision of / accountability for the Code and associated programmes.

Our responses to the questions highlighted in the consultation

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?

Were the Code to achieve its stated objectives, UK consumers would benefit from a significant number of consumers targeted for APP fraud not becoming fraud victims and from the safety net of reimbursement of their losses in appropriate circumstances. However, we have concerns that the Code, as it stands, could inadvertently contribute to more fraud, more fraud victims, 2 tier APP fraud protection and undermine support for customers in vulnerable circumstances:

Investigation and prosecution of fraud – A likely consequence of introducing more frequent reimbursement so that fraud becomes a victimless crime is that APP fraud and other fraud will rapidly become de-prioritised by UK law enforcement when allocating already tight resources. A lower priority on fraud would be a signal to criminals that the UK is not taking fraud investigation and prosecution seriously and would lead to even more fraud being targeted at UK plc and UK consumers.

Consumer recklessness– Responses to the PSR consultation earlier in 2018 that created the working party highlighted significant concerns that the reimbursement safety net might lead to consumers becoming reckless about APP fraud risk knowing that they have the strong possibility of not suffering any loss if they have misjudged a fraudster's approach. We note that the current consultation does not address this behaviour and the risk remains. This could be dealt with by evidential standards requiring the customer to show that they were not reckless though the judgement culture that this would create would not be helpful for building consumers' trust in financial services – particularly vulnerable customers (see below).

Support for vulnerabilities - The Code's proposed introduction of assessments for vulnerability to fraud risks undermines one of the basic principles of supporting consumer vulnerability in that you support customers in vulnerable circumstances without judging how they got there. We understand the need to introduce a case by case assessment of whether individual victims had vulnerable circumstances which would entitle them to automatic reimbursement because there will be individuals who abuse this but this process will make maintaining that customer's trust and willingness to highlight difficult personal circumstances much more difficult by introducing a judgemental element around their circumstances.

Inconsistent application - So long as all institutions and customer comply with the Code and work the same, there should be no negative impact to the victims. There would be implications for consumers where the customer or institutions are difficult or incorporative. Each institution will have additional controls, reporting and training to implement.

Our most urgent concern is that customers of firms (and firms themselves) in tier 2 for access to fraud prevention and response measures would obviously suffer the risk of being less protected by the Code. – see below.

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

In its current state, the CRM Code and associated planned APP fraud prevention and response measures will create a 2 tier APP fraud protection environment for UK banks, building societies and their customers:

- Tier 1 will consist of firms with full access to Confirmation of Payee from its implementation and full access to the infrastructure supporting the UK Finance APP fraud best practice principles.
- Tier 2 will be those banks, building societies and credit unions that will not have this access. Their customers will be less well-protected against APP fraud.
- Tier 2 firms will be more likely to be targeted by criminals for laundering the proceeds of APP fraud once it is clear that they have fewer defences than tier 1 firms. The firms also still carry the reputational risk of being expected to provide the same level of protection as tier 1 firms.
- 2 tier APP fraud protection will also have consequences for the Financial Ombudsman service in determining what is fair in APP fraud complaints. It is unfair to penalise either the customer or a tier 2 firm in this unsatisfactory situation.

This is obviously not what the Code intends but we are currently in a position where a group of firms would face the consequences of non-compliance through no fault of their own if they signed up - as providing the wider infrastructure that tier 2 firms need access to is mandatory for compliance with the Code but not a feasible option in the short term.

There is a significant risk of a large number of tier 2 firms not signing up to the Code because of their disadvantaged position (and a public explanation of why they did not sign up) undermining the launch of the code as an effective solution to tackling APP fraud.

The APP Scams Steering Group needs to undertake an urgent review as to how the Code can be adapted to operate within this unintended environment.

We assume that none of the above were intended. Our observation is that this situation has occurred because of a lack of consideration of the role of banks and building societies outside of the major clearing banks in preventing APP fraud and a lack of understanding of the importance of wide availability of key parts of the infrastructure to deliver the code – for example Confirmation of Payee. This has led to dislocation between policy and infrastructure development. Lack of representation of firms who are outside the larger clearing banks as participants in the APP Scams Steering Group has not helped with encouraging a wider industry perspective.

The BSA and BSA members will commit to working closely with APP Scams Steering Group and other relevant APP fraud programmes from now on - if invited to do so - to make sure that the CRM code covers all banks and building society customers at risk of APP fraud effectively and consistently.

How should the effectiveness of the Code be measured?

Effectiveness should be measured on delivery of the steering group's draft principles as set out in this consultation. On those terms, the code would be considered to be effective if:

- The overall level of successful APP fraud falls.
- More APP fraud victims are suitably protected from the consequences of being a victim of APP fraud.
- More consumers are aware of the nature of APP fraud and what they can do to avoid becoming victims
- Where reimbursement is appropriate, victims receive reimbursement within agreed timescales.
- All firms have access to prevention and response measures so can fully adhere to the code.
- Evidential standards prove to be realistic and workable.

It would be ineffective if:

- The level of successful APP fraud continues to rise. In particular, if numbers of repeat fraud victims increases.
- Some building societies and banks are unable to adhere fully to the code through lack of access to underpinning infrastructure.
- The code itself becomes an MO for fraud.
- The pressure for both firms and victims to prove that evidential standards have been met makes the customer relationship more adversarial and introduces a judgemental approach to customer vulnerability.

Effectiveness could also be assess through complaint numbers (the more complaints the less the code is working); focus groups and feedback from trade bodies.

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

We broadly agree with the standards set for firms, with the following qualifications reflecting the different levels of access to the infrastructure underpinning the Code and circumstances of a current account provider and a savings account provider:

SF1, (1), a – Firms who offer savings products only will not have the same granularity of transaction data that current account providers have so customer behaviour analytics will be less effective in identifying payments that are at higher risk of APP fraud.

SF1, (3) & SF2 (2) – There is no certainty when Confirmation of Payee will be available to building societies and smaller banks who rely on an agency bank to provide money transmission services to their customers.

SF1, (6) & SF2, (4) – Notifying receiving firms when an APP fraud is reported using the UK Finance best practice standard requires access to the relevant UK Finance Portal. At present access is only available to full members of UK Finance, which means that 41 of 43 building societies (credit unions also) do not have access to this facility and so would be unable to comply with this requirement.

The implications for firms not meeting these standards need to be reconsidered for those firms who don't have access to the APP fraud prevention infrastructure required for compliance with the above.

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 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.

Our members feel that a level playing field is required so that the customer cannot claim off both institutions. It would be useful to have central contacts so that firms can discuss common cases.

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.

Under current plans for the roll out of Confirmation of Payee it is not known when every firm will have Confirmation of Payee capability - the provision R2(1)b should not apply where the firm has not been given that capability.

We find it hard to envision a scenario where a firm has failed to provide an effective warning and the customer has then failed to act on it. The customer can't fail to act on a warning that hasn't been made. Our members suggest that it would be useful to have some examples of when this could apply. The Society feels where evidence shows all parties have not met the level of care, a 3 way split could be applied.

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.

Under current plans for the roll out of Confirmation of Payee it is not known when every firm will have Confirmation of payee capability - the provision R2(1)b should not apply where the firm has not been given that capability.

We find it hard to envision a scenario where a firm has failed to provide an effective warning and the customer has then failed to act on it. The customer can't fail to act on a warning that hasn't been made.

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

We agree that the customer should take responsibility for failure to spot APP fraud when they have received clear warnings or advice that they are at risk on a particular transaction. We propose amending the list of warnings in R2(1) to include:

- Warning given by the firm's staff at a branch counter or by telephone

- Warnings given to the customer by 3rd parties with whom the customer has a relationship who had warned the customer that they had been victims to cyber attack, data loss etc. and so the customer was at risk of fraudsters using their name.

Feedback from members is that with each case, the whole scenario needs to be reviewed. For example, where firms have provided a high amount of information and education to customers about these scams, the customer should bear some of the responsibility. Vulnerable customers should also be treated carefully and be made aware when they might have been scammed for their protection

As an observation, much of the language used in this section of the Code is very legalistic – for example "recklessly sharing access ", "failure to take reasonable steps" and "not acted openly and honestly". It would be helpful to both customers and firms to set out the customer's duty to protect themselves in plainer language and to include case study examples of what these terms mean.

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 strongly support the principle that a customer in vulnerable circumstances who is less able to protect themselves against APP fraud in the manner outlined in section R2 of the Code should not be barred from receiving reimbursement because of those circumstances. We also agree that it is right for firms to have to assess cases individually and solely in the context of vulnerability to a particular incident of APP fraud. However, there is concern that vulnerability is being applied too widely:

- Where customers are repeat victims of APP fraud, where do you draw the line between vulnerability and recklessness – not all types of vulnerable circumstances justify a customer not following warnings or past experience?
- What is the relevance of vulnerability in cases where the customer is acting logically and responsibly by responding to a legitimate request to pay monies due to a known third party that are then diverted by fraudsters?
- Requiring firms to reimburse customers whether or not the firm knew of their particular vulnerable circumstances at the time is not an approach that is fair to both the firm and the customer and has the potential to open firms to claims of retrospective consumer vulnerability by individuals, unscrupulous families or claims management companies.
- Assessing the non-financial impact of an APP fraud on a particular fraud victim requires financial services firms to act as medical experts - which is an inappropriate requirement on these employees.

In terms of unintended consequences, our major concern is that this approach pushes firms to become more intrusive and interventionist with their customers and to assess vulnerability on a judgemental and legalistic basis and make value judgements on how they think the customer should have behaved. For example, the test of whether it would be "reasonable to expect the customer to have protected themselves, at the time of becoming a victim of an APP fraud,

against that particular APP fraud to the extent of the impact they suffered" is difficult to assess without an intrusive review of the customer's personal circumstance and their handling of the payment journey.

This is a significant move away from the basics of good customer support as highlighted in the FCA's Occasional Paper *"Consumer vulnerability"* and other codes of practice where an environment where customers with problems feel comfortable about raising them without being judged on how they came to be there is key. There will be severe pressure on trust between firms and customers in circumstances where keeping the customers' trust is key to supporting them through them.

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

We believe this proposal to be reasonable but the timeframe should be kept under review to ensure that it fits with real life administration of the Code. Members feel that the customer must also report the scam in a reasonable timeframe and that there should be a maximum period of which the customer must report the fraud by. The customer must respond to any requests for additional information promptly.

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

As we have previously noted we are concerned that not every building society or bank has access to Confirmation of Payee and the infrastructure required for best practice standards for responding to APP fraud – which makes them vulnerable to being particularly targeted for fraud and at a competitive disadvantage in offering fraud protection against those who do. We suspect that there will be a similar disparity of access for Network-level transaction data analytics and Economic crime information sharing.

We would like confirmation of plans to ensure appropriate access for all firms to all of the fraud prevention and response tools outlined within the Annex to the Code.

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

We agree in principle – though this premise needs to be kept under review for evidence that this is making customers reckless to fraud risk. We also support the position taken in this consultation that there will need to be a sustainable pool of funding for no fault reimbursement to back up the principle with available funds before it can be delivered on.

It also needs to be clear to consumers that reimbursement under the Code is for monies lost to fraudsters only – falling victim to high-pressure sales tactics from legitimate firms, unwise spending decisions and buyer / seller disputes are not APP fraud and there should be no entitlement to reimbursement from funds reserved for APP fraud reimbursement in these circumstances.

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 bank should not be directly liable for the cost of no fault reimbursement if it has met its own standard of care – though the above statement does imply that the sending bank has some indirect liability. We would like clarification on what the consultation's authors believe any indirect liability to be.

We also agree for the sake of simplicity and delivering a quick outcome for the customer that the sending firm should administer any no fault reimbursement where the transfer is between two Payment Services providers (PSPs,) subject to confirmation of the source of funding for these payments. However, in the building society context, this is not the usual chain of events - most building societies and smaller banks provide facilities for CHAPS transfers from a customer's savings account to a 3rd party's account with the CHAPS transfer being administered by the society's own bank. In this scenario,

In these circumstances, we would like confirmation of who should be treated as the "sending firm" - the building society where the transferred funds were taken from or the bank that provided the CHAPS facilities to make the transfer?

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?

Any funding model must take into account that PSPs and customers are not always the only parties to an APP fraud and sometimes 3rd parties can enable the fraud to take place through their failure or negligence. Often, action or lack of action by a non-bank third party is the key to the fraudster's ability to convince the customer to authorise the fraud and they should face primary liability for compensating their customer (the PSR used an example of a firm of solicitors whose lax cyber-defences created the opportunity for APP fraud).

In such cases, it should not be the role of the financial services industry to subsidise failure in other sectors nor will regulators' objective of incentivising better anti-fraud practice in future be met if non-bank parties do not have the same incentives as PSPs to improve poor anti-crime defences.

Therefore, our preference would be a contribution mechanism across all parties with an ability to prevent APP scams from occurring (option a), including redirection of fines by the ICO and other regulators for data loss, control weaknesses, failed cyber defences etc. that enabled fraud. We would also advocate diversion of recovered proceeds of crime from APP fraud to contribute to funding "no fault" reimbursement, particularly where the affected fraud victims have already been compensated under the APP Code arrangements. Fines to banks in shared blame scenarios (option e) could also feed into this fund – but only if the Code was re-drafted to account for two tier APP fraud protection.

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

As discussed previously, we are concerned that use of evidential standards for firms and consumers – particularly in respect of vulnerability will pushes firms to become more intrusive and interventionist with their customers and to have to assess their conduct on a judgemental and legalistic basis that will make the future customer relationship much more difficult. Plainer, less legalistic language might help make this process less intimidating for both parties.

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

We agree – particularly with the objective that evidential standards should be reasonable and fair to all parties involved in the scam.

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

As (unintended) two tier APP fraud protection is going to be a with us for some time, the Evidential Approach working group will have to consider the issue of different evidential standards for tier 2 firms so that their requisite level of care aligns with their lack of access to APP fraud prevention infrastructure.

Members also recommend that the payee firm evidences any CDD taken. There should also be evidence in regards any ongoing payments to further institutions.

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

All assessment of vulnerability in the context of vulnerability to an APP fraud should treated as the customer's sensitive personal data and be conducted and recorded according to the consumer privacy requirements of the General Data Protection Regulation.

There does need to be a debate on how much of the information collected is shared with other institutions subsequently – for example aggregation services and open banking product providers – though this is not an issue just for APP fraud.

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

The Payment Services Regulator (PSR) would be the most appropriate body to govern the code, given its existing position as a regulator and statutory objectives.

- The current dislocation between policy and infrastructure delivery for APP fraud prevention appears to have occurred because there was no effective central body overseeing APP fraud prevention development in the round – this situation needs to be remedied from now on. The PSR with its objective "to ensure that payment systems are operated and developed in a way that considers and promotes the interests of all the businesses and consumers that use them" is the natural body to take on formal responsibility for proper co-ordination of policy and infrastructure.
- The complexity of the evidential and dispute resolution arrangements that the code will need to have in place means that a regulator's authority is needed to oversee the mechanisms behind the code.
- The code needs a governing body with sufficient authority to deliver a level playing field of access to fraud prevention / response tools.
- As the code touches on two very significant public policy issues in financial crime and consumer protection it is important that the overseeing body has clear accountability to the supervisory authorities for the UK economy and to Parliament - which the PSR already has.
- The PSR is already established so there would be no additional set up costs required.

We agree that it would be inappropriate for UK Finance to become the Code's governing body as there is a potential conflict of interest with their core role of promoting the interest of its members. For the same reason, creating a governing body out of the membership of the working group would also be inappropriate because many of the groups involved are also advocates for a particular agenda or interest group. There is no conflict of interest in the PSR assuming this role.

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

A 50:50 apportionment of reimbursement between two PSPs at fault is a reasonable start point position in terms of simplicity and a quicker result for the fraud victim But, this should be kept under review.

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

Our members believe these principles are appropriate – subject to being adapted to handle two tier APP fraud protection. However, as regards Open Banking itself, there are some concerns: How easy would this information be access; would it be by a fee; would it be by a 3rd party provider (e.g. CIFAS, not all institutions are members of); who would be to blame if the information was hacked or the system was down?

Other questions and comments on this consultation from BSA members

Section 4.8: Once the mechanism is created, there will need to be a process in place to reassess the ongoing funding, based on the amount remaining and the reimbursement decisions made. It is likely, therefore, that the contribution levels would change periodically and we would hope that they would reduce over time as the improved levels of care reduce APP scams. How would a small firm budget for these regular changes in costs and possible changes?

Section 4.9: *Until a funding mechanism is identified, customers might not be reimbursed in the scenario where all parties have net their expected level of care under the code. Once the funding mechanism has been agreed, whether it is legally and practically possible for customers to claim from that mechanism for 'no blame' cases occurring during the consultation period will be considered. However, this may result in 'no-blame' victims of APP scams occurring during the consultation period not receiving reimbursement.* Will this result in customers – possibly assisted by CMCs - complaining and reopening old cases which were addressed before the code?

Table 2 in Annex – *Credit Flags: Individuals can be registered as not having capacity and a flag placed on their account. With this flag, if credit is applied for in their name, it will be refused and a notification delivered to the person who registered the individual.* How will banks share this information? Is this compliant under GDPR?

Table 3 in Annex – *Current practice on APP fraud statistics. App fraud statistics ae collected and provided on a monthly basis to UK Finance who in turn, publishes these on a 6 monthly basis.* No all firms are UK Finance members. There is the possibility of double reporting where the fraud involved a transfer of funds from a savings account to a current account before the final payment to the fraudster.

Other - What will be the timescales the customer has to report the fraud by? We suggest 24 hours. What is to happen if they reported it 12 months later? This would be unrealistic for a firm to investigate.

What if the customer has just forgotten what they paid for or what if it is a dispute between the customer and the payee?

How will reimbursement happen; would it be different for each institution? If an invoice is sent, how quickly is this to be paid? What happens if one institution claims to have lost it after being chased? There may be difficulties in making firms pay their share.

If one institution is slow at responding to queries or lose information, what are the next steps which can take place by the other institution who have the victim waiting?

York House
23 Kingsway
London WC2B 6UJ

020 7520 5900
@BSABuildingSocs
www.bsa.org.uk

BSA EU Transparency Register No: 924933110421-64

www.bsa.org.uk

The Building Societies Association (BSA) is the voice of the UK's building societies and also represents a number of credit unions.

We fulfil two key roles. We provide our members with information to help them run their businesses. We also represent their interests to audiences including the Financial Conduct Authority, Prudential Regulation Authority and other regulators, the Government and Parliament, the Bank of England, the media and other opinion formers, and the general public.

Our members have total assets of over £387 billion, and account for 22% of the UK mortgage market and 18% of the UK savings market.

Authorised Push Payment Scams – draft contingent reimbursement model code

Consultation paper response from the City of London Corporation Trading Standards Service and the Chartered Trading Standards Institute

14 November 2018

About City of London

The City of London Trading Standards Service is a key partner in an initiative called 'Operation Broadway' that commenced in 2014. The other partners are the City of London Police, Action Fraud, HMRC, the Financial Conduct Authority and the Insolvency Service. The objective of Operation Broadway is to disrupt the activities of investment fraudsters who are operating, or claim to be operating, in the Square Mile. Fraudsters try and use the fact that they are 'based' in the City as an indicator that they are reputable, effectively exploiting the reputation of the City of London for their own criminal purposes. The types of fraud that are seen involve the sale of items such as diamonds, wines, carbon credits, car parking spaces, and burial plots to vulnerable consumers who are promised high returns. Alternatively, consumers are offered high interest bonds in commercial property, gold mining or environmental or renewable energy schemes. The fraud is often not obvious right away because the investment returns are promised over a period of time, often years, and by the time the victim realises that something is wrong, the fraudster has already moved on.

About CTSI

The Chartered Trading Standards Institute (CTSI) is the professional membership association for trading standards in the UK. Founded in 1881, we represent the interests of trading standards officers and their colleagues working in the UK.

At CTSI and through the trading standards profession we aim to promote good trading practices and to protect consumers. We strive to foster a strong vibrant economy by safeguarding the health, safety and wellbeing of citizens through empowering consumers, encouraging honest business, and targeting rogue practices.

Consultation Response

The experience of Trading Standards Officers who speak to the victims is that they often realise that they have made an unwise investment decision. This realisation can dawn within a few minutes after making the transaction or a few weeks or months later when the victim discusses the issue with family members or friends who can see exactly what has happened. However, at the time that the original purchase decision was made, the victim is in a 'hot state', under the control of a commission hungry, well-trained, deceitful and assertive sales representative who has made amazing promises of future returns. Once payment is made by authorised push payment, it is processed by the banking sector very quickly – within a matter of a couple of minutes – and it is not possible to recall the payment if the victim has second thoughts.

Consumers are sold these investments on the promise of making fixed returns, typically in the range of 8% to 22% per annum. None of these investments are required to be regulated under the FCA regulatory regime and a large proportion will fail after a period of time. We believe that many of these are set up as Ponzi schemes from the outset with initial returns to the early investors being funded by those investing later. These schemes can sometimes run for several years before it

becomes apparent that they will fail, and consumers have no recourse to the Financial Services Compensation Scheme. The individual losses can be significant and one recent example involved a gentleman who had lost around £1.2 million over a period of years to a succession of fraudulent investment schemes.

The City of London Trading Standards Service has been suggesting a possible solution to this type of fraud for two years. The payments that the victims make are normally always authorised push payments (APPs) through their bank, either via telephone or internet banking. Trading Standards Officers from the City of London have a strong belief that the weakest point in any fraud is the point where the money passes from the victim to the criminal. Therefore, the best way of preventing any investment fraud is for the intended victim to have the opportunity to discuss the intended transaction with a family member (son, daughter, brother, sister etc) or a trusted friend. The person consulted will not be in a 'hot state' and is more likely to take an objective and rational view and question the proposed transaction and, in most cases, to be a voice of reason. What Trading Standards would like to see is the ability for a bank customer who feels that they may be at risk of financial abuse to write to their bank and state:

- They feel they may be at risk from financial abuse if contacted by high pressure sales reps
- They would like any payments to a new payee exceeding a limit (say £1000) to be delayed by 24 hours
- They would like a text/email notification to be sent to a trusted family member or friend, whose details will be supplied, when such a transaction is first attempted.

The result of such a system would allow the trusted family member or friend to contact the intended victim and discuss exactly what has happened and whether the intended transaction should be stopped. If it should be stopped, the intended victim can contact their bank within the prescribed 24 hours and the money will still be there.

This idea around delayed payments has been raised with representatives of the banking sector over the last couple of years, predominantly via the work of the Home Office initiated 'Joint Fraud Taskforce'. Whilst, in general, the idea is seen as a good one, there has been no real enthusiasm from the banking sector to implement anything or even to think about any necessary back office alterations that may be necessary to make such a system viable in the future. A victim who loses tens of thousands of pounds to an unregulated investment fraud will never see their money again and the bank has no legal responsibility for their customer under these circumstances. All that the bank has done is to execute the APP as instructed. We therefore feel that delayed payments with notification should be offered to all banking customers as an option that they can accept or decline. Where such an option is offered, this might contribute towards demonstrating that the sending firm is more likely to have met a reasonable level of care as outlined in *Figure 1* on page 5 of the consultation.

The idea of delayed payments with notification is the primary point that we would like to make to the consultation process. However, there are several comments and observations that we wish to make that we hope will be useful. These do not necessarily follow the order of the questions as set out in the consultation document.

1. It is regrettable that the aim of the Payment Systems Regulator (PSR) is to establish "better incentives" (fact sheet number 18/1) for payment service providers (PSPs) to prevent and respond to APP fraud. The PSPs could have done much more to tackle these issues many years ago, but it seems that only now, when there is a threat that they will be held liable for compensation to victims, that more positive action is going to be taken. It seems that the Which? super-complaint has been instrumental in driving change and we are pleased that things are now moving forward and that there is a real appetite to tackle fraud and protect fraud victims.

2. We feel that terminology is very important, and the use of the term "scam" is inappropriate to describe what is, in reality, often a sophisticated fraud. Someone who steals money from victims using tactics that contravene the Fraud Act 2006 and/or the Consumer Protection From Unfair Trading Regulations 2008 is committing a criminal offence. This is a fraud and not a scam.

3. We feel that the definition of 'investment fraud' in the annex could be expanded and improved. Investment fraud covers far more areas than carbon credits, land banks and wine and we think it is worth spelling these out. Investment fraud includes dealing in diamonds, burial plots, parking spaces, Christmas trees, property bonds, art works, renewable energy schemes, gold and other precious metal bonds. In addition, it needs to be clearly recognised that it is not unusual, in fact it is quite common, for an investment fraud to take several years to become apparent.

4. There is a lot of data available that seeks to demonstrate the current level of APP fraud. We feel that this crime is under-reported for a variety of reasons and the actual levels of fraud are likely to be much, much higher.

5. A key consideration to any reimbursement model will be to establish what the expected levels of care should be, particularly in relation to the victim. This is a monumental challenge and the level of care will depend on the sophistication of the fraud and the state of mind or vulnerability of the victim. As recognised at point 3.69 of the consultation, just about everyone can become vulnerable to APP fraud. The victims that we speak to are often put into a 'hot state' by the person or entity defrauding them and they exhibit behaviours that seem unbelievable in the cold light of day. This 'hot state' experience needs to be recognised when a bank customer's level of care is being assessed.

6. We have concerns that it appears that the initial decision on whether the customer has met a good level of care is determined by the firm (bank). The decision potentially has a detrimental effect on the profitability of the firm so it could be argued that it is in their own interests to find against the customer. The evidential approach is considered at point 4.10 onwards but this is going to be fundamental to the fair operation of the reimbursement model. Will the customer have to prove on the balance of probabilities that they exercised a reasonable level of care or will the burden of proof be beyond all reasonable doubt? Is it fair to expect that they carried out any checks at all, particularly bearing in mind that they are in a 'hot state' and not thinking rationally.

7. The decision on whether a firm has taken a reasonable level of care is going to be determined, in the first instance, by the firm itself and the customer will have no way of

checking the extent and thoroughness of any investigation. Many frauds rely on moving money quickly through the bank accounts of money launderers or 'mules' and the customer will have no access to evidence that proper proof of identity and proof of address checks were carried out when those accounts were opened. The fact that so much money is laundered through so many bank accounts may show that it is too easy for new accounts to be opened with minimal checks, or ineffective checks, being carried out. One latest trend is for overseas students completing their studies in the UK to sell their bank account to a fraudster and it is surely a basic requirement for banks to 'know their customer' and put rigorous auditing in place where appropriate.

8. It is recognised that the decision on whether a customer or firm has taken a reasonable level of care can be challenged by going to the Financial Ombudsman Service (FOS). Presumably this route of appeal will be made clear to the customer and it is assumed that this will not involve payment of a fee by the customer? It is likely that the workload of the FOS will increase significantly so resources need to be available. In addition, an unintended consequence of the reimbursement model might be the rise of more claim management companies that offer to assist customers on payment of a fee or payment of a percentage of any compensation. These claim management companies themselves may be involved in committing criminal offences and misleading customers in the same way that PPI has been a problem for so many years.

9. Point 3.13 of the consultation states that the code does not apply to international payments. Surely, if the customer has a UK bank account that is being used to send money to a fraudster, it is irrelevant that an overseas bank is receiving the money? Perhaps this can be more clearly defined.

10. Point 3.20 of the consultation paper raises the issue of whether a customer is defrauded or unsatisfied. Often, it is difficult to differentiate between defrauded or unsatisfied and we are concerned that this could be a barrier to reimbursement. For example, if a customer decides to purchase concert tickets from an online secondary ticket seller but is refused admission to the venue, have they been defrauded or are they unsatisfied? The secondary ticket seller may still be trading, albeit from the sanctuary of another country like Switzerland, and the assumption of the consultation is that a complaint can be made under the Consumer Rights Act 2015. However, if the reality is that the complaint is simply ignored by the secondary ticket seller, will the customer be able to make a claim under the reimbursement model? We would argue that they could.

11. There is an emphasis at point 3.26 of the consultation that firms should participate in consumer education and awareness campaigns. This already happens but we feel that these campaigns have limited impact and therefore the fact that a firm operates them should be a very minor consideration when determining whether reasonable care has been taken. Back office actions such as offering slower payments with notification (as already outlined at the start of this response), analysing unusual patterns in transactions and introducing 'confirmation of payee' should carry far more weight when determining whether a firm has taken reasonable care. It needs to be recognised that the actions of the firms in trying to prevent fraud will inevitably lead to customer complaints where there are barriers to completing instant APP transactions. Clearly firms need to be able to have a legitimate defence to any complaints where they are trying their best to prevent fraud and

have not acted unreasonably.

12. Fraudulent transactions can sometimes involve part payment by APP and part payment by credit card. Has any consideration been given to whether defrauded customers should make any initial claims against the firm that processed the APP or against the credit card company citing Section 75 of the Consumer Credit Act 1974? We feel that this needs to be clarified under the code.

13. Point 3.55 of the consultation stipulates that customers should try and make sure that the person they are paying is legitimate. This is an increasingly difficult task and is something that may not be in the gift set of every customer. Many transactions are completed remotely and there is no face to face contact between a customer and a fraudulent trader. We feel it is impossible to define the general responsibility that customers should have because it will vary depending on the circumstances of the fraud and will vary depending on the state of mind and individual characteristics of the victim. Even the act of checking whether a company exists on the Companies House website may seem to many to be a reasonable precaution but, in reality, it is meaningless due to the fact that Companies House carry out no checks on companies who register. There are thousands and thousands of fraudulent companies currently registered at Companies House, which many people may not fully appreciate. There is a massive imbalance between the resources available to a customer when compared to the resources available to a firm when investigating if a trader is legitimate. The reality, therefore, is that there is little a customer can do to make sure that the person they are paying is genuine.

14. We are pleased that at point 3.69 of the consultation it is recognised that just about everyone can become vulnerable to APP fraud in some shape or form at any point in their lives. In our experience this really is the case which makes it even more important that more emphasis is placed on firms to have effective back office systems in place to prevent APP fraud, rather than relying excessively on customers to spot and prevent it.

15. It is assumed that the reimbursement model will apply to cases where APPs are made on the internet, over the telephone AND where a customer goes into a branch of the firm to make a payment. It is also assumed that it applies to payments by cheque but this is not clarified.

16. To assist law enforcement bodies, we feel it should be compulsory for any customer making a claim against a firm in relation to APP fraud to have first reported the matter to Action Fraud and to have obtained a NFRC reference number.

17. We feel that the reimbursement model, when determined, should be compulsory and not voluntary.

18. A big challenge for the reimbursement model surrounds the issue of who should meet the cost of reimbursement. We do not feel that asking customers to purchase an insurance policy is the right way forward but one consequence of the model may be that banks start to introduce compulsory charges on customers who have an account. At first thought, this might introduce interesting theories around customers switching their accounts to those firms that have excellent security in place and therefore do not have to make a charge to

fund compensation payments. However, based on the model of domestic energy suppliers, the majority of energy customers are averse to switching suppliers and we anticipate that bank customers are even less likely to shop around and switch bank accounts. This is an important area and the Financial Conduct Authority and/or the Competition and Markets Authority would need to ensure that firms could not take a collective decision to impose charges on customers.

We feel that slower payments with notification has the potential to prevent a large percentage of fraud related to higher value transactions above the determined financial limit. However, we wish to be clear that just because a customer has declined an option for this mechanism to be in place should not automatically preclude them from successfully claiming reimbursement. There may be other elements of the fraud or the APP process that involve the firm not being able to demonstrate a reasonable level of care.

For further information, please contact policy@tsi.org.uk

City of London Police

APP Scams
Draft Contingent Reimbursement Model Code

1. The City of London Police is responding to this inquiry as the National Police Chiefs' Council Lead for Economic Crime and National Lead Force for Fraud. The City Police operates Action Fraud which takes reports of fraud on behalf of policing nationally.

2. City Police supports the principle that the code should incentivise parties involved to prevent and reduce fraud and that additional measures should be put in place to protect vulnerable customers. This should consider management of fraud aftercare to prevent repeat victimisation, safeguarding referrals or signposting vulnerable victims to support services.

3. There are numerous types of fraud, and ways of changing the modus operandi and narrative used to defraud the public. However, fraud can be distilled into 5 key enablers. These are the main routes used by fraudsters to reach victims – home telephone, internet, mobile phone, letterbox (post) and the doorstep. Telephone enablers account for a third of all reports to Action Fraud. The core prevention message for all of these frauds is to verify unsolicited contact and never assume any cold contact is genuine. Further education on the best methods for verifying this contact is also required.

4. Many people are defrauded believing they are dealing with their payment system provider / bank (PSP), as texts can be hijacked and phone numbers spoofed. Cold calling and sending links or numbers creates a culture of bad practice where customers engage and click links or call numbers to get to their PSP. A minimum prevention standard could include PSPs never including links or phone numbers in texts or emails, instead encouraging customers to get numbers from a trusted source (eg secure app or back of a card). If this was introduced PSPs could deliver a single message that they will never send a link or a phone number in an email or text. This could minimise the compromise of customer data and lower the possibility of being socially engineered.

5. It should be noted that some fraud, particularly investment fraud, is complex. It can take years before victims realise they have been defrauded, and for police to investigate and prove intent to defraud. Reimbursement decisions in these cases will be challenging to manage within the proposed timeframes. In 2017/18 over 6,000 people reported to Action Fraud that they were a victim of a type of investment fraud. While this may include victims who used alternative payment channels not within the scope of this code, estimated losses are significant. The code should provide for a consistent approach to managing reimbursement and aftercare for these victims.

6. Customers who are refunded may no longer choose to report to police. Information on APP fraud captured by PSPs should be used to inform crime reporting as well as to provide statistical information. PSPs will need to collect information on the circumstances of fraud in order to determine whether or not a fraud has occurred (the elements of false representation) and the customer should be reimbursed. Information on APP fraud should be collected to a consistent standard and systematically shared with law enforcement to inform crime reporting and investigative opportunities.

Daily Mail

Response from Money Mail

For the attention of the Payment Systems Regulator re consultation on APP fraud

Dear all,

Here at Money Mail we are inundated every week with emails and letters from fraud victims.

Scams today are so sophisticated that anyone is at risk. We regularly hear from professionals such as doctors and lawyers who have lost vast sums of money, as well as vulnerable pensioners.

As banks push customers online and close bank branches up and down the country, it is only right that they take responsibility as the front line of defence against fraud.

This means that until a final decision can be made over who funds the proposed compensation fund, they should be forced to step in and cover victims' losses.

It is not right that it is the everyday customer, who is least able to afford such losses, is left out of pocket while banks continue to rake in billions of pounds in profits.

When it comes to deciding which bank pays – the customer's bank or the receiving bank – the industry will need to consider who has made the biggest mistake.

If the customer's bank has dragged their feet over reporting the fraud or failed to spot a suspicious transaction, you could argue they are to blame.

But on the other hand, you would also need to consider whether the receiving bank has done enough to stop criminals opening or taking control of a bank account in the first place.

Banks have a responsibility to know their customer. This means they must be able to prove they carried out sufficient checks to ensure the accounts were not being opened with fake documentation or being used as mule accounts. Currently the receiving bank has no official duty of care to the victim. This means they are able to hide behind data protection rules, refusing to provide vital information about their criminal customer which could help the victim track down their money.

Given the complexities of fraud and the challenges around assigning blame, Money Mail believes it is vital that banks are held to account by a third party regulatory body or arbitrator.

When deciding if a customer has been negligent the industry needs to consider how sophisticated scammers are today.

It mustn't be the case that victims who miss a warning, such as an alert on their computer screen, are suddenly deemed to be negligent.

Fraudsters know how to manipulate people into ignoring such security measures.

For example, we often hear from readers who were told to lie to their bank about why they are transferring money because staff at the bank are supposedly in on the scam.

The industry must also take the personal circumstances of the customer into account.

Vulnerability does not just mean old people and those with diminished mental capacity.

It might mean someone who was recently bereaved, going through a divorce, redundancy or who has just been diagnosed with an illness.

Anyone dealing with large sums of cash, such as someone buying or selling a house or who has come into an inheritance could also be classed as particularly vulnerable to fraud as they are commonly targeted. It could even be argued that someone who has only just signed up for online banking and is not familiar with the risks is also vulnerable.

This does not mean customers should be permitted to behave how they like, but it should be down to banks to prove gross negligence rather than assume it from the outset.

The banking industry introduced the faster payment system but it is vital to strike a balance between speed and safety.

When people are transferring large sums of money it would perhaps be prudent to introduce a cooling off period where payments can be delayed to give customers time to check everything is in order.

Attached to this email are examples of emails we have received from readers on the topic of fraud, many from victims.

We have also included a selection of work we have published on fraud in the past couple of years which point out glaring gaps in consumer protection.

We hope this will be of use as you discuss the new code of conduct going forward.

Best,

Money Mail
Daily Mail

Response from Dudley Trading Standards (Scams Unit)

Please find below feedback on the proposed draft code. The feedback is actually from a relative of someone who has been the victim of APP fraud, resulting in the loss of his life savings. The impact of this fraud and the ongoing battle with the financial institution concerned has been devastating for not only the victim but also his family. In this particular case the bank were put on notice by the family of concerns fraudulent activity may be about to take place and despite the victim never having made a previous transaction such as this in the 50 years he had banked with them the transaction was processed. It was a classic impersonation fraud that is now being reviewed by the Ombudsman. After becoming involved in this case I am interested to see whether things do improve for victims of this fraud as it has been astonishing how the bank in this case has not accepted responsibility despite overwhelming arguments to the contrary.

One suggestion I would like to make, before you get to the feedback, is that it may be beneficial to encourage partnership working between banks and organisations such as Trading Standards. Dudley Trading Standards is in the fortunate position of having a dedicated Scams Unit. I am in no doubt that if we received a call from a local bank regarding concerns about a customer we could speak to the individual about scams and I would be very surprised if we didn't manage to make them understand they were about to be a victim of fraud, or at least prevent them from making an immediate decision to complete the transaction. I am aware that banks take customers to one side to discuss scams if they are concerned but we have found that, whether it is a bank telling a customer on a single occasion or a friend or family member over a considerably longer period, many individuals don't take this information on board for many reasons. Although we aren't necessarily telling the individual anything different to what the bank/ friend or family member would say we have found, on numerous occasions, that it makes a real difference coming from a third party. I can only see that this type of assistance, where available, would be extremely beneficial to banks and customers alike. We are actually in the process of promoting a 'hotline' number to partner organisations within our Borough to be used in circumstances such as these – it would obviously be a very positive step if banks could be encouraged to use such a resource within this code.

In addition we are concerned that financial institutions are making an assumption of mental capacity in customers who are being scammed, when these customers are often elderly, vulnerable and suffer from failing mental health. The institutions have a duty under the Mental Capacity Act to refer to Local Authority Adult Safeguarding any customer who may lack capacity and may be suffering financial abuse (ie someone with onset dementia who is being targeted by scammers). This hardly ever happens and is a major failing of duty which facilitates the scamming of elderly customers. The institutions need to understand their responsibilities and take them seriously, as failure to act increases their liability. If the institutions have reason to suspect lack of capacity (ie an elderly customer who cannot understand when something is a scam) the institution should immediately make a safeguarding referral and restrict immediate access to the customer`s account. If this was done a huge amount of scam victims would not have lost their money.

Page 5 – SF1 (1)
Expand on definition of vulnerability?
Probably too much information to be included in the document, but we would like to point out that banks need to be made aware if customers have been recently bereaved.

Page 5 & 6 –SF1 (2) – Make an audio recording of the "Effective Warning."
Banks tell us that they record Mortgage applications, so why not an Effective Warning?

Page 7 – SF1 (6) – change "should" to "must" ?

Page 9 – R1 - states that "Subject to R2, when a Customer has been the victim of an APP fraud, Firms should reimburse the Customer".
Page 4 – GF3(a) – describes additional steps that Firms could take covering "more than simple reimbursement. "
Is it unreasonable to expect similar advice and actions to be taken even if a Firm should choose not to reimburse?

Page 9 - R2 (1g)

We have concerns over Firms alone being able to assess if a customer has been grossly negligent. After our experience, we feel this would be used, regardless of whether the customer had been negligent or not, in order to avoid reimbursement. We do understand that in such an instance, the case can be passed onto the Legal Ombudsman. However, in the case of our victim, if we had not had an input, he would not have taken it further.
R4 (Page 10) – Clarify and expand "enable"

Page 12 - Payment authorisation deferred

Deferring payment for 72 hours would be a very positive step. The statement about a customer speaking to a "trusted friend or relative" could be extended to include "or appropriate agency" e.g. Citizens Advice or Trading Standards, as not everyone has a friend or relative to speak to.
Banks could retain the right to refuse to carry out a transfer of funds if they are convinced of potential fraud.

Page 12 - Credit flags for customers with lack of capacity

Could the flag tool be used further? i.e. when a family member/friend etc. raises a concern to the bank over a potential fraud, prior to it being perpetrated.

In addition, the App Scams Steering Group press release of 28/09/18 states that consumers lost £92.9 million in the first half of 2018. This should read "a known £92.9 million" as so many people do not report that they have been defrauded. As such, the stat is not at all accurate.

Electronic Money Association
Crescent House
5 The Crescent
Surbiton
Surrey
KT6 4BN
United Kingdom
Telephone: +44 (0) 20 8399 2066
Facsimile: +44 (0) 870 762 5063
www.e-ma.org

Ruth Evans
Chair
APP Scams Steering Group

15 November 2018

Dear Ruth

Re: EMA response APP Scams Steering Group Draft Contingent Reimbursement Model Code

The EMA is the EU trade body representing electronic money issuers and alternative payment service providers. Our members include leading payments and e-commerce businesses worldwide that provide online payments, card-based products, electronic vouchers and mobile payment instruments. They also include a large number of smaller Payment Service Providers, including startups. The majority of EMA members are authorized in the UK, and operate across the EU, most frequently on a cross-border basis. A list of current EMA members is provided at the end of this document.

The issues raised in this response have significant competition and policy implications for our members. Implementation of the code in its current form could in our view lead to multiple failures of smaller PSPs, who would either be unable to compete with larger PSPs with more diverse sources of income, or be the subject of multiple fraud related compensation claims – over which they have no control, and which they cannot support. To this end, we counsel against extending the code beyond the meeting of a reasonable duty of care, and against a subjective definition of vulnerability. It is better to achieve a significant but incomplete protective environment for users than to seek to protect users perfectly and in doing so degrade the product offerings, increase costs for users and decrease choice.

I would be grateful for your consideration of our concerns and look forward to continuing this work.

Yours sincerely

==========

[✂]

==========

EMA response to consultation

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

We broadly agree with the standards set out in the Standards for Firms.

However elements of the Standards are very difficult, if not impossible to implement by smaller and alternative fintech PSPs. In contrast with large credit institutions, an APP Scam reimbursement could have a significant damaging impact on the business of a smaller PSP.

On the other hand, PSPs that cannot sign up to the Code will be at a competitive disadvantage in relation to those who are able to do so, as consumers will perceive greater protection offered by larger PSPs, leading to the contraction of the market for smaller PSPs, less choice for consumers, and fewer low cost services.

We regard this as a significant anti-competitive issue, and whilst we accept that a duty of care to alert a customer with regard to a possible scam can exist, that a consequent reimbursement may be desirable, and that our members may wish to participate in such a code, we have serious concerns and objections with regard to the extent and circumstances of compensation. We do not accept that a wider compensation obligation arises in the different circumstances contemplated by the standards, nor that the PSP which is in no way responsible for the fraud, should be uniquely placed in the role of insurer or arbitrator.

This is exacerbated by the fact that the fraud takes place entirely outside of the domain of the PSP, and the PSP does not have any statutory investigative powers nor the know-how or resources to discover the nature or merits of the claim. This is entirely a matter for law enforcement and for government led action.

It is noted PSPs who are members of the EMA are principally specialist payment providers who are proscribed from lending the funds of users, and therefore are restricted in the income that they generate to transaction related income streams. As an example, if the total revenue generated by a PSP was in the region of 1% of the value of a transaction, from which its cost of doing business must be extracted, it would have to process at least 100 equivalent size transaction to recover the loss on a single claim of fraud. Once the costs of doing business are taken into account, this is likely to increase to perhaps 1000 or transactions. There are other sources of fraud, and other costs that also have to be borne. The impact on small PSPs may very well be catastrophic.

In the response that follows, we have commented on the provisions in more detail.

Separately, it is in the interests of all parties, particularly UK consumers, that an appropriate Code is widely adopted and results in a significant reduction of APP Scams. Careful consideration needs to be given to ensuring that the Standards for Firms or related evidential requirements are not so prescriptive that they result in lower rates of adoption of the Code by PSP's.

In particular, non-Bank PSP's should be able to commit to and comply with the Code without a mandatory requirement to participate in other industry codes, data sources, technologies etc which require financial commitments to participate in and/or significant operational integration

resources. For example the EMA believes that it is desirable that a start-up Fintech PSP commits to the code from launch without having to become a CIFAS member provided that it has effective on-boarding fraud controls in place.

Specific comments:

a. General Principles for Firms: GF

A PSP's ability to ensure compliance with GF 1(a) may be challenging where the PSP works with many different partners such as programme managers, who would be responsible for designing and running any educational or awareness-raising project. This is a common business model for card based e-money issuers. It may be difficult for the PSP to ensure compliance by partners with their educational obligations at *all times*, so we propose that for the purposes of an APP Scam reimbursement decision, compliance with GF 1(a) is a relevant consideration only for the programme under which that particular APP Scam has taken place.

b. Standards for firms:

SF1

We agree that firms should take reasonable steps to protect their Customers from APP fraud. However we do not agree with the requirement that firms provide a greater level of protection for customers who are considered vulnerable to APP fraud. PSPs mostly hold very little personal information on their customers, making it almost impossible to make a judgement regarding their customers' vulnerability to APP fraud. Staff of EMA members do not hold appropriate levels of training to be able to judge whether a customer is vulnerable to APP scams or not. This issue may be even more acute for start-up Fintech PSP's. It is therefore very unlikely, or in some cases impossible for a PSPs to provide a greater level of protection for customers considered vulnerable to APP fraud. It is more appropriate for PSPs to defer such a judgement to the FOS and reimburse customers retrospectively than to take on such a role themselves.

It is specifically troubling that the code suggests that PSPs identify vulnerability with respect to APP Fraud; an impossible task given the breadth of fraud hat is covered, the limited engagement with customers, the skillset of PSP staff as well as privacy and customer expectations.

We propose the deletion of the text below:

"Sending Firms should take reasonable steps to protect their Customers from APP fraud. This should include procedures to detect, prevent and respond to APP fraud. ~~Procedures should provide a greater level of protection for Customers who are considered vulnerable to APP fraud."~~

SF1(1):

PSPs conduct transaction-based analytics as a matter of course, and often use artificial intelligence to improve their systems. However, the reference in SF(1) to firms not only identifying payments, but also **customers,** that run a higher risk of being associated with APP Fraud is very difficult to implement in practice, as it is highly subjective, and relies on a much greater amount of data held on customers than alternative/smaller PSPs currently hold. Communication by alternative/fintech PSPs with the customers is primarily online, and often for one-off or occasional transactions, so they do not have the same one-to-one interaction over a phone or face-to-face that a high street bank might have. The nature of products that alternative/Fintech/smaller PSPs offer mean that customers are usually not willing to volunteer more than the basic mandatory information necessary to open the account and perform the transaction. Even in relation to online data, alternative PSPs may not have historical payment data, or information on other financial products held by that customer. The only data in this regard that a fintech PSP is likely to hold is where that customer has previously been victim to an APP scam with that same PSP.

This requirement will lead to PSPs being held liable for information they don't hold. E.g. a Payment I*nitiation Service Provider (*"PISP") offering services to a fintech providing person-to-person payment services will hold no information whatsoever to perform anti-fraud analytics (the fintech would potentially have the information in this case)

In the case of programmes targeting vulnerable consumers, such as the elderly, unbanked, or immigrant communities, the expectation could be very different. However in general it will be extremely difficult for PSPs to identify consumers that are more at risk of becoming a victim to an APP scam.

We therefore propose to remove the word "customer" from SF1:

"Firms should take appropriate action to identify ~~Customers and~~ payment authorisations that run a higher risk of being associated with an APP fraud"

SF1(b)

We propose the following minor amendment:

"Firms should train their **relevant** employees…"

SF1 (2)(c)

We agree that warnings should be risk-based. However this should not preclude firms from

issuing warnings to all new customers, for example, or for all new payees.

We are also supportive of solution driven warnings, and other controls like Confirmation of Payee (CoP) that will educate consumers and drive down the incidence of APP scams.

A key point to note in all the standards is that any effective warning loses efficacy if consumers are aware that they will be reimbursed regardless of their own actions. We do not expect a significant reduction in incidents due to customer due diligence if a no blame scenario is introduced. We are therefore opposed to a no-blame-no-blame reimbursement scenario.

Reimbursement of users in all circumstances simply puts money in the hands of fraudsters, provides no disincentive to users, and incentivises fraudsters to continue this practice.

SF1 (2)(d)

The guidelines must be payment channel neutral, and not require firms to suggest using a competitors service or a more expensive payment method. Many consumers will be paying via a channel that is specifically requested by the payee. It is for example expensive for small businesses to accept card payments, if these are the proposed alternative. It is also expensive for PSPs to fund chargebacks for card payments. This suggestion does not contribute to a shift in consumer behaviour towards making safer bank transfers, or to reduce the incidence of scams. It goes against the guiding principles of the steering group, to mitigate the risk of payment by bank transfer rather than to disincentives the use of this payment method.

Effective Warnings should focus on effective customer due diligence -- which is the key driver of much APP fraud.

SF1 (2)(e)

We agree with the provisions in relation to effective warnings. However we note that there may be a conflict between the amount of information expected to be presented to the customer in SF1 (2)(c), SF1(2)(d) and SF1(2)(e)iii, and the requirement that the warning be "impactful". If presented with too much information, consumers may just wish to click through without reading any of it. For example for app-based products, a quick and simple pop-up will be impactful but may not include all the recommended information set out in the Code.

SF1 (2)(e)v

For the reasons detailed above in relation to identifying vulnerability, we propose the following amendment, as the PSP may not have any data to categorise the customer type:

"Specific – tailored to the ~~customer type and the~~ APP fraud risk identified by analytics during the Payment Journey, and/or during contact with the Customer."

SF1 (4)

Vulnerable customer identification: we can use information such as age to determine if someone is higher risk, but questions of someone's financial capability are unknown without making arbitrary judgements and using invasive techniques. A third party, like the FOS, would be better equipped to judge a consumers vulnerability objectively and fairly, thus sparing consumers the requirement to share intimate information with their PSP. Such vulnerability should however be defined in an absolute sense and not in relation to each type of fraud or scam – that is an impossible requirement that cannot be delivered by any third party, perhaps even family members.

How would a PSP know if someone is vulnerable to a Romance scam? Or how is vulnerability to a purchase scam quantifiable?

For clarity, we are strongly against proposals that involve the PSP seeking sensitive user information that is unrelated to their business relationship with the PSP, or of encouraging PSPs to make value judgements about users.

We propose deletion of the APP Scam subjective element of vulnerability. Vulnerable customers in an absolute sense, can make themselves known to the PSP, who could then make provisions for a more appropriate delivery of the service. Otherwise, the FOS is able to address issue of vulnerability.

Application to PISPs: for clarity, these provisions should not apply to a PISP that has no knowledge of the payer, but would apply to the payer's account holding PSP.

SF1(4)(c)

The Code should not mandate PSP's to participate in other non-public codes such as BSI PAS 17271 as this is a costly exercise that is not required by financial services regulation; it would therefore likely reduce participation of non-Bank PSP's. We suggest the following change:

"industry standards, **for example** BSI PAS 17271"

SF1 (5)(a)

Whilst we understand the rationale behind the desire for firms to be able to delay payments, PSPs offering push payments are undertaking to execute immediately. This is set out in the PSRs, Guidance, and also in payment scheme rules. A firm that delays a payment for any reason other than a legal requirement will be taking on a significant risk.

This requirement places smaller PSPs at a disadvantage, as they are not resourced to provide 24/7 service. Large banks are able to take a risk-based approach towards blocking transactions, then calling the customer to check (or expect the customer to call the bank). However smaller PSPs cannot provide this level of customer service, so are unlikely to block transactions. The emphasis in the Code should be on effective warnings rather than an expectation that PSPs delay or block transactions.

If this provisions is carried, then further regulatory guidance on delaying payments that would consider all participants would be required.

Impact on PISPs: it is not generally technically possible for a PISP to delay an immediate payment for a significant amount of time.

SF1 (6)

The **Best Practice Standards** are helpful, but provide an additional layer of compliance; consideration should be given to making adoption of BPS non mandatory.

SF2(1)(a)

Non-Bank and Fintech PSP's often use sophisticated techniques of CDD. It is important that any evidential expectations are broad and capable of accommodating differing means of risk based

CDD.

When proving compliance with SF(1)(a) PSP's are restricted in the information that can be provided to the Sending Firm. An arbitration process is needed to facilitate this.

SF(1)(b)

For non-Bank and Fintech PSP's it is critical not to mandate participation in Bank led data sources such as CIFAS, and others. This will reduce participation in the Code and will be regarded as an anti-competitive provision by our members. We propose the following amendment:

"Firms should use available shared intelligence sources and industry fraud databases **or deploy other effective techniques** to screen Customer accounts..."

SF2 (3)(b)

We agree that firms should train employees involved in transaction monitoring to identify transactions at higher risk of being associated with an APP Scam. However not all staff need to be trained in this way. We propose the following amendment:

*"Firms should train their **relevant** employees on how to identify indicators of circumstances around, and leading to, transactions that are at higher risk of facilitating APP fraud."*

SF2(4)

As stated above, it should be possible for non-Bank PSP's to comply with the Code without mandating full Compliance with the Best Practice Standards in order to maximize adoption of the Code.

SF2(5)

Repatriation should be to the Sending Firm and not the Customer. Clarification on the arrangements when the Sending Firm does not participate in the Code would be helpful.

SF2 (5) (a)

PISP impact: please note that a PISP which is purely initiating payments cannot freeze any funds as they never pass into the PISP's bank accounts. Therefore, these obligations can only apply to banks and other ASPSPs.

R1

The provisions on residual risk/no blame scenario are currently expressed in the draft code (R1) as being reimbursed by the PSP, along with other circumstances giving rise to reimbursement.

However the Consultation Paper (see paragraphs 4.3 and 4.4) states that in the "no-blame" scenario, PSPs may *administer* a refund, but not that they would be expected to reimburse from their own pocket. The conditions at R2(a)-(g) do not currently distinguish no-blame as an exception to reimbursement. We propose to include "no-blame" in the list of exemptions from reimbursement, and then later include a statement that in the case of no-blame, PSPs can administer a reimbursement from another source (amending R3).

"*The Firm has met the standards expressed in the Standard for Firms, and the Firm cannot establish any one of the manners described in R2(1) (a) to (g) has occurred through an act or omission of the Customer."*

This then leaves the opportunity for the PSP to *administer* the reimbursement on behalf of a third party, to simplify the process for the consumer.

A provision can be made at R3 with a new paragraph (3):
"*(3) Once the firm has received confirmation of the bona fide nature of the claim from [the police], and has received payment from [the designated fund], it can assist by administering the reimbursement.*"

As the PSP has no investigative powers outside its own business relationship, and as the scam draws in other parties and activities, the role of investigating to ensure there is no first party fraud needs to be undertaken by a third party entity with such powers, such as the police.

R2(1)(g)

Guidance is required on how "grossly negligent" will be interpreted. Clear examples would be helpful

R2(3)

As set out earlier:

(i) It will be extremely difficult for all PSPs and particularly smaller PSPs to enquire of information required to assess vulnerability In relation to a particular type od scam

(ii) It is impossible to conceive of a means by which a PSP could determine from their interaction with a customer whether such vulnerability exists, other than in absolute terms, where a customer notified the PSP.

(iii) Even attempting such a feat would involve unacceptable intrusion into the lives of customers, and a skill set that is closer to psychology than to payment service provision, and resources that are not available.

(iv) There are considerable public policy implications in the field of privacy and personal data that would also merit consideration.

Impact on PISPs: note as PISPs do not come into funds, they should not be expected to administer or reimburse funds.

R4

We agree with the sentiment of R4, that the customer have access to redress as quickly as possible, we believe it is in the interests of customer, PSP and the FOS that due process is followed and a complaints process completed with the PSP before the customer approaches the FOS. This will ensure that the PSP is able to complete all internal investigation, and will reduce the workload for both the FOS and the customer when it comes to adjudicating the case.

FOS charging process: there is concern regarding the suitability of the current FOS charging process for complaints that originate from compensation claims arising from APP Scams. The current FOS process involves the firm paying a fee of £550 in relation to the administration of a complaint irrespective of whether the FOS finds in favour of the firm or against it.

This could create a de facto threshold of £550, below which it would be uneconomical for PSPs to refuse claims, even if they are unfounded or where the user has been grossly negligent.

We propose the following changes to the wording:

"Where a Customer has received a negative reimbursement decision ***and complained****, all the Firms involved will take all reasonable steps to* ***accelerate their internal complaints process 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 ***as soon as possible***.

Furthermore, the FOS should give serious consideration to suspending the application of their fee, where a complaint is manifestly without merit, and the complainant to have pursued the complaint only as a means of forcing the firm's hand. This would be akin to the current treatment of vexatious complaints.

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 support the proposed provision in full, and do not believe it creates an incentive for firms to avoid reimbursing eligible victims. Its intention is not to create a loophole, but to introduce a natural balance to the Code.

The Code should incentivise PSPs to prevent APP fraud. It is reasonable to expect a PSP to reimburse the customer where they could have taken steps under their duty of care set out in the Code that would have prevented the scam from occurring. However, where the non-compliance has no bearing on whether or not the scam would have taken place, for example with GF(3) on customer aftercare, this should not lead to the firm being expected to fund the reimbursement to the customer. It is difficult to understand the rationale for applying irrelevant facts to justify liability/blame. Otherwise the Code simply creates an insurance policy penalising PSPs.

In any case, under the Code, "eligible" victims (i.e. victims considered to have met the Customer Standard of Care) will be reimbursed, whether by the PSP or the "no-blame" fund.

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.

This will depend on the factors of each case.

For example, the duty of care would serve an end only if the customer is not grossly negligent. If he is, it would make no difference, and the PSP should not be required to send any money to the no-blame fund. Given fraud is perpetrated on the customer by a third party, the shortcoming is in detecting it, not a shortcoming that caused it. If a customer is reimbursed in such a case, they are not encouraged to take care the next time.

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

Yes we agree customers should take these steps to protect themselves.

We propose elaborating on the standard consumers would be expected to meet, and to set out such guidelines and expectations in relation to 'too good to be true' offers or 'well known scam scenarios' etc.

We propose to amend R2(1)(d) to add: "and/or take reasonable steps to validate that a payment does not reasonably relate to a scam or fraud"

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 do not agree with the suggested approach to customers vulnerable to APP scams.

The broad definition of vulnerability leads to an obligation to collect a wide range of data from customers to establish the degree to which they may be vulnerable, and more specifically, vulnerable to APP Fraud.

Whilst asking for information on background, physical and learning difficulties, financial status, and financial understanding may be possible when opening a bank account, it is unlikely to be regarded as reasonable or proportionate when signing up to a single use payment product. Most e-money or payment institution accounts are specific in nature, and users are not likely to contemplate a lengthy sign-up process, or to be minded to share such information. Even if collected, there is no obvious link between fraud typologies and individual customers, except in the broadest sense; certainly not as a subjective judgement in the context of different types of frauds,

This is again particularly detrimental to the business of alternative banking PSPs who tend to provide products on Mobile Apps, a key differentiating factor from traditional banks.

The definition of vulnerability should therefore be objective in broad terms (eg. a person with learning difficulties, or elderly or disabled in some manner) and not subjective to the particular fraud typology. Furthermore, the interpretation of the vulnerability could be product specific as well as user specific, so that PSPs could only be expected to solicit such information as would be reasonable in the context of their relationship with the user.

More extensively utilised products would canvass more information whilst single use products would warrant less. Provision should be made for PSPs to develop knowledge of customer behaviour over a period of time, and they should not be penalised for not collecting personal information at or immediately after onboarding.

For ease of reference, we have repeated below, points made on this issue in commentary on provision R2:

(i) It will be extremely difficult for all PSPs and particularly smaller PSPs to enquire of information required to assess vulnerability In relation to a particular type od scam

(ii) It is impossible to conceive of a means by which a PSP could determine from their interaction with a customer whether such vulnerability exists, other than in absolute terms, where a customer notified the PSP.

(iii) Even attempting such a feat would involve unacceptable intrusion into the lives of customers, and a skill set that is closer to psychology than to payment service provision, and resources that are not available.

(iv) There are considerable public policy implications in the field of privacy and personal data that would also merit consideration.

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

Yes the timeframe of 15 days is appropriate in most circumstances, with an extension to 35 days where the PSP communicates to the customer.

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 agree with the measures included in the Annex. However we propose that the reference to the BSI Code of Practice be moved to the Annex, not the Code itself, as it is not a public document. It is not clear why this document should be included in the Code, whilst other reference documents are inserted in the Annex.

We note that some tools may require more time and resource to be implemented for smaller/alternative/fintech PSPs. For example, PSP business models that involve numerous partnerships such as with programme managers, who would be responsible for designing and running any educational or awareness-raising project. This is a common business model for e-money issuers. Allowance for some variation should be made, and each programme should be considered separately.

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 agree in principle; with two significant caveats.

The consumer level of care needs to be defined in a reasonable manner, that does not offer reckless individuals the opportunity to avoid responsibility, or a safety net for taking chances that would not otherwise have been taken. This would result in an acceleration of fraud, in users opting for 'too good to be true' opportunities etc. The position in relation to pyramid schemes for example is also worthy of specific consideration, as it could give rise to widespread and system claims.

For clarity, where a PSP has met their level of care, the reimbursement should be funded from a third source, and NOT from the PSP. Furthermore, no PSP should be expected to provide liquidity or interim payment in this regard. This is particularly important in relation to smaller PSPs.

We also object to proposals for industry funded sources of reimbursement in such scenarios, and warn against any such proposals that act as an anti-competitive provision, favouring larger and better funded institutions – please also refer to 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?

We cannot agree to this while there is uncertainty on key issues:

- How will the firm know that a user is eligible and not party to a first party fraud. It has no investigative powers, so what can it do to mitigate this risk?
- Given that it is not paying from its own funds, what process is there to implement controls over this process
- Is the firm the final arbiter or will its judgement be reviewed?

These issues need to be elaborated before a view on this can be reached.

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 do not support any form of PSP funding for the reimbursement of customer funds in a "no-blame" scenario.

The consequence is that PSPs will in effect provide an underwriting service for APP Scam fraud, offering compensation even if no fault can be shown (i.e. in the "no-blame, no-blame" scenario). For example, a failure in the security of an accountancy firm that allows hackers to substitute fake payment details, or poor oversight by a dating web site that allows scammers to perpetrate

widespread 'romance fraud' etc. would be regarded as shortcomings to be attributed to the PSP even if the PSP has met its requisite duty of care, detecting, preventing and responding to such risks.

This is inappropriate for a number of reasons: (i) it is contrary to the expectations of natural justice where compensation would be expected to flow from fault (ii) it creates a disincentive for third party actors who have the ability to reduce such risk – such as the accountants and dating web site providers in the above examples, to act to reduce the risk; (iii) it encourages fraud by providing victims with compensation in almost all circumstances, and (iv) it leaves the underlying fraud problem, a law enforcement and government policy matter, unaddressed. This would also create a disadvantage for alternative/smaller PSPs, who have less ability to absorb additional costs than large banks, and would need to pass the costs on to consumers, thus making their product less attractive.

We see a clear distinction between compensation that is triggered by PSPs failing to meet a duty of care, and one that amounts to an insurance scheme for all APP Scam Fraud; and we ask that the ASSG make a similar distinction, and restrict compensation to the former.

It is not in the interests of users, whether consumers or businesses to address fraud risk through underwriting; it simply shifts the cost of the fraud back to users who will have to pay through higher fees, and fails to address the vulnerabilities in the ecosystem that give rise to the fraud in the first place.

We support a government-funded scheme, as this would incentivize the government to bring all relevant parties together to address the issue.

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

It will be difficult for the Financial Ombudsman to judge compliance with the Code in many cases, for example in relation to the transaction risk analysis conducted by a firm. We propose that FOS staff dealing with these complaints receive specially targeted training in coordination with the FCA, PSR and industry.

This should be transparent, should reflect a broad cross-section of industry, and should also result in an output that can be used to inform consumers and increase their awareness.

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

Yes we agree. We do however stress the need to ensure that evidential requirements are not slanted towards larger institutions such as large Banks so that they present a barrier to entry or significant operational challenge for smaller PSP's with different operating and business models.

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

Staff of EMA member firms do not hold appropriate levels of training to be able to judge whether a customer is vulnerable to APP scams or not. It is beyond the usual remit of a PSP's role to ascertain the level of vulnerability to an APP Scam.

Vulnerability should be defined objectively, and users encouraged to make such needs know. Other approaches result in unreasonable demands on firms and their staff, as well as unacceptable intrusion on customers.

Once vulnerability is defined objectively, users will also be able to rely on the judgement of the FOS where they fail to implement appropriate measures, and result in a failure of their duty of care.

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

We do not agree with the suggested approach to customers vulnerable to APP scams.

We agree that firms should take a more sensitive approach towards customers considered to be vulnerable during an investigation, and where there are programmes or products specifically designed for groups that are vulnerable.

However the broad definition of vulnerability leads to an obligation to collect a wide range of data from customers to establish the degree to which they may be vulnerable, and more specifically, vulnerable to APP Fraud. Whilst asking for information on background, physical and learning difficulties, financial status, and financial understanding may be possible when opening a bank account, it is unlikely to be regarded as reasonable or proportionate when signing up to a single use payment product. Most e-money or payment institution accounts are specific in nature, and users are not likely to contemplate a lengthy sign-up process, or for the PSP to solicit such detailed personal information. EMA members also express a high level of discomfort at making such a judgment, and staff are not trained appropriately to be able to do so. It is therefore very unlikely that a PSP will be able to evidence compliance with a requirement that firms provide a greater level of protection for customers considered vulnerable to APP fraud. PSPs are more to defer such a judgement to the FOS and reimburse customers retrospectively than to take such a role on themselves.

The evidence required of PSPs to demonstrate treatment of vulnerable customers should therefore be product specific as well as user specific, and PSPs should only be expected to solicit such information as would be reasonable in the context of their relationship with the user. More extensively utilised products

would canvass more information whilst single use products would warrant less. Provision should be made for PSPs to develop knowledge of customer vulnerability over a period of time, and they should not be penalised for not collecting such information at or immediately after onboarding.

Please also refer to our response to Question 5.

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

Of the options set out in the Consultation Paper, Pay.UK appears to be the most appropriate body. However we note that there is very little to no representation of the alternative/small PSP view in the Pay.UK governance structure. Smaller providers are unable to deploy resources into such institutions and rely on their trade body for representation. The EMA is ready to discuss options in this regard.

In relation to management of the ongoing governance of the Code, we propose that – as the obligation to identify customers who are considered to be vulnerable to APP Scams is likely to be impossible for most alternative or small PSPs, and is the least tangible measure to introduce – this provision is removed from the initial CRM Code. The FCA is expected to consult on Guidance on their expectations in relation to the treatment of vulnerable consumers in early 2019. Once this Guidance has been adopted, it may inform the requirements set out in the CRM Code, leading to a Code that is achievable for smaller/alternative PSPs.

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

A review after a year seems reasonable, with regular reviews every few years thereafter. A further review should also be undertaken prior to PISPs being brought within scope.

In relation to management of the ongoing governance of the Code, we propose that – as the obligation to identify customers who are considered to be vulnerable to APP Scams is likely to be impossible for most alternative or small PSPs, and is the least tangible measure to introduce – this provision is removed from the initial CRM Code. The FCA is expected to consult on Guidance on their expectations in relation to the treatment of vulnerable consumers in early 2019. Once this Guidance has been adopted, it may inform the requirements set out in the CRM Code, leading to a Code that is achievable for smaller/alternative PSPs.

In relation to entities that may be permitted to propose changes to the Code, this should not be limited to signatories. There may be entities that wish to sign up to the Code, but are unable to do

so due to provisions that prevent their being able to comply. They should also be offered the opportunity to propose changes to the Code. This will encourage wide adoption of the Code.

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

Yes this is appropriate.

However, as set out in SF of the Code, where the compliance with that standard would not have had a material effect on preventing the APP fraud that took place, PSPs should not be expected to bear 50% of the cost.

The Code should incentivise PSPs to prevent APP fraud. It is reasonable to expect a PSP to reimburse the customer where they could have taken steps under their duty of care set out in the Code that would have prevented the scam from occurring. However, where the non-compliance has no bearing on whether or not the scam would have taken place, for example with GF(3) on customer aftercare, this should not lead to the firm being expected to fund the reimbursement to the customer.

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?

Yes these ADR Principles are appropriate.

As the Open Banking dispute management and arbitration process has been agreed amongst the CMA9 (and participating Third Party PSPs), this may be an appropriate starting point for disputes in relation to the APP scams process. The OB process is also intended to complement procedures adopted for FOS complainants so as to minimise impact on participants.

However, we note that the OB dispute management process is untested as yet.

We also note that the CMA9 members of the OBIE are currently funding the operation of the Dispute Management System process, and that the costs for individual cases that are referred for mediation/adjudication are to be apportioned equally between parties.

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

We note that the OB dispute management process is untested as yet. There is a risk that there are issues that will not be identified until the process is used.

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?

The requirements set out in the Code on PSPs in relation to identifying those vulnerable to APP Scams may lead:

- To consumers being labelled as "vulnerable" and perhaps not having access to services they might otherwise access.
- Fintechs to avoid taking on customers who are considered vulnerable to APP scams (if this is possible to identify at the outset at all).
- PSPs to begin asking intrusive personal questions when onboarding new customers

Furthermore, there is no Reasonable manner in which customers can be rationally labelled as vulnerable to different types of frauds, except in the a broad objective sense. The elderly may be vulnerable to fraud generally etc.

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 quantum of compensation that is being proposed by the CRM is not calibrated to the shortcomings that gave rise to the loss, nor is it proportionate to the income that is derived by the PSP from transactions. This is a matter for concern in itself, but is of critical concern for smaller PSPs and in particular to Payment Institutions and Electronic Money institutions who offer specialist payment services, usually prepaid or 'pass through', and who do not derive a supplementary income from other financial products that attach to an account such as overdrafts, personal loans, insurance etc.

The income derived by EMA member institutions is usually restricted to that from the payment service itself, and will be limited in scope. It may be a fixed amount that is not related to the transaction size, or it may be a percentage, usually significantly less than 1% of the value of the transaction.

User compensation however is proposed for the entire principal value of the transaction. This means that when compensating a single transaction of £100, it will likely require 100 legitimate non-fraudulent transactions of the same value to be processed in order for the PSP to recoup the cost of the compensation that was paid out – assuming for simplification a 1% transaction income.

The position in relation to certain alternative banking solutions, where EMA member PSP's support Fintech Client/Programme managers, is even more acute as the PSP average revenue for these types of programmes can be in the order of 5 basis points so an APP Scam of £5,000 would have generated revenue of £2.50. Compensation of the principal value would require 2000 legitimate transactions to recoup the compensation.

It is important to also note that APP Scams can be operated by highly sophisticated origanised criminal groups that specifically and aggressively target a particular group of users (this happens by analogy to different types of PSP). As such small and market entrant PSP's could be effectively driven out of business due to compensation payable in relation to quite a short period of time during which the PSP mitigates the specific targeting and prevents further APP Scams.

This can happen irrespective of the strength of controls in place as organized crime groups can be highly innovative. The pattern is then that the APP Scam migrates to another user group that may be attached to another PSP. Non-Bank PSP's are far less able to cope with the Compensation relating to such targeting APP Scams than Banks due to their business models and length of trading during which reserves are built up.

In the absence of other revenue streams, smaller PSPs will be disproportionately impacted by the proposed Code, and their ability to compete as specialist payment service providers will be adversely impacted.

The impact is particularly acute for non-bank PSPs providing innovative alternative banking solutions in direct competition to traditional banks as specifically envisaged by PSD2. The business models of these organisations and cost structures are entirely different from traditional banks. An underwriting type compensation model is likely to drive many organisations out of the market for banking services and represent a highly significant barrier to entry for potential new participants.

We therefore ask for more time to be taken by the ASSG to develop a more nuanced approach to user compensation that is fair and effective for all parties concerned.

The cost of compliance with the Code is disproportionately higher for smaller/alternative PSPs, and the costs of not complying also significant in terms of lost business. Smaller PSPs will essentially be caught between a rock and a hard place. For example, the data that PSPs are being asked to collect in order to assist in the determination of whether a customer is vulnerable to an APP Scam may easily fall within the definition of "sensitive personal data" under the General Data Protection Regulation. This type of information would require significant overheads to collect,

store and process, even if it could actually be applied for the purpose for which it is being collected. We believe the objective is untenable.

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

The requirements set out in the Code on PSPs in relation to identifying those vulnerable to APP Scams may lead:

- To consumers being labelled as "vulnerable" and perhaps not having access to services they might otherwise access.
- Fintechs could avoid taking on customers who are considered vulnerable to APP scams (if this is possible to identify at the outset at all).
- PSPs would be required to ask intrusive personal questions when onboarding new customers
- An unrealistic expectation that sensitive personal data could enable PSPs to predict vulnerability in relation to specific fraud typologies

If PSPs are required to fund the cost of "no-blame" reimbursement payments, smaller PSPs may not be able to compete with the larger counterparts, and ultimately the wider body of consumers will shoulder this cost.

Onerous obligations and evidential requirements which are not suitable for non-Bank PSP's will adversely impact such PSPs; FOS decisions based on compliance with these requirements will exacerbate the problem and the ultimate outcome could be an environment that reduces consumer choice and increases costs to consumers.

We counsel the reviewers to consider our submission carefully and to take the points made seriously. It is better to achieve a significant but incomplete protective environment for users than to seek an overly ambitious arrangements that cannot be achieved in practice and that undermines the positive results that have emerged.

Q23 How should the effectiveness of the code be measured?

The effectiveness of the Code can be measured be collecting data in relation to SF1 and SF2, and comparing it to similar data in one year, and on an ongoing basis thereafter. Specifically:

- Total value and volume of APP payments
- Proportion (by volume and value) of APP payments that were scam payments
- Of those scam payment, % of payments (volume and value) where the funds were frozen and repatriated.
- Number of claims made, divided by reimbursement outcome
- Categories of firms in each case should also be shown

This data could be separated into payments sent and payments received in order to determine the relative effectiveness of the requirements for sending and receiving PSPs.

It could also be separated by type of scam according to the scam types set out in the Annex to the Consultation Paper. This would allow for tracking of fraud trends.

List of EMA members as of November 2018:

Airbnb Inc
Allegro Group
American Express
Azimo Limited
Bitstamp
BlaBla Connect UK Ltd
Blackhawk Network Ltd
Boku Inc
CashFlows
Circle
Citadel Commerce UK Ltd
Coinbase
Corner Banca SA
Curve
Ebanx
eBay Sarl
Epayment Systems Ltd
Euronet Worldwide Inc
Facebook Payments International Ltd
First Rate Exchange Services
Flex-e-card
Flywire
GoCardless Ltd
Google Payment Ltd
IDT Financial Services Limited
Imagor SA
Intuit Inc.
Ixaris Systems Ltd
Merpay Ltd.
MuchBetter
Mypos.eu
Nvayo Limited
One Money Mail Ltd
Optal
Ozan
Park Card Services Limited
Paybase Limited
Paydoo
Payoneer
PayPal Europe Ltd
PayPoint Plc
Paysafe Group
PPRO Financial Ltd
PrePay Solutions
QIX Ltd
R. Raphael & Sons plc
Remitly
SafeCharge UK Limited
Securiclick Limited
Skrill Limited
Starpay Global Ltd.
Stripe
Syspay Ltd
Transact Payments Limited
Transact24 (UK) Ltd
TransferMate Global Payments
TransferWise Ltd
TrueLayer Limited
Trustly Group AB
Uber BV
Valitor
Vitesse PSP Ltd
Viva Payments SA
Wave Crest Holdings Ltd
Wirecard AG
Wirex Limited
Worldpay UK Limited
XCH4NGE LTD

FRAUD ADVISORY PANEL

FRAUD ADVISORY PANEL REPRESENTATION 08/18

RESPONSE TO THE AUTHORISED PUSH PAYMENT SCAMS STEERING GROUP ON A DRAFT CONTINGENT REIMBURSEMENT MODEL CODE PUBLISHED ON 28 SEPTEMBER 2018

The Fraud Advisory Panel welcomes the opportunity to comment on the consultation published by the Authorised Push Payment Scams Steering Group (the 'Steering Group') on the draft contingent reimbursement model code on 28 September 2018, a copy of which is available from this link.

This response of 15 November 2018 reflects consultation with the Fraud Advisory Panel's board of trustees and interested members who are counter-fraud professionals and financial crime specialists from all sectors. We are happy to discuss any aspect of our comments and to take part in all further consultations on the issue of authorised push payment fraud.

CONTENTS **PARAGRAPHS**

The Fraud Advisory Panel (the 'Panel') is the UK's leading anti-fraud charity.

Established in 1998 we bring together counter fraud professionals to improve fraud resilience across society and around the world.

We provide practical support to almost 300 corporate and individual members drawn from the public, private and voluntary sectors and many different professions. All are united by a common concern about fraud and a shared determination to do something about it.

For more information, please contact info@fraudadvisorypanel.org

www.fraudadvisorypanel.org

INTRODUCTION

1. We believe that there need to be better incentives for firms and customers alike to reduce APP fraud insofar as possible and to make it harder for fraudsters to succeed. Our goal should be to create a realistic and practical solution to a growing and costly problem that is in the interests of honest customers and firms alike.

2. As part of this, firms should have adequate safeguards to prevent fraudsters from setting up, controlling or manipulating bank accounts. They should also have better procedures to detect fraudulent accounts quickly and take rapid action to block them. This should include: keeping their fraud departments open 24 hours; empowering fraud departments to share information with other firms involved; and providing clear signposting to customers online, in branch and on automated phone systems for reporting suspected fraud and to facilitate quick action. Firms also need to give customers the knowledge they need (using a variety of delivery channels) to spot the warning signs and protect themselves.

THE CURRENT CONSULTATION

3. Generally speaking, we welcome the creation of an industry good practice code for the reimbursement of APP fraud victims. We believe that this is a positive step towards ensuring that victims are treated fairly and consistently. However, like any voluntary code, it lacks enforcement 'teeth' for firms that do not follow it which could be detrimental to other firms and customers alike.

4. Therefore we hope that all firms will choose to adopt the code as soon as possible as a matter of industry-wide good practice. Every firm should be required to tell potential and actual customers whether they are signed-up to the code so that customers can make informed choices about their banking service providers. In addition, the industry should take steps to inform the public more generally about the code and which firms have committed themselves to it as a means of fostering public awareness and confidence (of both the code and the ways to prevent APP fraud).

5. Consumer guidance in this area is key and it should be simply written to aid understanding and be available in a range of languages. However, we remain concerned about the continued use of the word 'scams' to describe fraud which we consider trivialises the crime and its harmful effects on victims. Our use of language in this area is crucial to ensuring that positive initiatives like this are given the priority they deserve.

6. We note that the code does not apply to international payments or payments made in other currencies and recognise that there are significant jurisdictional challenges in it doing so. However we question whether this will simply displace the focus of fraudsters' endeavours to these types of payments, so we encourage the sector and regulators to develop effective preventative measures (such as additional warnings and advice to customers about the risks associated with foreign payments and currencies) to stop this occurring insofar as possible.

RESPONSES TO SPECIFIC QUESTIONS

A. THE DRAFT CODE

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

7. In principle we agree with the draft standards SF1 and SF2 as set out in the draft code. However we believe that these should be reviewed within a reasonable time period of industry adoption to assess whether they are operating as intended and fit for purpose and then on a set periodic basis thereafter. In addition, the current proposals address only microenterprises, charities and individual customers; we believe the impact on corporate entity customers should also be considered.

8. We are particularly supportive of the minimum criteria for effective customer warnings (that they should be understandable, clear, impactful, timely and specific) and the constituent element that the customer is given clear guidance about the action they should take to avoid the risk of falling victim to an APP fraud. This latter point has been missing from much customer advice to date. Many firms simply provide warnings stating that once a payment has been authorised it cannot be returned and say nothing about the need to independently verify bank account details etc. Any actions suggested to customers must be practical and simply expressed to be truly effective preventative tools and need to be displayed at appropriate points in the customer's payment journey.

9. In our responses to previous consultations on this issue, we have suggested that firms may wish to consider compelling customers to take a five-minute interactive training session (or to watch a short video) every six months or so which explains APP risks, the common ways fraudsters try to trick victims, and the most important things they need to do to prevent it. This could be done, for instance, by building it in as a step for certain types or sizes of online transactions or when setting up or amending a payee. Consideration should also be given to providing advice at key financial milestones whereby vulnerability may be heightened, for example, during the mortgage approval process before a deposit is paid, when an unusually large lump sum (from a pension or inheritance) is deposited or when a loan has been approved. This would enable firms to show in a consistent and uniform approach to awareness and education.

10. The Standards for Firms state that '*If firms fail to meet these standards, they may be responsible for meeting the cost of reimbursing…*'. More consideration should be given to how this will be determined and by whom: will it be the sending firm, the receiving firm, an independent body, or a panel of these? Delays could be caused by lengthy investigations into whether the firms involved have met the standards or not. The definition of failing to meet could also vary significantly with the size and sophistication of the firms and customers involved.

11. The confirmation of payee requirement is an important part of combating APP fraud. However, paragraph 3.42 of the consultation paper states that the steering group does not want confirmation of payee to interrupt legitimate payment journeys unnecessarily. This may not be possible given that matching the payee's name to the account details may produce false positives which will necessitate investigation. This will take time and could cause delays to payments given that these checks are an additional step in the payment process which does not currently exist.

12. Furthermore paragraph 3.45 states that '*firms are encouraged to take steps to delay payments or freeze funds so they can make investigations where they are concerned about APP scams*.' This contradicts paragraph 3.42 in that firms will need additional time when payee name and account details do not match. This and other red flags need to be investigated. More consideration is needed on how these new requirements may place additional burden on firms and result in delays to payment journeys whilst investigations are performed.

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.

13. We believe that it should be possible to mitigate most unintended consequences in this regard through independent review of the adequacy of the effective warnings provided to the customer and verification of the customer's compliance with these warnings by way of complaint to the Financial Ombudsman Service (FOS). We reiterate our earlier points that effective warnings should include practical actions that customers can perform to confirm that a payee or payment is genuine before proceeding with the payment and that customers should be compelled to complete periodic online training.

14. One scenario which might prove much more problematic is R2(1)(e) whereby a microenterprise or charity does not follow its own internal procedures for approval of payments, particularly if that entity has:
    a. no formally documented procedures, and/or
    b. been the victim of a rogue employee, and/or
    c. had its email system compromised or credentials stolen by hackers.

    It should be borne in mind that many microenterprises consist of a single individual, who is unlikely to be in a position to take more security measures than a retail customer.

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

15. This question is difficult to understand and interpret. However if our understanding is correct, R2(1) sets out the criteria under which a firm may choose not to reimburse a victim. However in order to establish whether none of the parties involved have met their levels of care we believe you also need to take into account R2(2) which requires firms to consider whether they have meet the Standards for Firms or not.

16. It is our view that once such an assessment has been made by the firm, an independent determination can then be made as to which party has been the most competent/negligent and a proportionate reimbursement model applied (for example, an apportionment of 2/3s). Difficulty may arise if one of the firms involved is not a signatory to the voluntary code. An industry-wide protocol may be needed for the disclosure of confidential customer information (which may include the owner of the fraudulent account) to the independent third party.

17. If independent third parties are to be used to determine whether firms failed to meet the standards, consideration should be given as the background and experience required of those parties and whether their decisions will be binding.

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

18. Yes. We agree with the steps that customers should take to protect themselves.

19. However we also note that most victims of APP frauds genuinely believe that they are making a payment to a legitimate payee, otherwise they would not be making the payment in the first place. The sophistication of many such frauds means that it can be very difficult for the average person – however carefully they manage their affairs – to distinguish between the genuine and the criminal, and this is why the awareness-raising efforts of firms is so important. Frontline staff could also benefit from enhanced training in this regard to ensure that they ask customers the right questions (particularly in branch) when payments are being requested (for example, 'have you checked the bank account details are correct by …'). We understand that some firms are already doing this.

20. We agree that where customers have caused deliberate obstruction to firms investigating APP frauds or provided false information then firms can decide not to reimburse them (R2(1)(f). However in making such an assessment, firms will need to take into account extenuating factors such as whether the victim has been coached by the fraudster (impersonation frauds) or simply forgotten important details because of the stress caused by the victimisation itself or other circumstances. These situations should not be legitimate reasons for firms not to reimburse the customer.

21. Further consideration should also be given to how firms will go about proving the criteria set out in R2(1)(c),(d),(e) and (g). There may be limited evidence available to prove or disprove the facts around whether a customer, for example, '*recklessly shared access to their personal security credentials…*'. As noted above, consideration should be given to who will do these investigations and make decisions about negligence. These investigations could prove to be very time-consuming and costly for firms, especially if they have to engage with independent third parties or create new teams to review reimbursement claims and respond to disputes between firms.

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?

22. We agree that vulnerable customers should receive extra help to protect themselves and be assessed on a case-by-case basis to determine whether their personal circumstances indicate that they are vulnerable and should be eligible for reimbursement, regardless of whether the customer has been identified as vulnerable prior to the victimisation.

23. One unintended consequence of this approach could be that firms exit customers who are vulnerable and/or present a greater risk of causing loss to the firm as a result of falling victim to APP fraud and other frauds.

24. We recommend that if the code adopts BSI PAS 17271 'Protecting customers from financial harm as a result of fraud or financial abuse: code of practice' as a standard then the standard should be made publicly and freely available to customers for transparency and accountability purposes on a similar basis to the former PAS 1998:2008 'Whistleblowing arrangements: code of practice' (now withdrawn). Customers should also be signposted to it.

25. We also believe that firms could benefit from the experiences of the Action Fraud 'National Economic Crime Victim Care Unit' in respect of assessing vulnerability.

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

26. We believe that the proposed timeframe for notifying customers on reimbursement decisions (within 15 business days or 35 business days in exceptional cases) is a significant improvement on the current situation. Further guidance is needed on what constitutes an exceptional case.

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

27. Other good consumer awareness and education tools include the GetSafeOnline website and the Metropolitan Police Service's 'The Little Book of Big Scams' and 'The Little Book of Cyber Scams'. For microenterprises and charities the National Cyber Security Centre has published the following: '10 Steps to Cyber Security', Cyber Security: Small Charity Guide', and 'Cyber Security: Small Business Guide'.

28. Another measure could be to ask customers to complete a short checklist when amending an existing payee or setting up a new one in branch or online to confirm that they have taken adequate precautions.

B. OUTSTANDING ISSUES

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

29. Yes, in principle this seems to be the correct approach but it will depend to some extent on the final funding model adopted.

Q9. Do you agree that the sending firms 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?

30. Yes.

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?

31. We reserve our opinion on the funding options outlined in paragraph 4.6 until such time as further details are available. We hope that these will be the subject of a separate consultation.

32. We note that any new requirements (voluntary or otherwise) on customers to obtain insurance policies and/or pay additional charges on certain transactions may result in some customers looking for cheaper (and probably less regulated) ways to make such payments, for example,

cryptocurrencies and other higher risk transfer methods which may simply move the risks elsewhere.

33. In addition to the Criminal Injuries Compensation Scheme (CICS) another existing model that might merit consideration is the Motor Insurers' Bureau (MIB) which is the mechanism through which compensation is provided for victims of motor vehicle accidents caused by uninsured/untraced drivers.

34. In order to ensure the longevity of any funding model introduced it may be necessary to set a maximum value on reimbursement as per the CICS.

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

35. Firms will need to document evidence of the steps taken. Customers will need to show that they contacted the firm as soon as possible after they realised they had been defrauded and followed the advice they had been given. This may also include details of any checks they did on the payee before making the payment.

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

36. Yes. We agree that clear guidance is needed on the type of evidence which will be expected to be created and maintained when an APP fraud occurs, for both the firms and the customer. This will lessen the likelihood that there will not be enough evidence to complete a balanced investigation. Customers may feel at a disadvantage when dealing with their banks given the firms will be more sophisticated in producing evidence and defending their compliance with these standards.

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

37. No.

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

38. Some customers may need to waive their privacy in order to demonstrate vulnerability. This would be a decision for the individual customer or an appropriate other person. A customer could be given a standard checklist to voluntarily supply relevant information to assist with the assessment process.

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

39. We believe that the Payment Services Regulator is the most appropriate body to govern the code.

40. To foster public confidence and assurance in the integrity, independence and impartiality of the code it should not be governed by a body that represents the interests of a specific group of stakeholders such as financial services firms (for example, UK Finance) or consumers.

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

41. We agree that changes to the code should be permitted on an ad hoc basis (especially in response to changes to APP fraud typologies and findings from disputes between firms). These changes must be subject to an open, rigorous and transparent change process.

42. We also agree that the code should be reviewed periodically with the first one conducted a year after the code is finalised and then every three years thereafter. Reviews should be subject to wide public consultation supplemented by proactive engagement with key stakeholders where appropriate.

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

43. Yes.

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?

44. Further consideration should be given to how these principles are currently operating to deal with disputes and whether there have been any issues in satisfactorily resolving disputes. We note that these principles are also voluntary.

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

45. As noted above, consideration should be given to the evidential standards that would need to be followed to prove whether the standards for firms were met. Consideration should be given to who will adjudicate these disputes and whether they need to be independent from the firms. Customers should be given clear options on how they can appeal when the dispute is not satisfactorily resolved, in a reasonable time period.

C. 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?

46. We hope that the introduction of the code will have a positive impact on actual and potential victims of APP fraud by reducing the chances of falling victim in the first place (because of better awareness and safeguards) and providing reimbursement (where appropriate) where they do.

47. The main negative impact will be the potential de-risking of certain types of customer (for example, who might be identified as more at risk of becoming money mules) by firms. Appropriate safeguards will be needed to address this. It is our opinion that firms which have confidence in the adequacy of their account opening procedures and effective warnings shouldn’t need to de-risk.

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?

48. Firms that do not become a voluntary party to the code, who do not follow the prescribed standards, or who close victim accounts as part of de-risking processes, could suffer loss of customer confidence and reputational damage.

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

49. It is likely that there will be an initial increase in the number APP frauds reported to firms because of greater awareness of the standards. However as long as the principles of the code are adhered to consistently these should reduce soon thereafter.

50. There may also be increased costs to customers and/or firms depending upon the final funding model.

51. Finally, there is a strong likelihood that APP frauds will be displaced elsewhere such as international and/or foreign currency payments, and vulnerable victims.

Q23. How should the effectiveness of the code be measured?

52. Effectiveness of the code should be measured by the reduction in the volume and value of successful APP frauds reported to firms.

Lyddon Consulting Services response to consultation on Contingent Reimbursement model

November 14th 2018

Submitted by: Lyddon Consulting Services Ltd (www.lyddonconsulting.com)

What is Lyddon Consulting?
A specialist consultancy in payments and electronic banking. We have recently acted as advisor regarding the UK payments landscape to a trade body representing UK Payment Institutions and to a major payments communications cooperative reviewing their UK market positioning. From 2003 to 2016 we were retained to run the central secretariat of IBOS Association, a global banking club arranging accounts and services for corporate customers, a central feature of which was the fulfilment of regulatory responsibilities for Customer Due Diligence.

What we have done in the field of Authorised Push Payments Fraud up to now:
We have carried out a major piece of research under the name of Project Carlton which examines the quantum and trajectory of APP Fraud, and the flaw within the Faster Payments system that enables it, which is replicated in the way banks process Internal Transfers.

We have recently made a submission into the Treasury Select Committee inquiry into Economic Crime on the subject, and two supplements as the nature of the plans for Confirmation of Payee and for the Contingent Reimbursement model have taken shape.

Confirmation of Payee and the Contingent Reimbursement model accept the current Faster Payments system as a given, and take no issue with its being replicated under New Payments Architecture.

This is one of five key points of perspective that we believe are missing behind the PSR's approach to APP Fraud, and which therefore invalidate the Contingent Reimbursement model at a conceptual level.

In addition there are five further, overarching points, and points of detail which we have addressed in our responses to the individual questions.

Contact details
Lyddon Consulting Services Ltd

Overarching points

a. Drafting

We find the code poorly drafted, with imprecise phraseology.

b. Scope

The scope is inadequate if it only reimburses non-personal customers that are microenterprises and charities. SMEs have been major losers from APP scams and they should be within scope. Indeed, we believe that it would be better to have a negative scope, classifying all victims as eligible unless they fall within given, limited categories.

c. Value Proposition for customers

The customer need not, and should not, be a party to this entire code. The customer requires a clear Value Proposition, as they have with the Direct Debit Guarantee. Any code should then be entirely between Payment Service Providers ("PSPs"), who should make clear to the customers whether they support the Value Proposition or not.

The scope of the code can be limited to those matters that need to be regulated between PSPs in order that the victim receives their reimbursement from their own PSP, whether or not it is that PSP or the beneficiary's PSP that is at fault.

d. Fault of beneficiary PSP

In our view the fault will lie with the beneficiary PSP unless they can prove otherwise, as they have (i) opened an account for a fraudster; and (ii) handled the proceeds of a crime.

e. No description of "As-Is" rights of the parties

The code should base itself upon where liability for different actions that contribute to the fraud lie now, with reference – inter alia - to:

- The 2017 Money Laundering Regulations, and particularly the obligations of the fraudster's PSP under Customer Due Diligence and their liability when they handle the proceeds of a crime;
- The 2017 Payment Services Regulations, and particularly how a victim of a fraud perpetrated via a "payment instrument" is covered and how that differs from the coverage for the victim of an APP scam;
- Terms of access to the Financial Ombudsman Service;
- The duty of care that a PSP owes to an account-holder;
- The duty of care that an account-holder owes to their PSP.

Five key points of perspective

Five key points invalidate the Contingent Reimbursement model draft code at a conceptual level.

I. Flaw in the Faster Payments system

There is a historic flaw within the Faster Payments system that enables APP Fraud. It derives from the original design of the system in around 2005. The Faster Payments design was based on the system for card payments at Point-of-Sale, because that was the only payment process in place at all of the largest UK banks at the time where such a bank could receive a message, process it and send a response in near-real-time.

The prime indication of Faster Payments being based on the POS chassis is its usage of the ISO8583 data standard, which is the cards standard. Vocalink was able to create the infrastructure for Faster Payments at short notice and without a build from scratch because it was already using the ISO8583 standard within its infrastructure for LINK.

There was at the time a process in operation within IBOS for the European member banks to receive a message, process it and send a response in near-real-time, but RBS was the only UK bank in IBOS, the infrastructure used by IBOS was and is SWIFTNet FIN (meaning that the messages are SWIFT MTs), and Vocalink was not involved. In consequence IBOS was not considered as a model upon which to base Faster Payments, notwithstanding the wide usage of SWIFTNet FIN and MT across the payments industry.

It must also be mentioned that Vocalink was able to re-use the BACS Sort Code Routing Tables to support Faster Payments because Vocalink runs the BACS infrastructure as well, and it is not coincidental that the field lengths in Faster Payments for the beneficiary name (even though it is not processed and checked at the beneficiary bank) and for the reference are limited to 18 characters, because the implementation of ISO8583 for Faster Payments reproduced limitations in the Standard18 data format used for BACS.

Faster Payments can be viewed as a system which made significant re-use of pre-existing elements of POS, LINK and BACS.

The central flaw that came with using a pull payment chassis (POS) upon which to build a push payment service (Faster Payments) was the absence of a beneficiary name-check at the beneficiary PSP. This function is not needed in a pull payment model like POS: the beneficiary initiates the POS payment themselves at their terminal and they have set up the relationship with their acquirer so as to ensure the funds go into their own account.

The beneficiary has no need to capture their own name, and the payment message that results and which is sent to card issuer does not cause a name-check between the card details and the beneficiary, because the card is the card of the payer and does not contain the beneficiary name.

The ISO8583 message as used within a POS model, when used in the Faster Payments implementation, does not result in a name-check at the beneficiary PSP even though it is needed in a push payment model. The beneficiary name – even if it is input into a payment template by the payer – is not processed at the beneficiary PSP i.e. it is not checked to ensure coherence with the name on the account that is associated with the payment destination indicated by the Sort Code and Account Number.

Faster Payments should be fundamentally re-engineered to eliminate this flaw, but this is not foreseen in the New Payments Architecture project.

II. Failure of beneficiary PSP's Customer Due Diligence

The beneficiary PSP has opened an account into which the proceeds of the APP Fraud are received. This indicates a failure of the beneficiary PSP's Customer Due Diligence during the onboarding phase, for which the PSP's culpability is absolute. The PSP is an "obliged entity" and has specific responsibilities around customers for whom it opens accounts, and these responsibilities do not diminish because of how other market actors in a payment chain behave.

The victim of APP Fraud is not an "obliged entity", a fact which has major ramifications on liability but one which is notable by its absence in the draft code.

III. Beneficiary PSP commits Money Laundering if it receives, credits and pays the proceeds of a fraud

If a PSP receives, credits and then relays funds that turn out to have been part of a criminal wrong-doing on the part of the PSP's account-holder, the PSP has itself committed a Money Laundering offence. Again the commission of the offence is neither mitigated nor diminished by the behaviour of other actors in the payment chain.

IV. Poorer coverage for a consumer under APP Fraud than when they use a "payment instrument"

Where a customer has used a "payment instrument" to effect a payment, the 2017 Payment Services Regulations (transposing Payment Services Directive 2) protect the customer against fraud up to a high bar.

The bar is firstly that the burden of proof of wrongdoing is on the PSP, not on the customer. Secondly the PSP must prove that the mistake was due to gross negligence or similar on the customer's part. The protection for a customer should not be lower under APP Fraud. The CRM draft code, however, offers the customer a radically lower level of protection.

V. Too narrow definition of what constitutes a "payment instrument"

We have a definitional issue in what constitutes a "payment instrument" and is therefore eligible for the PSD2 level of protection. A prime example is where the PSP's method for its customers to authorise a push payment employs a "payment instrument" (a debit card) in combination with an authenticator (such as a Vasco Digipass device) that a customer might well understand also to be a "payment instrument". The customer for sure uses one "payment instrument" and in combination with another object that a Man on the Clapham Omnibus might reasonably consider also to be a "payment instrument".

But, when used in combination, the result does not rank as a "payment instrument" under the 2017 PSRs. It would require a change in legislation – but a worthwhile one – to enlarge the scope of the definition of a "payment instrument" in the 2017 PSRs to include the cards/devices/combinations used to authorise push payments, and to ensure that surrogates for these objects – like Memorable Information – do not fall outside the scope of legal coverage when – towards the PSP's computers – their impact is the same.

Since the European Banking Authority's Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication come into force in the UK in September 2019 and require at least 2-dimensional security on all electronic payments, there is a near-term opportunity to eliminate the security gap on push payments that makes customers liable to lose far more when they use a push payment mechanism than when they use a "payment instrument".

That is an opportunity in the short term, whereas in the medium term the priority should be to re-engineer Faster Payments so as to include the name-check and on every payment. Were that to be done, the Confirmation of Payee would occur as part of the processing of every payment, and there would be no need for it as a separate, "overlay" service.

It would also change the landscape in which the CRM code would operate, rendering it redundant in its current form.

The obligation to credit the correct beneficiary as named in the payer's payment order should already lie squarely with the beneficiary PSP. The risks should be the same as with a cheque that is crossed "Account payee".

It is the beneficiary PSP's risk if it credits the cheque to an account with different naming than what the payer has written in the payee line of a cheque; it should be the PSP's risk if they credit a push payment to an account named differently to the contents of the payee field in a Faster Payment.

The beneficiary PSP's options should be to credit the funds, or to return the payment (not to reject it, as they have received settled funds).

If the PSP credits the payment and it turns out to be part of a fraud in which the beneficiary is culpable, the PSP has handled the proceeds of crime, which is money laundering. That offence would bring certain sanctions down upon it which, hopefully, would include reimbursement of the funds to the payer.

The PSP will also have failed in its Customer Due Diligence under the Money Laundering Regulations, having opened an account for a criminal in the first place. This is an absolute failing, in that the onboarding process must filter out actual or potential criminals such that, if one slips through the net, the PSP is liable for everything that stems from their own offence – and it is an offence, not just a failing.

Once again that offence would bring certain sanctions down upon the PSP which, hopefully, would include reimbursement of the funds.

The responsibilities of the beneficiary PSP under Anti-Money Laundering/Countering the Financing of Terrorism regulations are absolute in almost all cases, and do not diminish depending upon the behaviour of other parties. Inexplicably this basic rule-of-the-road is lost in the CRM draft code.

This has the effect of overlooking the rights of customers that derive, as third-party rights, from the obligations imposed on PSPs as "obliged entities" under AML/CFT legislation.

The deviation from this rule-of-the-road is exemplified by the CRM draft code containing fourteen instances of the word "reasonable". When applied to actions a PSP may have taken, the impact of the insertion of a test of reasonableness has the effect transferring risk away from the PSP and on to the payer.

In our experience (from IBOS) there is only one instance in AML/CFT regulations where the concept of reasonableness comes into play in a material way, and it is in putting a limitation on the enquiries that a PSP might have to undertake to establish the Ultimate Beneficial Ownership of a non-personal legal entity that is applying for an account. This is test is laid out in article 13.1.b of the 4th EU AML Directive.

The fourteen instances of the use of the word "reasonable" in the draft code are in GF.1.a, GF.3.a, SF1, SF1.2, SF1.2.a, SF1.3.a, SF1.5.a, SF2, SF2.1, SF2.3, SF2.5, R2.1.d, R2.3 and R4. This is in a document of 12 pages.

By contrast the 4th EU AML Directive is 45 pages long and only contains three other instances of the word "reasonable" beyond where it deals with Ultimate Beneficial Ownership:

1. Article 21, regarding who is the beneficiary of an insurance policy;
2. Article 33.1.b where an obliged entity has to inform the local Financial Intelligence Unit if they have reasonable grounds for suspecting that funds derive from criminal activity;
3. Article 60, to do with the postponement of publication of specific names involved in an AML lapse for a "reasonable" period of time.

It can be seen, then, that a test of reasonableness – which in the best of circumstances will involve a measure of subjective judgment – appears in the draft code far more often, and in connection to far more central points, than it appears in the 4th EU AML Directive, of which the 2017 Money Laundering Regulations are the UK's transposition.

Where any degree of subjective judgment comes into play, it should go without saying that this judgment should be exercised by a court of law, tribunal, the FOS or similar and not by the PSPs involved in the case.

Measured against the points listed above, the proposed CRM code does not do justice to those current rights of a customer that derive from the laws binding upon a PSP. The draft code muddies the waters for the customer, when it should make them as clear as they are under, for example, the Direct Debit Guarantee.

Given that the customer's rights in law are actually better than the CRM code, all the code can serve to do is to both waste time and to give the PSPs greater apparent rights against their customer than they actually have.

The CRM code should not proceed.

Work should re-start based on:

- what the customer's rights in law are;
- what the PSPs' obligations in law;
- what rights the customer derives as a third-party beneficiary from the PSPs' obligations in law;
- what the flaw is in the Faster Payments system and remedying it;
- putting in place a code to govern the period between when the current Money Laundering Regulations came into force (26th June 2017) and when the flaw in Faster Payments is remedied, such that the customer is protected against APP Fraud during that period to the same level they would have been protected if the same payment had been carried out using a "payment instrument".

During this interim period, changes need to be put through to the 2017 Payment Services Regulations that work with the EBA Regulatory Technical Standards and re-define the devices and processes used to authorise a push payment – and their surrogates such as Memorable Information - as being covered by the term "payment instrument".

In addition, during this interim period, the responsibilities of PSPs under current Money Laundering Regulations need to be reinforced to them by their respective financial regulators - with a reciprocal assurance being delivered to customers from those same financial regulators - that the financial sanctions imposed on PSPs for (i) handling the proceeds of crime obtained via APP Fraud; and (ii) a failure of Customer Due Diligence in the onboarding phase, will deliver the amount of money needed to place the account of the victim of an APP Fraud in the same position as if the fraud had not taken place – the same yardstick as is used to protect a customer from fraud around usage of a "payment instrument".

Individual responses

Core questions

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

#	Comment
3.27	There should be no incentives to PSPs for them to carry out basic functions properly, and to comply with applicable laws and regulations
3.28	Self-assessment has no role to play here. The firm cannot be permitted to act as judge and jury
3.29	No comment
3.30	The word "better" is misplaced as the current protection is zero. What is the standard of protection that is being aimed at? If it is lower than that which applies when a customer uses a "payment instrument", there needs to be a solid justification as to why
3.31	This is absolute hygiene factor and has no place in such a code, or is it the case that firms do not have staff training?
3.32	The presupposition of this clause is that blame can be attached to a customer for falling victim to fraud. The best way to avoid fraud is to have products and services that frustrate fraud, not to put emphasis on the customer helping themselves. The underlying assumption is that if the customer does not heed the warnings that they receive during their "payment journey", the legal responsibility for the results can be transferred onto the customer, which is wrong
3.33	Incentivisation should play no role. If firms have expertise and ability they should apply this to doing the beneficiary name-check and to not opening accounts for fraudsters
3.34	This will be impossible to police and will have the sole effect of frustrating customers in obtaining redress from their PSP
3.35	QED – the warnings will frustrate customers in obtaining redress. A code such as this should not be about legitimising PSPs transferring their risks onto their customers
3.36	No comment
3.37	These generalisations set no effective marker
3.38	What does "do more" mean? More than what? Who will police this?
3.39	CoP was originally billed as solving APP Fraud. This downgrading of expectations of CoP is incorrect
3.40	No comment
3.41	Pay.uk has issued a brochure showing that CoP will only be available when a payment is set up, not each time the template is used, so the statement "When a customer is in the process of making a payment" incorrectly renders the scope of CoP. Pay.uk has also stated that a pay-out under the CRM will only be made if (i) the customer has used CoP; and (ii) the customer has received the "green tick" outcome of the three possible ones. There really needs to be clarity on what the actual deal is with CoP and it is disappointing that there are differences between the CRM code wording and communications coming from Pay.uk
3.42	This paragraph is very unclear and needs to be unbundled into what this means for the customer and the firm

#	Comments on Q1 (continued)
3.43	This paragraph, together with the following two, should rather be aimed at ensuring the victim is reimbursed speedily unless there is prima facie evidence that the victim acted with gross negligence or similar (the conditions under which a PSP can refuse to reimburse a victim of a fraud deriving from the usage of a "payment instrument"). The current contents, and the "Best Practice Code", smack of procedures to bat away customer claims
3.44	See response above
3.45	See response above

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

All we can see here is an infrastructure to legitimise firms not paying out, and being able to avoid their responsibilities not to open accounts for fraudsters. An inter-PSP code is indeed required to govern which PSP pays the reimbursement, and how the beneficiary PSP reimburses the victim's PSP, absent prima facie evidence of gross negligence or similar. There can then be a clear Value Proposition to the customer that the PSP community will meet the damage caused by APP Fraud, and then individual PSPs and Pay.uk need to make the necessary arrangements to squeeze APP Fraud out of the system without inveigling the customer into joint responsibility for 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.

The customer has no duty of care in law towards their PSP. It is the PSP entirely that has a duty of care towards their customer. Imposing a duty of care on the customer is wrong, when APP Fraud derives from two things (i) PSPs open bank accounts for fraudsters; and (ii) PSPs running an external payment system (Faster Payments) that has no name-check obligation at the beneficiary bank.

We would add to this the contention that PSPs run their internal transfer (the third type of transfer that the code is supposed to govern beyond Faster Payments and CHAPS) along the same principles as they interact with Faster Payments: crediting is based on Sort Code and Account Number alone.

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

It is hard to disagree with the steps themselves, but we do disagree with the supposition that there should be a transfer of responsibility from PSPs to customers based on whether customers have followed these steps.

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?

All customers are vulnerable to APP scams, as has been proved. If the issue was resolved properly there need be no extra measures for "vulnerable customers". Building in such measures is unfair to supposedly non-vulnerable customers, who are equally as vulnerable to APP scams.

Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?
We disagree with the contention that is an acceptable response to deny reimbursement other than where the PSP puts forward a prima facie case that the victim has acted with gross negligence or similar, an accusation which must be laid out in due bureaucratic form together with the process that the PSP intends to follow to prove their claim. As is normal in civil and criminal proceedings where the PSP is the plaintiff, they must set out their evidence in such a form that the victim's counsel can deal with the claim.

Access to Financial Ombudsman service – R4
There is no question relating to this section and we refer to point 3.77 where it is stated: "The steering group considers that a customer who is refused reimbursement by a firm or has any other related complaint about a firm should, where eligible, be able to challenge the outcome by going to the FOS in a timely manner and having FOS review the decision".

The FOS is a service available to customers without the say-so of this steering committee. The steering committee has no right to put inferred qualifications on a customer's access to the FOS with insertions such as "where eligible" and "in a timely manner". The customer can challenge anything within the FOS' scope, whether there is a CRM code in place or not.

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?
The measures can be described as "hygiene factor", "nice to have", "motherhood-and-apple-pie", because they do not go to the heart of the issue for the customer, are in many cases irrelevant to the customer and, if they happen at all, should happen out of view of the customer, without their involvement, and as measures for the PSPs to undertake in order to resolve the APP scams issue for their customers.

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 disagree that there should be a required level of care for customers at all: they should be reimbursed unless their PSP can prove gross negligence (same tests as in PSD2 regarding a "payment instrument")

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?
Only the sending firm – the victim's PSP – can deal with the victim. Whether they have to meet the full cost of reimbursement or can obtain some reimbursement from the beneficiary's PSP is a matter that should be dealt with in the only code that is needed: the inter-PSP one to back up the "Value Proposition" to the customer.

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 disagree with all the funding options. Once the sending and receiving PSPs realise they are going to have to reimburse victims to the same standard as prevails in the cards world, the problem will be resolved.

Major banks in the UK will find themselves as often on the victim side as on the fraudster side. Since they can be expected to adopt the Transaction Risk Analytics approach to complying with the European Banking Authority's Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication, they will find themselves in a far better position to identify and reduce fraud themselves, without any actions on the part of their legitimate customers.

The remaining loophole will then be the lack of name-check in the processes for both Faster Payments and Internal Transfers: if APP scams were to be reimbursable in full other than in case of gross negligence or similar, the amount that PSPs would be looking at losing over a 5-year period – given the current quantum and trajectory of APP fraud – provides the business case for investing in eliminating the underlying problems.

We repeat – if PSPs are in a position where they will be reimbursing all APP frauds except where the victim has been grossly negligent, they will then find the money to take the necessary measures to control and eliminate this type of fraud.

Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?
We consider this question as irrelevant given the views we have expressed above about the justifiability of the expectations and standards described.

Q12 Do you agree with the issues the evidential approach working group will consider?
As we have said that the code is unjustified in its present form, that the responsibilities of victim and PSP in law (including as third-party beneficiaries) should be the framework, as there is access to the FOS notwithstanding the existence of the code, we believe there is no need for the proposed task, and therefore no need for the evidential approach proposed nor indeed any other approach.

Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?
No, because the evidential approach is not required, as per our response to Q12 above.

Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?
It should not be, for the reasons laid out in our response to Q5 above.

Q15 Please provide views on which body would be appropriate to govern the code.
If there were a code that met the requirements as we see them it would primarily be the FCA as main AML/CFT regulator of the UK's PSPs, supported by HMRC as AML/CFT regulator for a subset of PSPs. The main adjudication they would be called upon to make would be on whether the beneficiary PSP had:

I. adequately discharged its responsibility for Customer Due Diligence when onboarding the fraudster's account;
II. whether it had made itself guilty of money laundering by handling the proceeds of the scam.

The outcome would be the sharing of the reimbursement between the two PSPs (the only issue that needs addressing in any code) and the requisite penalties imposed on the PSPs for AML/CFT failings.

Q16 Do you have any feedback on how changes to the code should be made?
As our view is that the code is flawed in its suppositions, scope, intentions and content, we would reserve comment on this question until there was a draft code available that met with our concept.

Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?
See response to question 15 above.

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?
No, they are not needed if the code had the scope we have outlined above.

Q19 What issues or risks do we need to consider when designing a dispute mechanism?
None, as there is no need for one.

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?
Victims have more responsibilities placed upon them, possibly unknowingly. They will be gulled by PSPs into surrendering both rights under any code (which have no legal force anyway) and rights that exist in law. These impacts can be addressed by not proceeding with this code and instead by re-starting the project in the way we recommend in our introductory section.

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?
PSPs will act as judge and jury over whether they have met the standards in the code, including applying their own subjective judgment as to whether their actions meet a test of reasonableness. This is unacceptable and will provide a bogus cloak of protection to PSPs against their customers. The code transfers risk from the PSP to the customer, without emphasizing the absolute responsibilities in law of PSPs in the AML/CFT area. These impacts can be addressed by not proceeding with this code and instead by re-starting the project in the way we recommend in our introductory section.

Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?
The transfer of risk from PSPs to customers.

Aside from what we have already said, there is another aspect that has aggravated APP fraud, and this is the progressive increase in the Faster Payments system limit from its initial £25,000 at launch to £250,000 now.

For a payment mechanism aimed at standing orders and at retail payments initiated from a mobile phone, tablet or PC, £25,000 was already too high. Now, at £250,000, it is in effect a High-Value Payment System and with the name-check defect.

Whilst it is the Faster Payments scheme company that has to propose any increase in the system limit to the Bank of England so as to be granted the Bank of England's non-objection, the increases have been driven as much by the Bank of England's policy of driving "non-systemically-important" payments off the CHAPS system, as by Faster Payments' desire to increase its payment volumes.

When CHAPS had its outage in October 2014 it came to light that the Bank of England had separate processes for "systemically-important" payments and "non-systemically-important" ones. We feel that we can say with assurance that customers were unaware of there being a process where PSPs submitting payments into CHAPS would decide which CHAPS function was to be invoked.

The Bank of England's defence that it is the submitting banks who decide whether a payment is systemically-important or not is invalid, because there is a financial incentive to submitting PSPs to classify payments as non-systemically-important, and because no benefit is offered to or accrues to the ordering party when their PSP decides that their payment is non-systemically-important. Ordering parties are only ever offered CHAPS as a unitary service, with a set fee per payment, and are not given a choice between the two modes of processing at the Bank of England, or a differential price.

On 20th October 2014 all systemically-important payments were processed, but non-systemically-important ones were not, and were held over until the following day even if some related to property completions. These customers had paid their £30-50 for a first-class payment, and then their payments were treated as second-class and they had to sleep in their cars overnight.

The Bank of England's contribution to APP fraud through their pusillanimous policy of pushing "non-systemically-important" payments off CHAPS and onto Faster Payments has not been surfaced anywhere in the PSR's work on the subject so we have taken the opportunity to record it here, for the customers who spent the night of 20th October 2014 in their cars, and were given no reimbursement of their £30-50 CHAPS fee.

Q23 How should the effectiveness of the code be measured?

Notwithstanding our views of the code in its current form, the yardsticks are simple:

- The average loss on an APP scam should be £300, the same amount as the average loss on card fraud;
- 60% of APP scams should be prevented by PSPs, without any action by the customer, the same percentage of fraud losses that are prevented in the cards world before they impact a victim;
- All APP scam victims should be reimbursed in full within 15 days by their PSP, unless their PSP can make a prima facie case of gross negligence or similar;
- A name-check is done at the beneficiary bank on all Faster Payments and Internal Transfers, and the risk of crediting for the beneficiary PSP is the same as crediting a cheque.

BL/14.11.18

MoneySavingExpert.com

Response to APP Scams Steering Group Draft Contingent Reimbursement Model Code consultation

MoneySavingExpert.com is pleased to see the progress in the Draft Contingent Reimbursement Model Code towards better prevention of APP scams – and reimbursement for consumers who fall victim to them.

While we welcome the improvements to consumer protection this would bring, we respond to this consultation with comments focused on creating a stronger still level of protection for consumers, which is the minimum consumers need.

The code must have comprehensive membership

All banks and Payment Service Providers should sign up. While there is an expectation that large firms will sign up, smaller firms *must* also be members in order for the intentions of the Code to be reliably delivered in practice. If consumers fall victim to a scam and the 'at fault' firm is not a member of the Code, then the Code becomes meaningless, and the intention for consumer protection evaporates. Furthermore, crucial consumer communications of the Code will be compelling with full membership, and unconvincing without comprehensive coverage.

Innocent consumers must not be liable for losses

In other payment services – such as with credit and debit cards – when consumers are the victim of fraud that is not their fault, they are not expected to pick up the bill. Faster payments is an anomaly, and this is a flaw.

While it is positive to see agreement that firms should be liable for losses where they are to fault and the consumer is not, the Code needs to go further: in a no-blame situation (either on the part of a firm or a consumer), consumers must still be fully protected. In short, if the consumer has met the requirements of the Code, they are not to blame and should not pay.

There are several different models which could be used to ensure that the consumer doesn't pay. As happens with other types of fraud, it makes sense that the firm has to pick up the bill. In addition to protecting the consumer, this would also incentivise firms even more to prevent APP fraud, while doing so on an interim basis would reassure them that they do not have unlimited liability.

Governance of the Code should be carried out by Pay.UK

As Pay.UK already oversees faster payments and has expertise in this area, it is logical for this body to carry out governance of the Code. Pay.UK could incorporate the Code into its faster payments rules.

Awareness campaigns must be carried out in the spirit of the Code

All efforts to raise consumer awareness of scams, how to avoid them, and their responsibilities are welcome. The scammers are naturally expert in this, and consumers need to be empowered as much

as possible to be able to spot scams, avoid them and report them. And that must be the objective of these campaigns. Firms must commit to the spirit of the campaigns, it should not be seen as an opportunity to build brands or attract new customers.

The Code must be ready before it is launched

We recognise the amount of work that has gone in to getting the Code to this point, and that issues remain to be agreed upon. However, with the intended launch date of early 2019, it is imperative that the Code is not rushed and accordingly delivered unready. While it is, of course, always possible to improve the Code after launch, it must be fit for purpose before it is launched. This will avoid a false start that could severely undermine the vital (and urgent) purpose that sits at its core: to properly protect consumers from criminal scammers.

About MoneySavingExpert.com

MoneySavingExpert.com is the UK's biggest consumer website dedicated to saving people money on anything and everything by finding the best deals, beating the system and campaigning for financial justice. It's based on detailed journalistic research and cutting edge tools, and has one of the UK's top 10 social networking communities.

During October 2018 MoneySavingExpert had 18.1 million users, visiting the site 33.1 million times, and looking at over 78.7 million pages. Over 13.5 million people have opted to receive our free weekly email, more than 1.7 million users have registered on the forum and over 3.7 million have joined our Cheap Energy Club.

In the event of any queries, please contact the campaigns team:
campaigns@moneysavingexpert.com

NATIONAL TRADING STANDARDS
Scams Team

National Trading Standards Scams Team

APP Scams Steering Group – Draft Contingent Reimbursement Model Code

Please note that in this response the terms scam and fraud are used interchangeably. The NTS Scams Team believes that the division made by financial institutions between fraud and scams based on whether or not a payment is authorised or unauthorised is an artificial one that is incomprehensible to victims. Further we believe that distinguishing between fraud and scams has allowed 'scams' to be viewed as less serious, downplaying the impact on victims and resulting in weaker public and private action to prevent and tackle them. Our policy is that ***Scams are Fraud and Fraud is a Crime****.*

The National Trading Standards (NTS) Scams Team welcomes the opportunity to respond to this consultation. We support the idea of a contingent reimbursement model for authorised push payment (APP) scams which we hope will create greater protection for victims and raise standards for financial institutions. The original principles set out by the Payment Systems Regulator (PSR) are sensible and useful. We welcome the draft code which makes progress towards these goals and should ensure greater consistency of outcome for victims of APP fraud between different financial institutions. We hope that the final code will be adopted quickly by firms in 2019 and interpreted in the spirit in which it was drafted to ensure maximum impact. If the code is not voluntarily adopted by firms, we would support making the code compulsory or legislation change which will help to protect victims of APP fraud.

The Scams Team were pleased to be invited to be an observer member on the APP Scams Steering Group and believe that the creation of the draft code has been a largely positive process, attempting to balance industry and consumer representatives and challenge assumptions on both sides to create a better code. In the rest of this response we will set out our views on the unresolved issues set out in the consultation document as well as pick up on some of the specific details of the code which we believe could be improved.

Scenario outcomes

Victims should always get their money back if they have met the level of care in the code – in other words that they are not responsible for the fraud as defined in the code. It is important that the process of being reimbursed is the same for the victim regardless of whether the firms involved have met the standards set out in the code. As a result, we agree that the victim's firm should administer the reimbursement in all cases, regardless of where the funding for the reimbursement is ultimately coming from.

In the so-called 'shared blame' scenario, where neither the firms nor the victim have met their level of care, we suggest that there should be some penalty on both the victim and the firm. However, we recognise that the impact of the fraud on the victim may be severe, and that firms may wish to make some reimbursement to the victim. As a result, we would support a system where firms were required to pay the cost of the fraud into a pot used to fund the 'no blame' scenario reimbursement but may at their discretion pay up to 50% of this back to the victim instead of into the pot. We are reluctant to support a system where the firm can choose whether to pay the full cost direct to the victim or into the 'no blame' pot, as we expect that firms will almost always choose to refund their customer, leaving the pot underfunded. Moreover, this would weaken the rationale for consumers to follow the level of care prescribed in the code as they would be reimbursed anyway.

Where firms and the victim have met their level of care, victims should be reimbursed. We are strongly opposed to a consumer funded option where consumers can purchase insurance against this type of fraud as it breaks the principle of consistency of outcome for victims. Moreover, an unintended consequence of this may be the rise of insurance scams which mislead customers. Some of the funding for reimbursement should come from the pot created in the 'shared blame' scenario, however this may not be sufficient to cover the total costs of reimbursement in the 'no-blame' scenario. We believe that the rest of the funding for this scenario could come from a number of sources, including the proceeds of regulatory fines resulting from breaches or failure of care which contribute to the likelihood of fraud being perpetrated – for example data breach fines issued by the ICO or FCA fines related to the behaviour of financial institutions. However, this source may not be available at the outset of the code, and moreover may not be sufficient to cover the total costs of reimbursement. Therefore, we would also support the idea of a contribution mechanism across all parties with an ability to prevent APP scams. Such a mechanism could also be used to fund the management of the scheme, including governance and auditing processes (covered below).

Governance of the code

The NTS Scams Team believes that getting governance arrangements right is essential to ensuring the code achieves its aims, in particular ensuring greater consistency among different firms. We suggest that there are two separate parts to the governance arrangements: auditing of decisions made by firms and communicating best practice to ensure consistent application, and managing reviews and additions to the code.

The first role is particularly important since victims will not have enough information to assess whether their bank has made a fair decision when they refuse reimbursement. Some victims will take their complaint to the Financial Ombudsman Service and it is important that the code facilitates this. However, as recent FCA research has shown, not all victims who are dissatisfied with the decision will make a complaint. Auditing is therefore important to establish confidence in the new code and may be done on the basis of a sample of claims rather than auditing every decision.

Auditing is also important to ensure consistency across firms in the process of making a claim and the treatment of victims, as well as in the messaging to customers in how they can avoid falling victim before and during the transaction process. On the basis of their work, the auditors would be able to make recommendations to individual firms on how to improve their application of the code as well as make recommendations for changes to the code itself. They could also be responsible for communicating best practice across the sector and providing case studies of how firms are interpreting the code. The NTS Scams Team currently performs an auditing function for the Mail Providers Code of Practice which operates in a similar way to this. We have trained mail providers to identify mail which is fraudulent and audit their opinions on the mail to provide assurance that they are meeting their legal obligations. The team have also created a new intelligence sharing system for mail providers which allows them to flag criminals and prevent them from opening accounts with other mail providers. This kind of information sharing had previously been impossible because of competition concerns. We suggest that the auditing of the code could operate in a similar way and may bring additional benefits and new ways to prevent APP fraud. We would be happy to provide further details of how this might work if required.

The second requirement of the governance arrangements is a body to review and agree changes to the code. Our preference would be for the Steering Group to continue to do this as the work on drafting the code puts them in a unique position to understand the issues from a range of angles and

understand the intentions of the code. We are concerned that the other bodies listed in the consultation document as options, such as Pay.UK (formerly the NPSO) and the Lending Standards Board, have little expertise in fraud. However, we recognise the resourcing issues that may arise in continuing the Steering Group and suggest that the Joint Fraud Taskforce (JFT) could be approached to assist with providing resources.

As stated above, changes to the code could be suggested by the auditing body as well as by other interested parties. It is essential that the annex is updated regularly and used as a way to promote cutting edge best practice and the newest methods to prevent fraud.

Firms' standard of care

The NTS Scams Team is keen that the code should raise standards among firms rather than simply enforce the status quo. However, it will not be easy for some of the measures of the code, particularly in the level of care for firms, to be assessed externally. For example, we are unsure how firms will be able to demonstrate that they have fulfilled their obligations with regard to transaction risk analysis and flagging. Information about the systems used to handle this is likely to be commercially sensitive and it will be difficult for firms to be transparent about the performance of these systems. This is another reason why auditing of firms' adherence to the code could be valuable to establish consistency and build confidence.

Education campaigns by firms should be very explicit about the steps which customers need to take to protect themselves from APP fraud, how they can meet their level of care and the process for claiming reimbursement should they fall victim. There should also be consistency in language across the industry, perhaps under the Take Five brand or similar, to ensure that customers are not confused or required to take different actions for accounts with different banks. It would also be helpful if the messaging used during the payment journey was similar – the JFT Banking Interventions project is working on this aspect and should be able to provide some research and analysis on the messaging that is most effective in 2019.

Customer level of care

There are two criteria within the customer level of care that the NTS Scams Team finds unnecessary and inappropriate as currently phrased. These are R2(1)(c) and (d). The description of the intention of these clauses in the consultation document is also significantly narrower than the drafting of the code provisions.

While we accept that R2(1)(c) is a standard piece of advice in preventing fraud, there are very few cases, as described in the consultation document, where this is relevant in preventing an APP fraud. We are concerned that unscrupulous firms may use unrelated incidents such as sharing access to banking systems with their partner as an excuse not to refund a customer. As a result, we would recommend the wording in the code is amended to read:

> 'Recklessly sharing access to their personal security credentials or allowing access to their banking systems such as online platforms or banking apps *where this had a material impact on the fraud succeeding.'*

In the case of R2(1)(d), we are concerned that the current wording in the code is too broad to be easily evidenced or communicated to customers. The wording in the consultation document relates this provision to a very specific type of APP fraud, i.e. internet sales scams. However, the code as

currently written does not make this clear. We would recommend the removal of this provision altogether as discussion around the Steering Group alone has indicated that 'reasonable steps' the customer should take to make sure the person they are paying is the right person can be interpreted very differently. For example, is the customer expected to check on Companies House if the company they are paying exists and the details match the ones they have been given? We do not believe this would be a reasonable expectation in the majority of cases. If the provision is intended to refer only to a specific type of fraud, this should be made explicit in the wording of the code.

Vulnerability

We welcome the definition of vulnerability in the code and fully support the suggestion that those vulnerable to APP fraud should be reimbursed by their bank regardless of whether they have met the level of care. However, we believe that some firms may not be as familiar with this definition of vulnerability as others and may require further training in how to apply this. There is evidence of considerable variation in firms' assessments of vulnerability at present. Additional training may also be required on mental capacity as decision specific and fluctuating rather than static as historically interpreted.

Implementation

In order to meet their obligations under the code, banks should ensure they are signed up to counter fraud initiatives across the board and are actively communicating with their customers about fraud risks.

We see a role for local authority trading standards officers as advocates for victims of APP fraud, particularly those made vulnerable by circumstance. We believe this will be a natural fit as trading standards officers are skilled in dealing with consumer law and assisting consumers in making claims.

The NTS Scams Team can also offer training to firms on aspects of fraud, and particularly identifying vulnerability and mental capacity, should that be required.

Contact

For any queries or further information about this response, please contact the NTS Scams Team.

Response from Sunday Times newspaper

Dear sir,

Please find feedback from the Sunday Times newspaper on proposed industry code to protect consumers against APP scams.

The Sunday Times has been in contact with hundreds of readers who have experienced bank fraud over recent years, and has also highlighted a number of new scams. We have also raised concerns over the way victims of APP scams are treated by banks.
A frequent complaint is that the banks show little regard for individual circumstances of the victim, and are frequently slow to respond to fraud reports.

The Sunday Times broadly welcomes the positive steps taken in the code, which are clearly designed to keep consumers better informed and use new technology to reduce fraud.

It is encouraging that reimbursement and the mechanism for refunding customers at the heart of the code.
The use of employee training and, particularly analytics should form a core part of the code. Banks have the systems to trace and identify unusual payments and these should be used to help target fraudulent transactions.

More use should also be made of freezing funds and delaying transfers in the case of suspect payments. That this is referenced in the draft code is also encouraging.

However, there are concerns over the prescriptive nature of the seven grounds to refuse to reimburse consumers. Frequently, the definition of 'grossly negligent' or 'recklessly sharing' information is open to interpretation, where the banks are judge and jury. Often judgements are based with little evidence.
Different banks have different protocols, and many consumers are largely unaware what information it is appropriate to share - particularly with regards to bank security codes.
Customers cases are rarely assessed on an individual basis, with regards to the expectation of their knowledge and their circumstances. A prescriptive set of grounds would merely reinforce this.
Fraudsters have proved to be highly sophisticated in duplicating bank systems, and banks also have been poor in communicating the risk of fraud to vulnerable customers.
It is encouraging that the code identifies the need to assess on a case-by-case basis, and the individual customer capability.
This is a critical part of assessing compensation for any fraud victim. The Ombudsman must also consider this when assessing reimbursement complaints.

As well as reference to responsibility to the consumer, it would be encouraging to see more prescriptive guidelines emphasising the responsibilities of the bank.
The general expectations of firms, emphasises education, compiling statistics and customer aftercare. These are welcome.
But the code does not highlight other expectations on banks with regards to the steps they should take to ensure fraud is prevented.
This could include, by way of suggestion, a failure to stop funds leaving accounts after being notified of a fraud, or failing to answer fraud helplines when a customer calls.

This would, in effect, create a contract between the bank and customers with regards to proper behaviour.

A further concern remains over the opening of fraudulent accounts.
Prevention is better than cure, and stopping bank fraud must be at the heart of the new code. In a large number of cases seen by the Sunday Times, concerns have been raised over how fraudsters have managed to open accounts. In some cases this has been done with fake documents.
It is encouraging that part of the code addresses firms taking reasonable steps to prevent accounts being opened.
However, on top of this increased regulation and investigation of the opening of accounts operated by fraudsters must be a core part of the remit of the PSR or FCA. Whenever an account is identified as being operated by a fraudster, banks must be made to carry out a full investigation in to the security measures and Know Your Customer information supplied on account opening. A report should then be submitted to regulators. Regulators must also have the power to investigate individual cases in this way.
Banks which fail to spot fraudulent account opening should be made to reimburse customers, rather than the customers own bank.

The FCA and PRA should also compile statistics on recipient banks, in order to get a picture of accounts where fraudulent funds are being received.

While the code is designed to be voluntary, it would seem sensible for the it be compulsory for all banks operating current accounts, in a bid to protect as many consumers as possible.

Regards,

Money
Sunday Times

Telegraph Money's response to the APP Scams Steering Group's CRM Consultation Paper

Contents

Consultation response

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

We agree that firms must be incentivised to prevent fraud and we argue that this can only be done by asking banks to pay for refunds. We, and the majority of our readers, strongly support the introduction of confirmation of payee.

The warnings are welcome, however we are concerned about the level of specificity required. For example, consumers are likely to ignore pop-up warnings or warnings they see all the time. Therefore we feel there should be a clearer definition of a “specific warning”.

On response, we feel the victim’s bank should be required to contact the recipient bank within 30 minutes of a fraudulent transaction being reported.

One additional comment we would have is that we were disappointed that the code was not ready to be implemented on September 28, as had originally been planned. We would like to see these standards, and the code, applied retrospectively by those who fall victim to APP scams between that date and the date at which the code is finalised and introduced.

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.

The code must not become a “get out clause” for banks to avoid paying. For example, if a consumer ignores a generic pop-up warning about fraud (as explained above), this should not be held up as a reason they should not be refunded – particularly if the bank is also at fault.

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.

If the bank has failed to meet its requisite level of care to a customer there should be some requirement to issue a partial refund, the amount of which should be clearly defined.

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

The level of care a customer must take needs to be clearly defined within the code. The definition of gross negligence given would be difficult for many consumers to understand and judge themselves against. A list of examples of gross negligence would help consumers understand their responsibilities, although we recognise that this list cannot be exhaustive.

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 welcome the recognition that anyone can become vulnerable to APP scams, and that these people would be given extra protections.

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

We are happy with the timeframes suggested but are concerned that the complexities of the complaints process could mean a further wait before a customer is able to go to the FOS. Customers should, within reason, be able to take their complaint to FOS without having to wait for their bank to investigate a separate complaint following a negative decision to reimburse.

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

No strong opinions.

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, we strongly agree. Research conducted with 446 Telegraph readers found that the largest proportion agreed with this sentiment.

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 have no opinion on who should administer the reimbursement. Banks should be required to pay. In most cases the recipient bank will be liable. Where this is not the case, then some form of shared cost between the firms involved could be a fair resolution.

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?

Research conducted with 446 Telegraph readers found a tiny minority would be in support of a charge on bank transactions. An insurance policy, to be purchased by the customer, was slightly more palatable – but still supported by only roughly one in five.

The customer should not be made to pay.

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

We agree that an evidential approach is vital, but would stress that this cannot be overly onerous for consumers – ie. require them to provide evidence they would not reasonably have access to.

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

We would echo the above. Consumers cannot, for example, be expected to provide recordings of phone calls with fraudsters in which they attempted to ascertain their legitimacy.

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

There should be a requirement on recipient banks to prove the circumstances in which the fraudster's account was opened. In our experience, getting refunds for scam victims often hinges on this question, given that many use false documents, however it can be almost impossible for a victim to get this information. Any action which forces banks to provide evidence that regulations were followed would be welcome.

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

We are concerned that a customer may have to show they told the firm they were vulnerable, as many would not consider themselves to be so. Firms should have to keep a close eye on warning signs. For example, in many cases an elderly person entering a bank branch to transfer thousands to a new payee may not have flagged that they are vulnerable – but the out-of-character nature of the transaction should be strongly queried.

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

No views.

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

No, beyond that changes should be made with transparency in mind.

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

We agree that a 50:50 apportionment would be fair.

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?

While it is too early to comment on the ADR, any service should be industry wide.

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

No comments.

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?

A significant positive impact could be that banks are properly incentivised to prevent APP scams, but this will only happen if it is firms that are required to foot the bill. The suggestion that refunds will cause customers to become more relaxed is, in our view, incorrect, as few consumers will want to go through the experience of being scammed, even if they eventually receive a refund.

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 above. No further comments.

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

As above. No further comments.

Q23 How should the effectiveness of the code be measured?

The code can be judged a success if the overall amount lost in APP scams reduces, and the proportion returned to victims increases.

Reader comments

The following is a small selection of comments and emails received by readers of the Telegraph in response to our five demands published on Friday, November 9, and included in the links section of this document.

Member of the public 1 [x]
If a bank allows an account to be opened by a fraudster with fake ID then I think the bank should be liable for any resulting fraud.
Explicitly stopping banks hiding behind GDPR as an excuse to not help when fraud is reported would also be helpful, as would requiring all banks to have their fraud desk staffed 24/7 - there have been too manor cases reported in the DT where a fraud victim has not been able to get through to their bank in a reasonable space of time.

Member of the public 2 [x]
I fully back the Telegraph's demands to the consultation on the new rule book.The British Government should be doing what is best for its people, not what is best for Corporations. As an individual one has no power against Banks, so the rules must be fair for those who are defrauded.
If banks were liable, they would soon swing into action and minimize fraud. Why is it always such a fight just to try and get what is fair for the general population from the Government?

Member of the public 3 [x]
May I suggest that it cannot be that difficult for all High Street Banks to be made to insist that any new customers wanting to open new accounts must present themselves to the bank with their passports. The teller will confirm the customer is the one pictured on the passport and if a fraud is attempted the photograph is available for identification.
If the customer does not have a passport the teller will advise him/her that the bank is required to take a photograph there and then before an account can be opened. Also, any bank instructed to remit funds over a certain amount should text the client asking for confirmation that the order is genuine. Non High Street Banks must have confirmation from someone on the electoral roll that the client is genuine.
The bank should contact that person before opening the account. Any unusual instructions must be confirmed.

Member of the public 4 [x]
I totally agree with the five points you make to improve the proposed code without which it will be toothless.
However I would also suggest that any negligence or failure in its duty of care by a bank leading to the opening of an account used for criminal purposes amounts to aiding and abetting the fraud and therefore the bank should be criminally liable jointly and severally with

the fraudster to any party defrauded by the use of such an account whether or not the defrauded party has a contractual relationship with the bank concerned.
The only way to make the banks really sit up and co-operate is to make them criminally liable.

Member of the public 5 [x]
In my book the banks are very much at fault, they are attempting to force people to convert to electronic banking, the tactics they use are to close many branches and the branches left open have only two till positions and it is common practice for only one of the tills to be open, resulting in long queues, which is vexing.
Without electronic banking most of the frauds the article is concerned with would not be possible. I suspect the banks are quite happy with this as it is not their money, would they bring in more stringent safeguards if it were their money at stake, Why is the cheque system hedged with so many safeguards, perhaps the banks have been bitten before.
Under the present electronic system I wonder what the banks will do when we are all paupers thanks to bank fraud.

Links

Below are some links to our reporting of the code and the issue of bank transfer fraud, including case studies to highlight the impact of this issue.

Banks want you to foot the bill for paying back fraud victims – help us stop them:
https://www.telegraph.co.uk/money/consumer-affairs/banks-want-foot-bill-paying-back-fraud-victims-help-us-stop/

Here are the excuses banks make for allowing £1m to be lost to fraud every day:
https://www.telegraph.co.uk/personal-banking/current-accounts/excuses-banks-make-allowing-1m-lost-fraud-every-day/

'I lost £10,500 to eBay fraudsters and all I got was one call from the police':
https://www.telegraph.co.uk/money/consumer-affairs/lost-10500-ebay-fraudsters-one-call-got-police/

Code to reimburse scam victims could create 'get-out clause' for banks:
https://www.telegraph.co.uk/money/consumer-affairs/code-reimburse-fraud-victims-could-create-get-clause-banks/

'I lost £600,000 to a conveyancing scam – why will no-one help?':
https://www.telegraph.co.uk/personal-banking/savings/lost-600000-conveyancing-scam-will-no-one-help/

APP Scams Draft Voluntary Code
UK Finance response to the APP Scams Steering Group Consultation

Executive Summary

1. UK Finance represents nearly 300 of the leading firms providing finance, banking, markets and payments-related services in or from the UK. UK Finance has been created by combining most of the activities of the Asset Based Finance Association, the British Bankers' Association, the Council of Mortgage Lenders, Financial Fraud Action UK, Payments UK and the UK Cards Association. We and our members welcome the opportunity to respond to this consultation. This is an important issue that no sector can tackle alone. It is right that we all look at what more can be done to protect consumers from APP scams, stop money going to criminals, and to support consumers if they become victims.

2. The industry supports the intention behind the draft Code and the consultation and see them as a positive step forward. All need to work together to ensure we better prevent fraud and help ensure more consumers get their money back. We also support any future moves towards ensuring that all parties in the wider eco-system are involved, accountable, and carry the right balance of responsibilities and incentives for their part in reducing and preventing fraud. We believe this, given how many of the drivers of economic crime sit outside the financial sector[1], is an essential step that Government and regulators should take, perhaps through the Joint Fraud Taskforce (JFT).

3. Within that, it should not be forgotten that Payment Service Providers (PSPs) already do a significant amount to prevent, detect, and disrupt all types of fraud and the volume of APP scams should be put into context of the overall volume of payments. Figures (at Annex C) from the first 6 months of 2018 suggest that the volume of APP scams equated to approximately 0.0078% of payments in that period and is equal to around 2.9 pence in every £100.[2]

4. However, behind every case is still a victim who has suffered loss which is why the industry wants to do more. Firms will continue to invest in systems to protect consumers and reimburse victims. They will continue to have a strong focus on vulnerability of consumers.

5. The industry is strongly supportive of taking further steps to reduce APP scams and so will, in any case, introduce measures in line with elements of the draft Code standards on what is expected of PSPs (provided that any unintended consequences can be managed). Most members are also content to increase compensation of customer losses where the PSP is at fault and the customer has met clearly defined standards of care. However, as below, the standards of care expected of consumers and evidencing that will be fundamental to the successful operation of the overall Code.

6. However, whilst supportive in principle, given the complexity and the importance of the outstanding issues still to be resolved most PSPs will only be able to take a view on their stance towards the challenges of implementing any further elements of the Code once the detail has been developed. All parts will need to work in a holistic way to avoid unintended consequences.

7. As well as unintended consequences there is a need to consider the operational feasibility of the Code. A final Code in early 2019 which includes a clear implementation timetable is laudable. But we should not underestimate the challenges and the time required for many PSPs to implement these standards given the changes IT, processes and systems required to support the aims of the Code.

8. We also should not underestimate how difficult some of the measures may be for new and challenger PSPs to put the Code in place quickly given their business models (designed within the context of the

[1] NCA National Strategic Assessment of Serious and Organised Crime 2017
[2] Based on UK Finance APP Scam management information and Faster Payment management information.

legal and regulatory framework set by Government). Many smaller PSPs have highlighted the very real difficulties they will face in implementing this Code, and the risks of creating a two-tier approach towards both APP scams and inconsistent outcome for consumers.

9. It is important a reasonable and workable implementation timetable is developed. Given the range of different business models of PSPs the timetable and Code will need to be calibrated accordingly to size and type of PSP as one size cannot and should not fit all. As such we believe the Code should be explicit that the PSP standards in any Code will need to be implemented in phases following the consultation given the changes to processes and operations required. We also believe a clear commitment to a phased approach will help manage the risks of unintended consequences of a one size fits all approach, including potential anti-competitive effects.

10. There is concern that unrealistic expectations have been raised as to what can be done by early 2019, including the extent of implementation and a perception that nearly all consumers will be reimbursed. Not least many of the more difficult issues were not resolved prior to the consultation and further work is required to address these issues for the Code to be successful. These are:

    - the expected customer standards of care and how to evidence that;
    - the source of funding for reimbursement in no blame scenarios;
    - developing a timetable for implementation;
    - developing a complaints process that aligns with current DISP rules, and the aims of the Code;
    - apportionment of liability between PSPs and how to resolve inter PSP disputes;
    - the potential impact on competition, how this sits with competition law;
    - what happens when one or more of the PSPS involved are not signed up to the Code;
    - how this interacts with the impact of the extension of Open Banking, particularly where PSPs may have little interaction with the customer or the customer journey; and
    - the future composition of the SG and the governance of the Code.

11. The complexity of these outstanding issues should not be underestimated. Furthermore, there is a very strong view that that some elements that may otherwise be desirable to have in a Code will require a regulatory framework. We need to recognise the law on liability has been set by HMG and regulators, after careful consideration of how the payments system should operate as to the benefit of all its users. This is why, as above, a voluntary Code can only go so far.

12. As such we would encourage and support the Government to regulate on many of the outstanding issues, particularly those relating to liability and competition rather than seeking to address in a voluntary Code. This would provide certainty to all involved and help avoid some of the current risks including any unintended consequences of Code having an anti-competitive impact. This is particularly in terms of impact on smaller PSPs and/or those who do not have full access to all the necessary infrastructure to implement the Code such as Confirmation of Payee (CoP) or who rely on other PSPs to provide a clearing function. It is essential the Code is voluntary to help, in the interim, mitigate some of the risks around competition impacts. It also needs to be clear that expected standards for PSPs are reasonable and proportionate to the size and type of PSP. However, given the FOS are to give weight to the Code it, this will drive approaches and so it would be desirable to provide more certainty through regulation

13. Regulation would help provide important consumer protection and ensure that HMG and regulators can carefully consider what are the right drivers in the system, where liabilities should sit and the right balance between growth and control. It would create a set of minimum standards for all to adhere to (or very clear criteria on who the Code covers and does not cover) as well as ensuring that responsibilities and liabilities are clearly defined for all parts of the eco-system (such as Payment Initiation Service Providers (PISPs)). It is the best way to ensure consistent consumer outcomes.

14. Alongside that, a regulatory steer or regulation is also required to balance the apparent tensions between the Payment Services Regulations (PSR 2017) and the Code. Many firms believe there is a tension between the PSR 2017 and the Code as firms are required to ensure payments are initiated and confirmation provided to the Payment Initiation Service Provider (PISP) or customer immediately.

PSPs are under scrutiny from the PSR to ensure that customer journeys do not contain any unnecessary friction, so there are challenges how a voluntary Code that can lead to a delay in payments will sit with PSR 2017. As the PSR oversee the relevant regulations and established and directed the SG to deliver a voluntary Code we would welcome the PSR providing a clear steer on this issue. This will help avoid unintended consequences and inconsistent application across PSPs.

15. [✂]. The industry believes this process should be undertaken by the PSR. [✂]. We believe the SG should be reconstituted to be more formally overseen by the PSR – not least they have, rightly, played a controlling role as to the direction of the group.

16. As we believe that without regulation, the voluntary Code will only be able to go so far in resolving outstanding issues. We must make clear that involvement in the working groups (evidencing the standard of care expected for consumers; options for funding 'no-blame' scenarios'; and options for designing a mechanism for resolving inter-PSP disputes) is not the same as industry agreeing to own these issues. Despite the commitment of all involved, we may not, for example, be able to identify an acceptable voluntary solution for a funding source for reimbursing 'no blame' scenarios.

17. We do not believe it is right that in those cases where it has been agreed, including by consumer groups, that neither PSPs nor consumers could have reasonably been expected to prevent the scam from happening (e.g. because the cause of the scam was a vulnerability in another sector) that PSPs should be the long-term funding option. It does not incentivise consumers to take care (and so could drive up fraud) and would lead to PSP consumers underwriting the costs of failings in other sectors.

18. There is also a need to ensure that the standards for consumers are reasonable and fair and that incentives are put in the right place to ensure consumers take reasonable steps. We need to ensure that any scheme does not act as driver for increasing money going to criminals by reducing the care consumers take or even PSPs being targeted for first party fraud. Our own research suggests this should not be controversial. Consumers understand the principle of having to demonstrate reasonable care when making an insurance claim.

19. Ultimately whilst our members support the aims of the Code, they do believe that if the aim is to reduce scams, protect consumers and prevent money going into the hands of criminals, there needs to be a stronger regulatory and Government focus on resolving longer term issues such as repatriating funds to victims. Without this we believe that the Code fail in its aims to reduce scams, protect customers and prevent money going into the hands of criminals. A voluntary Code unsupported by regulation will forever be a short-term solution that simply ensures that APP scams is still attractive to criminals, but that PSPs are compensating more victims in the absence of an effective public-private partnership approach to preventing scams.

20. Calling it a reimbursement scheme is a misnomer as this is about when PSPs will compensate victims. The stolen money is still in the hands of the criminals which is why we need a focus on increasing repatriation from criminals. This would ensure more consumers, even those at fault, get their funds back, and reduce the size of the funding source for 'no-blame' scenarios. Given the opportunity for a more effective approach we are disappointed on the progress by Government to unblock the legal issues preventing repatriation. The technology now exists to quickly follow, trace, and even potentially recover the proceeds of APP scams thorough the UK financial system. However, the legal and regulatory framework to support this does not. This work should be prioritised.

21. Finally, we are struck by how this work is out of step with the wider work on economic crime. We believe that this work should now be brought under the auspices of the Joint Fraud Taskforce (JFT) which has representation from across Government, regulators, law enforcement, the private sector and consumer groups. As the NCA Strategic Threat Assessment recognises the threat is growing and many of the drivers sit outside of the financial sector (e.g. ISPS and telecom companies), so there is a need to consider how the Code should ensure that the right incentives sit for other sectors who need to play a part in preventing and reducing scams.

Consultation Questions

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

- We are supportive of the principles set out for firms in the code. Irrespective of the publication of the Code PSPs want to do more to detect, prevent and respond to scams as well as educating and warning consumers. However, many members have noted that the current standards, as drafted, need further work to avoid inconsistency and confusion. We believe further work is required to ensure that the standards and expectations are clearly documented, and as far as possible that there is basic a level of consistency across the entire payments industry.

- It is unclear what assessment there has been of the potential impact of the expansion of Open Banking. Account Information Service Providers and Payment Initiation Service Providers (AISPs and PISPs) could have relatively little interaction with the customer compared to other PSPs, including when payment initiation takes place. Given that the PSR has been working with industry to remove barriers for Open Banking providers we would request that the PSR provide a very clear steer as if to the use of warnings to consumers when using an Open Banking provider (in the same way as other warnings for other channels) is acceptable. We understand some PISPs have concerns over such an approach.

- We believe that further analysis is needed by the SG regarding PISP liability and how the Code would interact with the requirements on PSPs to comply with PSR 2017, including the Regulatory Technical Standards on strong customer authentication and secure communication which also comes into force in 2019.

- Equally, a number of members have suggested it would be helpful for the relevant SG sub groups to consider what is expected of receiving PSPs in terms of standards. This will again help ensure clarity and consistency as well as incentivising steps to reduce APP scams.

- On the standards themselves, many members believe there is currently too much subjective language in the Code, for example, words such as 'meaningful'. As far as possible, the standards would benefit from further redrafting to ensure there is greater clarity in order to avoid inconsistency for consumers.

- Many members believe that the standards on vulnerable consumers should be clearer. Whilst we appreciate that some vulnerable consumers may require additional protection, it should be noted that not all vulnerable consumers identify themselves in this way. A proportionate approach is required to prevent interventions creating undesired outcomes for some consumers. We believe this is an area where regulation could potentially help mitigate this by providing a framework for what any extra layer of protection should look like.

- [✂]

- The Code would also benefit from being clearer on how any potential tensions or conflicts with other legal and regulatory requirements should be managed. It needs to set out what happens in relation to Open Banking, and what this means for liability and expectations for PISPs to adhere to the Code. For example, some members note that as drafted SF2(1) is not aligned with the Money Laundering Regulations 2017 and should be redrafted accordingly.

- This is important as there are potential tensions between the PSR 2017 and the Code as firms are required to ensure payments are initiated immediately and confirmation provided to the PISP or customer immediately. PSPs are under scrutiny to ensure that customer journeys do not contain any unnecessary friction. Delaying payments is not consistent with PSR 2017

requirements. It also runs contrary to some PSPs business models which have been developed within the framework of legal and regulatory expectations.

- This issue has been previously noted by the PSR who stated that "*a PSP's principal duty is to obey its customer's mandate…[and] in the context of APP scams, since the customer has authorised the payment, the sending PSP's ability to prevent fraud is limited by its duty to comply with the mandate. While the sending PSP can try to dissuade a customer from making the payment in question, or notify him or her of the risks of doing so, in the end it is obliged to comply with the authorised instruction and will be liable for failing to do so. A sending PSP therefore has limited options when faced with a customer that is determined to make a payment."*[3]

- Now that the Code is in draft we would welcome the PSR providing a regulatory steer on this issue to avoid unintended consequences, inconsistent application across PSPs, or an anti-competitive stance. [✂].

- Whilst further work on the standards is required, it should be recognised that many PSPs have independently been taking many of the steps suggested in the draft Code and will continue to do so. There is a desire within the industry to take further steps to protect consumers, including introduction of many of the measures in line with the interim Code standards, provided that any unintended consequences outlined in the consultation can be managed.

- However, to implement the Code effectively, the specific measures will need to be calibrated accordingly to the size and type of the PSP. One size cannot be expected to fit all. We also must be careful to avoid any unintended consequences of a two-tier approach to APP Scams driven by a lack of capability as opposed to willingness. As above, some PSPs, particularly the smaller ones and/or those who do not have direct access to all the necessary infrastructures, will find it hard to adopt the same standards as larger PSPs.

- Not only could an inflexible approach reduce competition and consumer choice, it could also cause a shift in industry approaches on economic crime. Previously, the prevention of economic crime, including APP scams, has been an area where members are seeking to work in collaboration as opposed to competition. We do not wish to jeopardise this ethos.

- In any case, whilst clear standards and expectations are important, realistic expectations on timing could also be a key factor in the success of this aspect of the Code. There are challenges which will need to be overcome to implement this level of change across multiple customer channels and these should not be underestimated. This is particularly important when key areas of the Code remain outstanding, including customer standards of care and losses which are determined to be "no blame". All parts of a further iteration of the Code will need to work holistically for the Code to be successful and avoid unintended consequences. Otherwise it could lead to an increase in APP scams and inconsistency of treatment. Establishing the right standards of care for consumers and how to evidence that will be a key pillar required for the Code to be successful, including underpinning what is expected of PSPs.

- In the same way, expectations over an implementation timetable for PSPs after the consultation need to be realistic and reflect what is feasible. We should not underestimate the challenges and the time required for some PSPs to implement these standards. As above, there is significant regulatory change already underway, particularly for payment initiation with PSR 2017 and Open Banking. A final Code in early 2019 which includes a clear implementation timetable is laudable. However, it may be unrealistic. Not least CoP is another key element of the Code, so it is difficult to know how it can be fully implemented before that system is even in place let alone live and stable.

[3] https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Which-super-complaint-response-December-2016_0.pdf

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 do not recognise the risk that this provision may enable firms to avoid reimbursing eligible victims. All PSPs wish to protect their consumers, and act in accordance with the rules and regulations set down by the Government and regulators.

- This provision is key to ensuring a proper assessment is carried out on the actions of the PSP and the customer set against the circumstances of each particular case. There must be a balanced assessment carried out in order to provide a direct link to causation and loss. We also do not believe that assessment under this provision will lead to eligible victims being refused reimbursement. This provision aligns to the principle that responsibility and liability is properly balanced between consumers and PSPs.

- Some firms have identified that without this provision there could instead be a risk of an excessively binary an approach on liability and standards, not least as it could conflict with the other areas of the Code that have not been resolved, including no blame, shared blame and the requisite standards expected of consumers. Without these issues being resolved, too heavy handed an approach could, in essence create strict liability on PSPs which would discourage PSPs from subscribing to the Code in the first place.

- The biggest risk is rather about seeking to apply a one size fits all approach and unrealistic expectations on implementation – these are covered in more depth below.

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.

- We believe this needs to be tested more fully, so we would suggest running test examples through this scenario to identify the potential outcomes that occur.

- However, from a policy perspective, if we are pursuing a principle where all consumers who have met their standards of care should be compensated, then the corollary (if there are no extenuating circumstances such as vulnerability that contributed to the scam itself) should be that no consumer who has not met their standards of care should be reimbursed.

- In cases where the customer has not met their standards of care, and so triggered the initial action, but the PSP has failed to subsequently meet its standards of care, then the original factor in this loss still sits with the consumer. Some members are willing to explore if PSPs in these circumstances should be required to make some contribution towards either the consumer or instead, any wider fund used to contribute towards reimbursing those who have acted responsibly.

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

- Identifying appropriate steps is essential for the Code to succeed in preventing fraud and important for consistent outcomes for consumers. Otherwise all the responsibility and liability sit with PSPs which runs contrary to the legislation and regulation in this space. Equally it would not ensure the right drivers sit in the right place for seeking to prevent APP scams.

- The standards of care expected for consumers and how this will be evidenced must be clearly defined. However, the draft Code currently sets a very low threshold for customer standards with no need to evidence compliance with those standards. If this is not addressed, it will be very difficult for some firms, particularly smaller and newer PSPs to adhere to parts of the Code. They have developed business models in line with legal and regulatory frameworks and may not have the necessary resources to investigate and compensate consumers in all circumstances.

- More specific and clearer standards for consumers would partly address this issue by reducing the investigation burden and scope for dispute. It would help increase certainty for both consumers and PSPs on expectations and reimbursement under the Code. This in turn should help increase consistency of outcome and mean fewer disputes over liability.

- Without significant change to the current draft Code, it would be very difficult for firms to refuse a customer claim on the basis that the standards of care have not been met. For example, many members believe the reference to gross negligence should be removed as it suggests that consumers are not expected to take any proactive steps to mitigate the risk of APP scams. Consumers would need to have acted in a manner which was deliberately negligent before they would be determined to have failed to meet the standards of care.

- As currently drafted the Code does not support the fundamental principle that responsibility and liability for APP scams should be balanced across PSPs and consumers. Equally we believe that the very low standard of care for consumers currently defined in the Code could lead to an increase in APP scams as consumers view PSPs as effectively underwriting APP transactions.

- This perception could reduce the standards of care consumers currently take when making a payment (which the PSR recognised as a legitimate risk in their 2016 response to the Which super-compliant). Equally we believe a very low standard of care would lead to UK PSPs being targeted by criminals pretending they had been defrauded (i.e. first party fraud).

- These unintended consequences would increase the amount of money going to criminals. We know fraud is often used as a revenue source for organised crime involved in other areas, such as drugs or human trafficking as well as being often associated with funding terrorist financing.

- We believe consumers are comfortable with having to take steps to protect themselves and are well used to having to demonstrate they took reasonable steps to protect themselves in other areas – such as when making a claim on insurance.

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

- In broad terms, it is agreed that the Code should help ensure that consumers who may be considered vulnerable are protected. The industry takes its responsibility to vulnerable consumers very seriously, as evidenced by the creation of the Financial Services Vulnerability Taskforce and initiatives such as the Banking Protocol. More information on these is at Annex B.

- There is a general view that if the vulnerability contributed to the APP scam, then PSPs should consider reimbursement. However, in practical terms the Code does not go far enough in describing on how this aim should be put into practice. The commentary suggests that PSPs are expected to utilise a significant degree of individual interpretation to determine both whether the customer is vulnerable to the specific APP scam and if this has had a material impact on their ability to protect themselves. This approach could lead to inconsistent outcomes.

- We are aware of the FCA definition of vulnerability, and the expectation that firms should ensure that indicators of vulnerability are spotted and responded to in a considered manner. This definition would need to be refined for the more detailed aims and subject-specific purposes of the Code. However, having two definitions would create operational difficulties of adhering to different approaches to vulnerability. This is a challenge that will need to be considered by the SG in collaboration with wider public policy initiatives, such as the Joint Fraud Taskforce.

- The Code will need to recognise that vulnerability is both fluid and permanent and will need to be considered on a case-by-case basis as to if the vulnerability was a factor in the scam occurring. It is important to avoid a tick box approach of any indicator of vulnerability requiring reimbursement

as this could have unintended consequences, such as more restricted payment access for categories of customers with certain indicators of vulnerability.

- Equally, consideration will have to be given within the Code of how to reflect if the PSP could reasonably have been aware of the vulnerability and taken steps to protect the customer. This will be more difficult for many PSPs, particularly smaller ones, where much of the interaction with their consumers may be limited, and/or primarily through functions such as apps, messaging and other digital services.

- We suggest that there are further case studies conducted in this area to ensure proper protection for vulnerable consumers while managing the risk of unintended consequences such as restricted payment access. This work could help inform the definition of vulnerable consumers.

- The significant amount of work which firms are already doing to support vulnerable consumers against the risk of APP scams should also be evaluated. A 'strict liability' approach may undermine the support that many PSP's already have in place and avoid unintended consequences. The balance needs to be struck so as to ensure that vulnerable consumers do not find it hard to carry out day to day banking.

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

- In general, yes. Not least PSPs are being asked to investigate claims that a criminal offence has occurred. The timescales align to the PSD2 complaint timescales and are agreed in principle. This may be something that can be revisited once standards of care for customers and evidential standards have been established as this would give a clearer view of the investigations that firms may need to undertake. Members strongly believe that firms must be entitled to fully investigate a complaint and reach a resolution prior to the complaint going to the FOS. An alternative approach would not be customer centric as it would not facilitate a proper 'fresh complaints' investigation.

- Equally there needs to be recognition that different PSPs have different business models, so some PSPs, particularly smaller PSPs would not be able to easily work to swifter timescales given the complexity of some of these cases. Some PSPs also do not have 24/7 customer service teams in place. We do believe the Code would benefit from providing more clarity on what an exceptional circumstance would be. For example, if there are ongoing legal proceedings, it is not necessarily appropriate to have these timelines apply.

- We believe the SG previously agreed that if the customer had not supplied the necessary evidence required for the investigation within the 35 days (without mitigating circumstances) they would not be reimbursed. This should be reflected for full customer transparency.

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?

- In principle, the idea of an Annex is a positive one as it allows a measured approach to keeping the Code updated with relevant measures. However, the Annex does not distinguish between the measures and tools which are currently available or those which are in the process of being developed (currently the Annex could be interpreted that every tool listed is an industry standard).

- There is also 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, many of the measures rely upon direct contact with the customer as part of the payment initiation when payments are increasingly instructed through digital channels.

- It is important that the Code is clear on the optional status of the Annex, as a non-exhaustive guide. This is important to avoid confusion and inconsistency, such as where a PSP chooses to take a different approach to those listed in the Annex. [✂]. Here, as elsewhere, the Code needs to recognise that different PSPs have different business models and so will need to implement the measures and tools in different ways accordingly.

- In the same way, expectations over an implementation timetable for PSPs after the consultation need to be realistic over what is feasible. There needs to a reasonable implementation timetable that works for all PSPs and there needs to be an approach of proportionality taken. A final Code in early 2019 which includes a clear implementation timetable is an important aim, but we should not underestimate the challenges and the time required for some PSPs, even those involved in the SG, to implement these standards. Nor should there be raised expectations for the SG participants. This would be a disincentive to join such collaborative groups in future.

- We also want to reiterate that the PSP standards in any Code will need to be implemented in phases given the multiple changes to processes and operations required. We believe that phasing will also help manage the risk of unintended consequences of a one size fits all approach, including potential anti-competitive effects.

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

- In principle we do. However, if the PSP has done everything expected of them it would seem perverse that the reimbursement be expected to come from them. We are strongly opposed to the notion that PSPs should carry 'strict liability' for nearly every fraud, even if it is accepted that a PSP could not reasonably have been expected to have prevented the criminal activity from occurring. This was also the view of the PSR who stated they believe "*that a wholesale shift in liability to PSPs that requires them to reimburse victims of APP scams, even with an exception where the victim has not acted fraudulently or with gross negligence, is inappropriate*"[4].

- We believe nothing has changed since the PSR made this assessment. We also do not accept the argument that this is residual risk in the system which PSPs must manage. PSPs cannot for example easily or quickly detect when an account which has been opened legitimately and operated correctly subsequently becomes a money mule account. Again, the PSR have previously this and observed "*increasing the obligations for PSPs to do more checks before opening accounts could affect other policy goals. For example, it could conflict with efforts to increase competition in retail banking if it increases the barriers to switching bank and opening a new bank account. It is also possible that additional checks will deter some of those that are currently unbanked from opening an account. The problems faced by groups denied access to the banking system is something that policymakers, including the FCA, are keen to address"*.[5]

- Equally highlighting the risks of a 'strict liability' approach is not "banks blaming the victims". Far from it, we share the ambition for the UK to be safest place for consumers to do business. It is that we do not believe it is right that in those cases where it has been agreed, including by consumer groups, that neither PSPs nor consumers could have reasonably been expected to prevent the scams from happening (e.g. because the cause of the fraud was a vulnerability in another sector). In those cases, it would seem unreasonable for PSPs to simply pick up the costs of failings elsewhere where it has been agreed PSPs could not have stopped the scams occurring. This does not incentivise either consumers or other sectors to act responsibly. Additionally, as the PSR noted, consumers may face additional charges due to "industry underwriting" of APP transactions.

- As such, there remains a lack of agreement on "no blame" scenarios. It is not accepted that firms should fund the cost of APP scams when the firm is not at fault, has met the required standard of care and could not have prevented the financial loss for a transaction which has been correctly authorised by the customer. This is because fundamentally PSPs are not prepared to accept what would effectively be a 'strict liability' position where they automatically have to cover the

[4] https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Which-super-complaint-response-December-2016_0.pdf
[5] https://www.psr.org.uk/sites/default/files/media/PDF/PSR-Which-super-complaint-response-December-2016_0.pdf

long-term costs of nearly all APP scams, no matter the cause as this would undermine the whole intention of the Code.

- We believe the aim should instead be to raise standards across the board for PSPs and consumers so that the risk is reduced. This issue at essence is not about reimbursement but about who compensates the victim of a crime - the money is still going to the criminals. This is where there are good precedents elsewhere, be it the Criminal Injuries Compensation Scheme or Flood Re where charges are built into insurance products to provide a pooled risk fund to compensate consumers. This is supported by Government agreeing to step in and provide resources if the cost of a flooding risk exceeds the pot of funds available.

- We do wish to highlight that any move towards a 'strict liability' approach could lead to unintended consequences from a competition and public policy perspective. This has already been recognised by the PSR and members agree this could create very real unintended consequences by introducing barriers to operational and technical costs.

- The cost of funding APP scams may also be disproportionate for smaller PSPs who are forced to leave the market or restrict the profile of consumers they deal with and the type of business they can conduct. It could also act as a barrier to new entrants. It may be uneconomical for smaller PSPs who would be unable to mitigate their risk or quantify potential payments.

- [✂].

- Other risks include consumers who have profiles which are similar to those who have become money mules could be off-boarded as PSPs look closer at their risk profile and the liability it could pose. PSPs may also determine that payment functionality should be restricted. This creates other legal risks. It is important to recognise that while PSPs may be able to freeze payment accounts under the Proceeds of Crime Act (POCA), this power requires PSPs to have formed suspicion. This is different from the precautionary approach in the Code and so generates regulatory tensions. There can also be addition tensions arising from the POCA prohibition against tipping off the subject of a suspicious activity report. This will need to be resolved.

- It is credible to anticipate that the level of APP scams could increase if PSPs are effectively underwriting the risk of a customer making an APP. Consumers are likely to be less cautious if they are aware that they are not at risk and this is also likely to be exploited by criminals. This risk is heightened by the low threshold suggested for the customer standards of care.

- Therefore, we believe there is a better case for looking at other options, such as more easily unlocking frozen accounts containing illicit funds. Some members, but not all, would also want the option to pool risk in the same way as we see in the insurance sector, but a funding mechanism would be needed for this type of approach which does not include PSPs directly funding it. Alternatively, there would seem better ways to incentivise the right behaviours in other sectors, such as for HMG to use fines from data breaches.

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?

- This will depend on the final funding model. If there is a centrally administered scheme akin to the Criminal Injuries Compensation Scheme, then it may be appropriate for a consumer to be refunded by them rather than PSPs, not least as any fund holder may wish to assess if the consumer did act reasonably.

- However, in other scenarios, where a PSP has not met its standards of care it would seem easier for consumers to be reimbursed by the sending firm provided that the sending firm can easily access funds where the receiving PSP is at fault. That would be consistent with the principle that the sending PSP completes the investigation.

- This is linked with wider issues as to where PSPs may not be signed up to the Code. If the receiving PSP is out of scope of the Code, then it would not be appropriate for the sending PSP who has met their own standards of care to be expected to reimburse the customer.

- More widely there will be a need for a timeline and mechanism for resolving inter-PSP disputes, as well as for receiving PSPs to send, if at fault, funds to the sending PSP. This will equally apply if there is a separate entity that administers the 'no-blame' 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?

- As above, we do not believe that PSPs should be fully or directly liable to cover the costs of compensation in cases where it is accepted that they could not have reasonably been expected to have prevented the scams.

- We believe that examining funding options may need a multi layered approach in order to be sustainable. There are a number of different options, including to (a) allow PSPs to unlock frozen accounts connected to illicit funds (b) pool the risk by voluntary extra charges on certain transactions where the consumer can take out protection; (c) look at ways for other sectors who are exploited by criminals to pay into a pooled risk fund – so for example, we see mobile phone numbers being compromised and ISPs failing to carry out comprehensive KYC on sellers; (d) use fines from data breaches to refund victims since the aim of exploiting stolen data is in the vast majority of cases to get financial benefits through defrauding a victim.

- Even where consumers are compensated in 'no blame' scenarios, their scammed funds are still going to criminals which will often be used to fund other serious and harmful crimes. That is why we are frustrated that more progress has not been made on the legal issues around unlocking frozen criminal funds.

- Equally, it is cause of considerable concern that there is no real pace on efforts to redress the fact that even where the stolen money has been traced, PSPs have no easy legal vehicle to take the money from a criminal and return it to the victim in the absence of a court order. In doing this, particularly in the absence of any regulatory steer, PSPs are exposing themselves to greater risk of challenge. This is both alleged criminals (and it is important to note PSPs cannot investigate to the level of law enforcement) who argue that their customer mandate has been breached and from other victims who may argue the proceeds in an account was originally their funds.

- We should instead be far more ambitious in this space. The technology now exists to quickly follow, trace, and even potentially recover the proceeds of fraud thorough the UK financial system. However, the legal and regulatory framework to support this does not. This work should be prioritised as not only would it be transformative on fraud, but also the technology could, in theory, be extended to cover other forms of illicit finance such as the proceeds of crime.

- We would welcome Government and the regulators seriously focusing on this issue. In the absence of the legal and regulatory change PSPs are unable to take the steps necessary to increase the value of funds recovered from criminals and cannot exploit the full benefits of technology. However, whilst fraud continues to be profitable for criminals it will continue to grow, and fraudsters will continue to invest in technology.

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

- Clarity on the evidential approach for all parties is critical to the success of the Code. To be successful there will need to be clarity on evidential standards from consumers and may require those in vulnerable situations to provide some material to help the PSP (and if necessary the FOS) to reach a decision. If there is not clarity, or there is an unevenness in terms of what evidence is expected then this will create inconsistencies in application and treatment for consumers. The work on consumer standards of care is fundamental to the success of the Code.

- Firms will have to show what parts of the Code they believe they comply with and how, and consumers will have to demonstrate that when making a claim to the PSP. Given the FOS will act as an adjudicator, that will ensure that consumers have a right of redress if they feel they have been unfairly treated. However, in doing this, there is a need to set clear principles now that PSPs should not be expected to have to share publicly with consumers any material that could help criminals. This could include the criteria influencing risk-based decisions or the KYC material to show how money mule accounts were opened. As far as possible, the evidential standards framework should be confidential to help reduce the risk of first party fraud or 'coaching 'of victims on what to say when making a claim. None of this would preclude the FOS from being able to query these decisions if relevant.

- Some smaller PSPs have raised concerns as to what evidence would need to be provided to the FOS, and what is expected for them to demonstrate they have the right controls in place. Equally, there is a serious concern about if there is an approach of comparison between the PSPs, particularly between smaller/larger PSPs. The FOS will also need to understand the equivalency of controls some challenger and FinTech firms have in place in absence of 'normal' banking standards otherwise it will create anti-competitive impacts. The SG will need to consider this before the Code is issued.

- A body overseeing the Code will have to ensure that the principles of the Code are delivered against, and this includes that outcomes are predictable and reasonable to all parties. There is still the issue to be resolved on scenarios where only one PSP is signed up to the Code.

- Lastly, some smaller PSPs have noted extending the jurisdiction of FOS may have another unintended consequence. Firms are required to pay a £550 fee for every referral. Criminals may soon be aware that consumers are more likely to get an automatic recovery for these lower value payments as the time and cost associated with FOS referrals is not economical for some PSPs.

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

- We agree it is important that there are a clear set of principles and criteria developed that will allow PSPs to properly and consistently come to a view on whether consumers have taken reasonable steps to protect themselves.

- We do not believe that this is a controversial approach – this principle is well understood by consumers when making an insurance claim. However, if a solution is not reached, then we believe regulation would be the right route to follow.

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

- We would like further consideration on if and how any previous evidence or intelligence that an individual has been suspected of making fraudulent claims can be considered in the decision making of a PSP, and how this information can be passed to the FOS in the event of any appeal.

- The working group needs to consider how the evidential standard would be met where there are multi-party PSP's involved in each transaction. There is also the issue to be resolved on where only one PSP is signed up to the Code, but another is not. Resolving this, as well as consumer standards of care is critical to the success of the Code. Many consumers are multi-banked so divergence across different banks would be visible quite quickly.

- This equally applies to where some PSPs are not signed up to the Code and/or where some 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?

- It is inherently difficult to define a vulnerable customer. As the consultation describes, most consumers can become vulnerable to APP scams at any point in their lives, for many different reasons. Balancing the PSP duty of care and privacy of consumers is difficult. PSPs are very limited in how an operational team can establish whether a customer is vulnerable and determine evidence of that vulnerability, particularly if their direct contact with the customer is limited (which is often the case for some of the business models of our smaller and challenger PSP members).

- There is a need for tangible evidence to mitigate first party fraud and clarity to help consumers understand what could be expected. However, this will need to be handled sensitively given that PSPs will be dealing with vulnerable consumers who have suffered a loss. As such, whilst some guidance should be provided, given the sensitivity, each case should be treated on its own merits. As we indicated earlier, further work on case studies may help to form an industry view on common indicators and develop acceptable parameters.

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

- The most logical outcome is for the PSR to own and oversee this Code. They have driven this work and established the SG and have decided what outcomes they want the Code to achieve. Equally, they have the function and remit necessary and have the authority to perform this role. They are also the body who should opine on where the balance should be struck on some of the areas of regulatory tensions we identified above.

- [✂].

- [✂].

- UK Finance cannot be the replacement body remove as this could create conflict of interest issues, and it is important that the body is seen as independent from the financial sector. One alternative model is the Lending Standards Board which is independently constituted as a legal entity.

- Another more responsive model, given that the drivers of APP scams also sit in other sectors, is for the PSR to be the deciding body on the Code, but then for the wider governance to be brought within the Home Office led Joint Fraud Taskforce (JFT). That would be consistent with the Government's economic crime reform strategy and the importance of stronger public private partnership working and the need for a more holistic and strategic approach to economic crime.

- This would allow the JFT to ensure that all relevant parts of the public and private sector could be brought into discussions as necessary on the Code. It would also allow a mechanism for the Government to challenge the financial sector as to whether the Code goes far enough, whilst allowing the payments sector to highlight areas of legal and regulatory concern which act as a challenge to implementing the Code. This also provides the right mechanisms for law enforcement to feed in their views and any relevant intelligence.

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

- The most important thing is to allow the Code to be implemented and become operationalised and consistent over time before looking to make any swift changes. Changes need to be scheduled, consistent and tested before they are made in order to ensure there are not perverse outcomes and that PSPs can properly plan.

- Once established, we would propose a mechanism of identifying issues at a 6-month period, working up options and then consulting as necessary, before agreeing those changes annually, ideally with an agreed timetable for adoption. Ahead of that stable state being reached there is a case for allowing changes to be proposed on a 6-monthly basis.

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

- There is no consistent agreement by members, but this needs to be resolved before any or all elements of the Code can go live. As above, clarity on expected standards by sending and receiving PSPs and consumers is essential for the Code to operate effectively. This will need to include clarity on what happens when only one PSP has signed up to the Code and/or where responsibility and liability is drawn when PISP or agency PSPs are involved in the process.

- On the approach itself, it is administratively more straightforward and less likely to lead to disputes. However, we need to be careful that a blanket approach does not lead to unintended anti-competitive impacts, particularly with regard to larger PSPs being more easily able to absorb the costs of a 50/50 approach.

- Equally it could be argued that this approach does not act as an incentive to all PSPs to drive down APP scams. A more equitable approach could be to have different levels of apportionment depending on the extent of the blame, so some members want further work to test scenarios.

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?

- They seem a good starting point. However, we note they have 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 so as to avoid creating a backlog of outstanding decisions.

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

- That decisions are made quickly, are consistent and understood and that there is consideration frequently given as to whether the impacts are causing unintended consequences around competition or favouring PSPs who have taken less care. There are also the risks of uneven treatment when one PSP is signed up to the Code, but another is not.

- From an operational point of view, this will also depend on which body is running the dispute mechanism as it may take some time to get this body in place and up skilled.

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?

Positive

- There is a view this could lead to fewer victims as the Code starts to be rolled out and CoP is delivered, implemented, and starts to take effect. It would also deliver a more consistent approach to victims and ensure more consumers are reimbursed where PSPs could have done more to prevent the scam, or where the consumer is vulnerable.

- If agreed, it could/would deliver clearer expectations for consumers on what steps they should take to protect themselves and a right of redress to the FOS for APP scams as well as ensuring firms are continually taking steps to reduce APP scams.

Negative

- There will be significantly more friction in the system for genuine consumers. There is also the risk of raised and unrealistic expectations by consumers that they will be reimbursed for APP scams in all circumstances. We believe this is a significant risk, so the parameters will need to be carefully communicated and the principles endorsed by the PSR.

- There is a risk of the UK becoming a target for criminals if there is not a focus on repatriation (as opposed to compensation). Criminals will exploit any indication that consumers are more willing to authorise payments or move funds if there is an expectation they will be reimbursed. That is why it is important to address the barriers to repatriation to disrupt the criminal business model.

- Other risks include inconsistent application across the industry and inconsistent outcomes for consumers, as well as consumers having to justify the steps they have taken to protect themselves or having to explain a vulnerability that they would rather keep private. All these will need to be mitigated by sympathetic customer service and privacy as to circumstances. The public sector agreeing a consistent definition to vulnerability would be helpful as would a greater willingness by the public sector to seek permission to share details of vulnerability with PSPs where appropriate (or to suggest to the individuals they are dealing with that they do so).

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?

Positive

- A clear set of principles and standards to adhere to, and clarity on what is reasonable for consumers to do to protect themselves, as well as, if resolved, a clearer approach to disputes and reimbursement. It should lead to more consumers being protected and refunded and a Code endorsed by consumer groups supporting greater public awareness.

Negative

- There could be raised expectations from consumers that that they will be reimbursed in all circumstances. The parameters will need to be carefully communicated and the principles endorsed by the PSR.

- There is a lack of clarity as to how the Code applies to PISPs and MSBs which could impact smaller firms. Equally, firms will have to evidence to the FOS that they have implemented the measures they are signed up to effectively which may be harder for smaller PSPs and FinTechs that lack the resources to do so. There is a risk the relationship between the Code and DISP complaints is not fully worked through so PSPs have to apply complaint principles (and this distorting their complaints figures) for cases where the customer is not complaining.

- Another risk is scope creep – whilst this is a voluntary Code there is a risk that the FOS could start to extend all parts to PSPs that have not signed up to it all, have not finished implementation or have not agreed to implement the Code. This will require the FOS to take a proportionate view and for the status of the Code to be clear from the outset.

- As above there are possible anti-competitive impacts on smaller PSPs. This can be partly mitigated by the Code being flexible as to how the measures are implemented and to what timetable. There also needs to be careful review of inter PSP disputes. Longer term the best mitigation is for the PSR to own and regulate as necessary on the Code.

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

- As a result of PSPs taking steps to scrutinise more payments, consumers are more likely to suffer delayed and blocked payments and could be required to provide more information about their circumstances. This could lead to increased challenges and complaints to PSPs. This could be mitigated by the PSR and the FCA making very clear that PSPs are acting in good faith to investigate payments that may be a person being scammed are protected. Legislation would be needed to ensure that this can be operated effectively.

- Consumers may find it more difficult to access payment services if PSPs are held liable on a no blame basis and a customer has made multiple claims. The impact on the customer experience for Open Banking is also unclear.

- As noted previously, competition could be hampered, with a decrease in range of services and products if smaller PSPs find it harder to access market, become less competitive as a result and or cannot innovate. This will need to be part mitigated by the steps above.

- Depending on the funding model for no-blame, possible increases in fees and charges to consumers to fund non-blame. It could also see legitimate consumers who fit risk profiles of being higher risk of becoming a money mule may find it harder to access the full range of services and products on offer from PSPs or face more restricted controls on what they can do.

- The FOS will need to act 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 of a scam. The paying customer claims they are the victim of a scam and requests the monies are returned. If the receiving PSPs 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 the title to the money is with the payer or the recipient.

- Enclosed at Annex A which members is a list of questions and issues firms believe the SG still need to consider.

Q23 How should the effectiveness of the code be measured?

- A simple reduction overall in APP scams alone would not be an accurate and useful metric. Whilst we would expect to see a reduction in APP scams, particularly once CoP is introduced, we note law enforcement threat assessments show that increasingly organised criminals and hostile actors are targeting the UK financial system and UK consumers for the purposes of committing fraud.

- A sole focus on complaint reduction is misleading given that the failure could lie elsewhere, and it is not clear how PISPs are in scope. Equally some PSPs could have robust prevention controls, but if the customer logs a complaint as the driver is purely reimbursement and so escalates to the FOS that is not a reflection on the PSPs controls or adherence to the Code.

- We believe a light touch range of metrics should be developed including increased reimbursement of consumers who have met reasonable standards of care and PSPs will need an appropriate amount of time to set up reporting against the decided measures.

Annex A: Issues to be resolved and additional questions.

Some members have highlighted that in the draft code APP Scams is defined as a transfer of funds sent by Faster Payments or CHAPS, or transferred internally that is authorised by the customer (as per Reg 67 PSR) where:

- the customer intended to transfer funds to another person, but was instead deceived into transferring funds to a *different person*; or
- the customer transferred funds to *another person* for what they believed were legitimate purposes but were in fact fraudulent.

Many firms have online savings account where as well as that account the customer must also have a nominated account in their own name. This means that money can only be transferred in and out of their savings account with them via their nominated account (usually their current account). On a very strict reading of the APP definition, these accounts would not be captured by the code as there is no transfer of funds to a *different/another person*.

However, if the customer is then subsequently deceived into transferring the funds from their STB savings account to their current account, and then deceived into transferring funds from their current account to a fraudster or for fraudulent purposes it raises several issues around:

- who is liable particularly if that nominated account is with another PSP?
- would the customer claim under the CRM against their current account provider as that is where the funds went from them to a *different/another person*?
- where the transaction originated?

It has also been highlighted that in section 3.15 of the draft code it talks about the first-generation account and it is suggested a better definition of this would help in the scenario above.

Members have also identified a number of other questions where there would welcome the Code providing clarity. These are below.

1. Clarification to understand if consumers who have an account in the 'isles' are out of scope in the CRM.

2. 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?

3. 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)?

4. Clarification that currency accounts are out of scope.

5. The scope of push payments technically includes BACs direct credit payments, but this is not reflected in the Code. We would appreciate guidance on whether or not these are in-scope, given that consumers can initiate payments using third party platforms, or direct submission into the payment system itself. If so, where would the responsibility to adhere to the Code sit?

6. 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.

7. 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.

Annex B: Further information on some of the measures taken by the financial sector on vulnerability.

In 2016 – in response to the FCA's 2015 Occasional Paper Consumer Vulnerability – the industry established the Financial Services Vulnerability Taskforce, chaired by Joanna Elson CEO of the Money Advice Trust. The Vulnerability Taskforce Report Improving Outcomes for Consumers in Vulnerable Circumstances recognised that vulnerability can be fluid, temporal, and specific to an individual's circumstances.

The report concluded with nine high-level principles and a series of recommendations which the financial services industry has actively sought to employ as a consistent framework for delivery. High street banks and building societies and other financial services firms agreed to implement the new set of recommendations and principles under the Vulnerability Taskforce.

Good progress has been made towards the identification and support of vulnerable consumers in a range of product and service areas and, importantly, vulnerability policies are embedded within and across organisations – a clear indication of positive shifts in firm culture. Working alongside consumer groups, government and other experts, as part of the industry's wider commitment to provide the best possible service for those who may need additional support, we have completed/or are in the process of completing industry wide work on delivering on a wide range of projects. One of the Principles in the Report is Principle 6 – Scam Protection where the industry has implemented a range of measures to protect consumers and target the unscrupulous fraudsters who prey on them.

This includes the Banking Protocol, a scheme that allows bank branch staff to contact police under a quick-response guarantee if they suspect a customer is in the process of being scammed.

The Banking Protocol has been rolled out across the entire UK, including Scotland and Northern Ireland, with all 45 police forces using the process since March 2018.

Branch staff, call handlers, police and trading standards officers in each area have all been trained in the Banking Protocol and the steps that need to be taken when a customer is at risk. As well as stopping frauds taking place, the initiative ensures a consistent response to potential victims and gives them extra support to prevent them becoming a victim in the future. This kind of joined-up approach is crucial to stay one step ahead and ensure that unscrupulous scammers preying on consumers are brought to justice.

Since the Banking Protocol went live nearly £37m has been prevented and 5,319 emergency calls have been made by bank branch staff, resulting in 336 arrests (figures from October 2016 to September 2018).

We have also looked at non-system-detectable financial abuse and have published a voluntary Financial Abuse Code of Practice which can help members build out their policies and provide more consistent support to victims of financial or economic abuse.

Annex C: Calculation of volume and value figures on APP Scams

Data Sources –

APP Scam Data (https://www.ukfinance.org.uk/wp-content/uploads/2018/09/2018-half-year-fraud-update-FINAL.pdf) – UK Finance Half Year 2018 Fraud Update (Page 19)

Faster Payment Data (http://www.fasterpayments.org.uk/sites/default/files/Quarterly%20Statistical%20Report%202018%20Q2.pdf) – Faster Payments Quarterly Stats (Page 4)

Calculation:

For the calculation we have used the total number of scam payments in H1 2018 (regardless of payment channel) and divided by the total number of Faster Payment (Single Immediate Payments) to give us an overall %. The same has been done with values to give us an overall % which has then been translated into value of fraud per £100.

It is important to note this is the best approximation as we are not comparing like with like. Fraud totals include all payment channels whilst payments relate to FP SIPs only. We have used this approach, even though it results in a higher % of fraud per transaction and £ per transaction figures as we do not have and cannot include the genuine transaction volumes for all payment channels – they are therefore excluded from the genuine payment volumes and values but not from the fraud totals.

All data below for H1 2018:

Volume:

Total Scam Payments	-	50,966 Total
Faster Payment: SIPs	-	648,647,000
Outcome	-	0.0078% or 1 in every 12,727 payments being associated with an APP fraud case.

Value:

Total Scam Value	-	£145.4mn
Total Faster Payment: SIPs	-	£500.8bn
Outcome	-	0.0293% or 2.9pence in every £100 processed.

Consultation Response to APP Scams Steering Group Draft Contingent Reimbursement Model Code

Dr Steven Murdoch, University College London

Thank you for the opportunity to contribute to this consultation, my response is not confidential and may be published and shared with the Steering Group in full.

The introduction of a Contingent Reimbursement Model is an unconventional approach to consumer protection and the Steering Group have made an admirable attempt at tackling the difficulties this creates when compared to more conventional approaches like the Consumer Rights Act and the protection against unauthorized transaction in the Payment Services Directive. These difficulties particularly result from the complex criteria that fraud victims must meet in order to be reimbursed and from the responsibility for reimbursement to be on parties which have no contractual relationship with the victim, resulting in the need for strict governance over the process and the development of rules for evidence. Some of these difficulties could have been predicted (indeed, I pointed some out in my response to the consultation by the Payment Services Regulator[1]) while others appear to have become apparent only during the course the Steering Group's work.

I will discuss some ways in which these difficulties could be mitigated in my answers the consultation questions. In some cases, these mitigations are not how UK banks conventionally do business, and so the firms may prefer less transparency and less external scrutiny. However, it is important to note that these mitigations follow naturally from the application of the Steering Group's principles when taking into account the banking industry's preference for a Contingent Reimbursement Model.

Firms which do not wish such transparency measures should have the option to adopt a more conventional consumer protection approach by having the sender bank reimburse victims unless they can demonstrate that the victim was complicit in the fraud. Whether the sender bank then makes a claim against other parties regarding the handling of the stolen funds would then be a matter that could be resolved privately within the industry.

Similarly, if matters such as the apportionment of funds for reimbursement cannot be resolved by agreement within the industry then the fall-back position of the Steering Group should be for the sender bank to be liable. Taking this approach allows the sender bank to still obtain reimbursement for the funds should another

[1] https://www.benthamsgaze.org/wp-content/uploads/2018/06/pushpayment_murdoch.pdf

party be at fault. In contrast, a victim without access to legal and technical expertise is in a much weaker position to obtain funds which are due.

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

The code refers to "best practice" but too often this is a euphemism for current practice, and such standards serve to entrench poorly evidenced measures that are selected to minimize compliance costs and shift liability away from the industry. This is risk is exacerbated by the code proposing best practice standards developed by the industry itself.

Instead, as proposed by the Royal Society[2] "competent security and reliability must be based on a rigorous and evidence-based standard of engineering – one that is continually rising based on strong scientific evidence. 'Best practice' should not refer to average practice, nor to a check-box approach, but to an ambitious, state of the art standard for security and reliability, informed by research."

Standards which form part of measures that transfer risk from the industry to the customer, such as referred to in the code which is the subject of consultation, should be developed and assessed independently of the industry. Legislation such as surrounding Customer Due Diligence should be treated as a minimum level of care, not an acceptable level. As noted at the start of the consultation, if the industry does not wish this level of scrutiny, they should be able to adopt a more conventional consumer protection approach of reimbursing victims and then assigning costs within the industry.

These standards should also rapidly adapt to changing criminal behaviours, including by identifying characteristics of fraud. For example, a common approach today seems to be to breach a customer's online banking and change the name of the account to be "FROZEN" and thus persuade the customer than they indeed should move money out of their account. Criminals use similar techniques and infrastructure for multiple frauds. It would be reasonable to expect firms to identify such characteristics of impending fraud and take action to protect the customer.

The standards are also too narrow and focus just on warnings – generic warnings as part of GF(1), more specific warning as part of SF1(2), and warnings relating to confirmation of payee in SF1(3). It is well established that customers suffer from "warning fatigue"[3] and just adding more warnings will at best do no good and at

[2] Progress and research in cybersecurity Supporting a resilient and trustworthy system for the UK, Royal Society, July 2016. https://royalsociety.org/~/media/policy/projects/cybersecurity-research/cybersecurity-research-report.pdf

[3] Security Fatigue, Stanton et al. IT Professional 18(5), October 2018. https://www.computer.org/csdl/mags/it/2016/05/mit2016050026-abs.html

worst harm security. Firms should be required to show that customers know how to perform transactions securely, and that these measures don't require more time or mental effort than would be reasonable for someone carrying out normal daily activities.

This guidance should include information on alternative ways to make payments. As in-branch payments and cheques are at lower risk to push-payment frauds, these measures should not be discouraged by banks. Credit and debit cards have different liability for fraud. Trade-offs in terms of revocability, liability and checks performed should be provided to customers.

An assessment as to whether a customer can be reasonably expected to know how to perform actions securely should not only take into account actions by the firm, but also the actions of other firms and industry bodies which the firm could be reasonably expected to know of, following the same principle as the Consumer Rights Act. This is because an individual's behaviour will be guided by the combination of the advice they receive. If a customer could reasonably be confused by advice that is contradictory, excessive or which requires excessive effort then they should not be held liable for fraud.

For example, one of my banks informed me by letter that they would never contact me and ask me to transfer money. Another of my banks called me and asked me to transfer funds from my current account to a savings account which the staff member would open for me and gave the reason that a savings account was a safer place to keep money. I contacted the bank branch and confirmed that this was a genuine call from the bank, and they were trying to promote savings accounts to their customers. Such behaviour could easily lead a customer to become confused about what industry advice to follow.

Currently the scope of the code is restricted to domestic payments and only to the firm which sends and first receives the funds. This may be which the current banking system allows to be done but doesn't meet the objective creating incentives to improve the banking system to allow more to be done. All payments which a customer can reasonably be expected to perform should be covered, and potential liability for fraud should include all firms which process a payment until it leaves the banking system (such as by being withdrawn by cash).

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.

If the Firm has not met their level of care the customer should still be reimbursed because otherwise there not be the incentive required by OP1(1) for Firms to meet their standards. Firms have full visibility over the payment process so can with reasonable confidence evaluate whether a customer has or has not met the level of

care specified in R2(1) – for example through showing a warning or flagging a negative Confirmation of Payee result. In this case a Firm would be free to make a cost-based decision to not apply further fraud prevention mechanisms, such as manual review of the transaction or contacting the customer, which may incur expense or inconvenience to the Firm.

It could be claimed that the same argument applies to customers, but this is implausible. Even if a customer thinks they are likely to be reimbursed, the stress and inconvenience of disputing a transaction and being without funds for almost two months is a strong motivation for them to act with appropriate levels of care. Customers are also unlikely to know whether or not a bank is going to act with due care in carrying out a transaction. It's implausible to claim that a customer is going to act negligently on the off-chance that a bank might have failed to meet the requisite level of care.

For this reason, the requirement of R2(2) that Firms should "consider" whether they could have done more. This vague specification leaves Firms free to act in their own financial interest to deny refunds for frauds that a diligent firm would have prevented. Such a specification is likely to result in inconsistent outcomes, in contravention to CP(2), and offers insufficient to form a consideration for the Financial Ombudsman Service, in contravention to CP(8).

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

Customers are entitled to have a reasonable expectation that the payment system is safe. This expectation is reinforced through banks' marketing material. Due to cost-saving measures resulting in bank closures and the push for customers to use FPS, customers are increasingly being discouraged to use in-branch transactions and cheques – both less vulnerable to push payment scams than online-banking FPS transactions. The onus therefore should be on firms to take on the responsibility for making online banking safe.

For this reason, R2(1) should specify that in order to refuse a refund they must demonstrate that a customer acted with "gross negligence". This is the level of care specified in the Payment Services Directive and therefore facilitates the base of precedent resulting from court decisions and those of the Financial Ombudsman Service. This would also allow the code to take advantage of the result of UK Finance's efforts to define "gross negligence" with more clarity[4]. The current terms in R2(1) could then be indicated as considerations when assessing whether a customer

[4] UK Finance response to the APP scams steering group's draft voluntary code, 28 September 2018. https://www.ukfinance.org.uk/uk-finance-response-to-the-app-scams-steering-groups-draft-voluntary-code/

has acted with gross negligence, but ultimately this assessment must be made in the full context of the situation.

It is certainly inappropriate to elevate the importance of warnings and Confirmation of Payee as being sufficient in themselves as a reason to refuse to reimburse. Depending on the context of the situation, the fraud technique employed, and the way in which the warnings or confirmation of payee is shown, it is possible that a diligent customer could still be defrauded. In such circumstances the victim should be reimbursed.

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

Due to the large sums typical for push payment scams any delay in reimbursement is likely to cause substantial distress. An ambitious schedule for reimbursement is therefore justifiable, as would interim support to mitigate hardship. If a decision to reimburse has been made and communicated to the victim, this is should be the final decision and must not be subsequently revoked. In my experience of assisting victims of unauthorised transfers, a frequent scenario is the victim to initially be reimbursed but later the bank reverses the reimbursement and claims that the customer authorised the transaction. This puts victims at a disadvantage because this delay in the eventual denial of reimbursement means that the customer would not have the opportunity to make a request the retention of evidence such as CCTV which could support their case before it is deleted. If a decision is made to not reimburse a victim, the sending firm should automatically retain information relevant to the case which may be called for in resolving the dispute in the FOS or courts and instruct other participants in the payment to do the same.

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, customers should be reimbursed, regardless of the actions of the firms involved. If a fraud occurs in a payment system despite all parties acting properly then this shows that the payment system is flawed and should be improved. Not reimbursing the customer in such circumstances would violate OP1(1) by not incentivising the industry to reduce fraud in such circumstances.

Push payment fraud is only possible as a result of the irrevocable nature of such payments and is facilitated through the push towards online and mobile payments in preference to cheque or in-branch transactions. As a result of branch-closure programmes, some customers may not even have an effective option of in-branch

payments. Customers have little influence over such industry decisions, particularly due to the lack of competition in the UK banking industry.

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?

As noted in the beginning of my response, having the sending firm not be responsible for reimbursement is an unconventional approach to consumer protection and therefore introduces difficulties. One way that this exhibits itself is that by administrating the reimbursement the sender is responsible for making the case as to whether the receiving firm met its standards. Because it is proposed that the sending firm will not be liable for the reimbursement if it has met its own standard of care, the sending firm will not have an incentive to demonstrate that the receiving bank has failed to meet its standard of care. If it is easier to make a case that customer failed to meet the needed level of care, when compared to making the case that the receiving bank failed to meet its level of care, there is no incentive to protect the customer because both options are cost neutral from the perspective of the sending bank. For this reason, in cases where the customer is not reimbursed there should be some penalty for the sending bank, to provide incentive for it to either have prevented the fraud or make a case that the failure occurred elsewhere in the payment system.

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

Whether a customer complies with required standards should be assessed by criteria developed by an independent party and be specific to the banking platform(s) in question. Following the operating principle of transparency, this assessment report should be made available to customers and be sufficiently detailed for them to be able to appoint an expert to repeat the assessment. The assessment should be performed according to the best-practices for evaluating security techniques[5], to ensure that the results of experiments are a valid representation of customers actual behaviour and the actual experience the customer would have while performing a payment. The criteria for a sufficiently

[5] Towards robust experimental design for user studies in security and privacy, Krol et al. LASER 2016
https://www.usenix.org/system/files/conference/laser2016/laser2016-paper-krol.pdf

secure system should be that all customers, taking ordinary care and in a realistic context, should have a proper understanding of the consequences of their actions and be able to reliably detect and prevent frauds.

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

The high costs and "loser-pays" model of the UK court system creates a significant problem with access to justice in the UK. Push payment scams commonly exceed the limit for the small claims court and therefore a customer pursuing a case in the courts is at risks of being required to pay the legal costs of their bank, likely a five-figure sum that few could afford. For all but the richest customers, this situation effectively eliminates the option of escalation to the court system.

As found by the Civil Justice Council, the current situation particularly affects customers[6][1]:

"Existing procedure does not provide sufficient or effective access to justice for a wide range of citizens, particularly but not exclusively consumers, small businesses, employees wishing to bring collective or multi-party claims. … There is overwhelming evidence that meritorious claims, which could be brought are currently not being pursued." The Financial Services Bill 2009 incorporated provisions to allow collective proceedings regarding financial products, in order to spread the risk of legal costs over multiple members of a class. However, the Financial Services Act 2010, as passed, had this provision removed.

The Financial Ombudsman Service offers an alternative dispute resolution system but is still insufficient because few customers can afford the specialist legal and technical expertise needed to argue the complex points that would be raised when raising a dispute under this code. In particular, arguments about the effectiveness of fraud detection schemes cannot be made by examining only an individual case, but instead need a statistical argument based on data held by the firm.

For this reason, the dispute resolution scheme should allow collective actions as proposed by the Civil Justice Council. This would allow the costs of legal and technical expertise to be shared over multiple claimants which share some common characteristics or raise related matters over the interpretation of the code. The scheme should be designed to provide incentives for legal and technical experts to assist in such collective actions and oblige firms to disclose technical evidence to

[6] Civil Justice Council. Improving Access to Justice through Collective Actions. November 2008. https://www.judiciary.gov.uk/wp-content/uploads/JCO/Documents/CJC/Publications/CJC+papers/CJC+Improving+Access+to+Justice+through+Collective+Actions.pdf

allow the effectiveness of their detection and prevention measures to be assessed.

Q23 How should the effectiveness of the code be measured?

The Code permits the Firms significant discretion on whether to refund a fraud victim, resulting from the subjective criteria in R2 and possibility of ex-gratia payments (OP2). This discretion may inadvertently result in discrimination, as has been found in the case of reimbursement for other financial disputes[7]. Following Core Principle 2 (consistency of outcomes), and the Operating Principle of transparency, statistics should be collected and published on a per-Firm basis which show the fraud levels and reimbursement rates both overall for the Firm and split out by characteristics protected by Equality Act, as well as by indicators of wealth and profitability for the Firm.

These statistics would also facilitate the PSR's competition directive, allowing customers to select a payee bank which is more likely to protect their money and thus also facilitate the Core Principle 1 of the Steering group by creating an incentive for banks to reduce the level of push payment fraud. It is not sufficient for these statistics to be provided to the trade bodies and withheld from customers, as proposed in GF(2), because the code assigns cost of security failures to customers in some circumstances, and the choice of a sending bank is one which the customer must make.

[7] Banks biased against black fraud victims, The Times, 12 January 2017. https://www.thetimes.co.uk/article/banks-biased-against-black-fraud-victims-237z7rxvm

2. Member of the public

Dear Sir(s)/Madam,

Please find attached my response to the draft Voluntary Code on APP scams.

Yours sincerely

_____

CONSULTATION RESPONSE TO DRAFT VOLUNTARY CODE TO APP SCAMS

I just have read the draft Voluntary Code to APP scams and have to say that I am astonished to see that there is very no onus on the banks to perform their own **Level of Care** in the conduct of the management of customer accounts. It appears that banks have in place very poor levels of security where checks on those opening accounts with intent to using them to conduct APP scams are clearly and grossly inadequate. The Code will fail in its objectives to combat reduce APP Scam unless there is an explicit onus made on the banks to increase the level of security checks on the opening of accounts. Where banks have failed in this respect then they must face penalties for their lack of duty of care/ negligence. This should be a factor to be taken into account in determining whether or not a victim (be it firm or bank customer) of an APP should be entitled to reimbursement and even where these parties have not met the required level of care. I would ask the person overseeing this consultation to review the present parameters of the Voluntary Code. It must be expanded to take into account and include the need for new and strengthened responsibilities and duty of care from the banks. Without this the present Code will fail in its objectives.

Yours sincerely,

3. Member of the public

I am responding as an individual with an interest in retail FS regulation.

I endorse the SGs work and general approach.

My sole view relates to the question of reimbursement. The consultation paper does not consider the role of KYC in prevention of APP fraud, but that seems really central to the allocation of responsibility. A firm that allows an account to be set up in a way which does not allow the real principals to be traced should be wholly responsible for reimbursement of frauds run through it. To my mind - and this is admittedly a bit less clear - the same principle should also apply to firms which fail to recognise that an account which was operated legitimately was now being run by a mule. The patterns should be easy enough to spot.

It would be convenient if firms could suspend receivables into such accounts, though I'm not sure that's possible. Either way, firms which can't do customer diligence should pay, or buy insurance.

Regards

4. Member of the public

Sirs

I am responding with regard to the ability of the banks to reduce/prevent fraud rather than to the re imbursement code per se.

I am a recently retired accountant. At my last organisation we regularly received scam "CEO" – "please make an urgent payment to abc" type emails. On a few occasions I tried to phone the receiving bank to advise them that one of their customer accounts was being used fraudulently so that they could do whatever flag setting or monitoring was appropriate. I would have been happy to continue doing this were it not for the difficulty of actually getting hold of someone to speak to – as we were not the customers of the receiving bank. I also think all the cases I saw only involved the major UK clearing banks.

My understanding of these frauds is that money is moved almost immediately it has been received in the nominated account – and may travel through several different accounts before reaching its final destination – and in terms of mitigating/preventing these scams time is of the essence – ie action needs to be taken in minutes.

My request would be that the industry creates a central office for dealing with these scams with personnel from those banks which have a significant number of payment scams. The teams would have access to their own respective bank customer databases – so that where a scam was advised the relevant bank accounts could immediately have restrictions placed on them.(Smaller financial organisations would need to nominate contact points and would be included by phone). It should be possible to avoid any data protection issues as the activity is based around the avoidance or investigation of crime. The ability to have easy access to a number of bank systems would be to make it easier to follow any money which was being passed through several accounts.

Yours sincerely

5. Member of the public

My comment relates to Q5 "Do you agree with the suggested approach to customers vulnerable to APP scams?"

No. The approach is not proactive enough. Banks should be forced to offer customers automatic safeguards against APP fraud that can only be removed or diluted by the customer's own premeditated actions, so that vulnerable customers can be protected from making the kind of hasty transactions, under pressure from the fraudster, that usually characterise such frauds.

The mechanism I suggest is that every new account opened should start off with a default ceiling on push payments (BACS, CHAPS or debit card payments), together with a default built-in delay before the bank will execute such a transfer. An appropriate ceiling might be £100-£300 (although an argument could be made for £0) and a delay of two or three days. The customer would be allowed to modify these parameters, but only after giving appropriate notice to the bank in writing or by some other secure means. The bank would enforce an appropriate notice period before actually changing the account's parameters to enable higher-value transactions to take place. Other safeguards at this point could be considered as well, for example examining the customer's personal profile and assessing his or her vulnerability to fraud.

Many customers who only use on-line or phone payments to buy small items or pay household bills will never need to change the default parameters. Those who do wish to

change them would be warned by the bank that they are risking being defrauded. These warnings would become more strongly worded, with more careful checks required, where the customer asks to be allowed to make large transactions with short delays.

Banks would be able to introduce such simple technical changes without any difficulty at all. Those that did not do so would be made automatically liable to reimburse their customers for any APP fraud.

There are, of course, obvious ways in which the system may cause inconvenience to some customers. Better security always comes at a convenience cost. But, if sensible procedures are put in place by banks, customers who are sufficiently self-confident and competent will be able to get the flexibility they want, while vulnerable users will be at much less risk than they are now.

Name [✂]

Financial journalist

6. Member of the public

Dear Sir/Madam,

The voluntary code should be a step forward in ensuring consistency between banks and providing clear guidance on how both consumers and banks can reduce the risks of APP fraud.

However, the wording of the standard of care set out for consumers still allows for too much interpretation when what consumers need is clarity as to what their responsibilities are.

The governance of the scheme is a concern, for example, who will arbitrate if no agreement can be reached on whether the sending and receiving banks have met the standard of care?

Customers who need support to pursue a claim, complete paperwork etc, will likely turn to already stretched Citizens' Advice Bureaux and other advocacy services and might find it difficult to get the support they need within the allotted timeframe.

For customers who are vulnerable to this and other types of fraud because of their circumstances, there could well be unintended consequences because banks might be less willing to offer banking facilities to these customers.

It will be necessary to gather data from banks once the scheme is up and running to compare its efficacy across the sector.

Kind regards,

7. Member of the public

Firstly, thank you for your work on this matter.

I became the victim of an APP fraud in August this year losing £164,000 after making 10 transactions (from 4 accounts) of up to £20,000 per time from my [✂] bank Account in an attempt to avoid a fraud on my account after responding to a text from [✂] my official bank number. I did not receive one warning from [✂] my bank and the money was moved within

25 minutes. The fraudsters knew exactly how much was in my accounts to the penny so I can only conclude that there was help from within the bank. I am a professional and former Army Officer, this was a convincing scam. 3 months post the Police have yet to take any action.

[✂] my Bank have denied any responsibility and their HQ has declined to provide the bank account details on the receiving two banks under the excuse of data protection. In terms of context, I fell for the scam when exhausted in early pregnancy, this is the majority of my life savings including my house deposit. My husband and I do not own a home; I am truly devastated.

In terms of feedback on the consultation; I feel very strongly about 4 points:

1. This should be retrospective compensation pre Sep 2018. Fundamentally the responsibilities of the banks have not changed, irrespective of this code. Plus arguably those duped earlier were more vulnerable as there was less awareness. This is critical for victims like me.
2. Banks who allow criminals to fraudulently allow accounts to be opened should recompense but also they should have to answer to the victim / FCA– the police clearly do not have the resources to deal with this.
3. The banks should be made to provide the receiving bank victims – [✂] my bank is hiding behind data protection with me which is just insulting given that under money laundering regs they can release. It simply acts to delay investigation and adds to victim stress considerably.
4. The banks should be made to limit immediate transfer and should be forced to disclose what security mechanisms they have in place. I emptied 4 accounts including my ISAs without them realising……

Thank you once again for your work. It means a lot to me.

8. Member of the public

I only received a copy of your draft a matter of hours ago and my commitments tomorrow don't allow analysis, which it definitively deserves.
However, I would like to reiterate two points which I submitted when they occurred I.e. following my four hour "impersonation" scam in March and four months later, when I applied for another current account.

I appreciate the prime reason for the new code is reimbursement for fraud victims, but also ...."3.2. The code is designed to be adopted for the benefit of both firms and customers, with the **overall aim of reducing the occurrence of APP scams". Hence...**

The leader of the gang impersonating *Action Fraud* told me he didn't have to spend time on 2 of my 8 banks, [✂], because hackers couldn't touch them. This is obviously because a scammer couldn't receive an **OTP** on a landline phone, whilst using the phone for the scam.

Coming from an experienced scamming expert, shouldn't such a revelation be seriously considered in future banking standards?

Being a scam victim, I was appalled in July when [✂] one of my banks told me they could do nothing in branch with my ID, and I must "upload" it elsewhere, using their **Digidocs** system (so often used by the ever growing number of scammers). Abolishing such a technique, another example of labour saving, must surely reduce mule accounts, the main tool of trade of scammers.

I am pleased the code does not intend restricting goodwill payments and in time I will be reading about the plans to prevent becoming a second victim, but for now I have devoted my time to the two points above

9. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is Took s call.for my elderly neighbour from bt saying there was a problem with my broadband payments and the internet would go.off. she had no broadband so asked them to explain. Hung up straightaway

My bank responded by Rang bg who said they'd had a few reports about this scam. Have banned all known scam numbers from phone. Very helpful

My bank could have helped me by See above

Thank you for taking the time to read my response.

Kind regards,

10. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is Twice both to tune of £5000.00 All seemed legit requested documents etc invest money we pay 8% Jan 2018 then May 2018. Found out after second investment that first was a scam so looked into second and found to be a scam too!! I was sick but only reported 1st one as I felt so stupid

My bank responded by Tell me to report it. Took details and said we won't pay you back!!

My bank could have helped me by An e mail or text just pause that payment TIL I'd replied

Thank you for taking the time to read my response.

Kind regards,

11. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is being asked for help to return to the uk

My bank responded by sensibly warning me about scams and scammers

My bank could have helped me by not much else they could have done

Thank you for taking the time to read my response.

Kind regards,

12. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is A phone call from someone who spoke quickly saying that he was from BT regarding a problem with our broadband supplier. He asked lots of small questions, then to make a connection from my laptop. I realised that it was not right and excused myself.

My bank -I did not contact them.

My bank could have helped me by As I said they did not know.

Thank you for taking the time to read my response.

Kind regards,

13. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is A man 'phoned me, and said that he was a Law Enforcement Officer. He said I owed £2000 to a Company, but that he wasn't allowed to tell me the name of the Company. I am 80 years old, and it scared me. He said that if he was forced to call here the charge would go up to £2800. He gave me a Bank Account Number, and told me to do a Bank transfer to this account, but that I mustn't tell the Bank clerk what it was for, as I should really be paying V.A.T. on the transfer. I followed his instructions, and transferred the £2000. I told a friend about it, and she said that I had been scammed. I reported the matter to the fraud department of my bank, and to the police. A week later a man, saying that he was a bailiff, 'phoned me and said that he was coming to collect £1000 cash that I owed. I pretended that I agreed, but added that I have been advised to have my solicitor present to ensure that the transaction was above board. Needless to say, I heard nothing more from him.

My bank responded by I am happy to say that the bank refunded me the £2000.

My bank could have helped me by My bank [✂] couldn't have been more sympathetic, though they told me to be very careful about 'phone calls, where someone is asking for money.

Thank you for taking the time to read my response.

Kind regards,

14. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is It happened at least 18 months ago I had applied for a loan online and out of the blue a company I had not applied to contacted me offering the loan. They said that I needed to make a payment of £50 at the bank and to call them as soon as I made the transaction whilst still in the bank I did as they asked and whilst still in the bank I rang them and they wanted me then to take out an insurance and pay a further £99 for this insurance I said I could not afford to pay out this second sum and they said in that case we cannot transfer the loan. I asked for my £50 to be returned to my bank and they point blank refused as I was stood in the bank and it was every busy I was embarrassed and left the bank. My bank were never aware of it.

My bank responded by Rather stupidly I did not speak to the Bank about it because of my embarrassment as people had heard me raising my voice and I was on the verge of tears.

My bank could have helped me, I now know that my bank could have stopped the payment but by the time I had realised this it was too late. I did however make my own enquiries into the Company and found out that I was not the only person to have been scammed by them the address they were using was not theirs it was an office block with no company of their name having offices there. The matter had been sent to Action Fraud before I was scammed.

Thank you for taking the time to read my response.

Kind regards,

15. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is Utter shock and feeling sick and ill all at the same time and totally disbelief that I had been Scammed how on earth could I have been so stupid and mad at myself.Lesson learned.All this was gut churning.

My bank responded by Taking down all the details of what had happened making phone calls to get information on how best to help me and filling out forms to the relevant people to try to help me get my money back.

My bank could have helped me by They couldn’t have done anymore then what they did.They were fully supportive .

Thank you for taking the time to read my response.

Kind regards,

16. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is I was a treasurer of a community organisation and the email of a contractor working for us was hacked and I paid invoices of over £10,000 into a false bank account.

My bank responded by The bank attempted to recover the money but were unable to do so because it had been closed.

My bank could have helped me by If automatic checking of the names of the accounts matching had been introduced the transactions would not have gone through

Thank you for taking the time to read my response.

Kind regards,

17. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is telephone calls pertaining to be from hm customs and revenue..quite threatening , demanding response to avoid prosecution

My bank responded by didnt get that far, i didnt respond to the phone call message

My bank could have helped me by they were not involved as i didnt follow the demand..i would like others to be alerted to this sort of telephone message..

Thank you for taking the time to read my response.

Kind regards,

18. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is My card was cloned at [✂] cash point at Sheldon Birmingham , when I realised the money was gone from my account I spoke to that bank [✂]staff member who said I would get it back but it would take a while , they got footage of where it was taken from (great Barr) in Birmingham , of course the offender was wearing a hoodie and gloves so wasn't likely to be caught but they did pay me back my money , it took a month or so

My bank responded by Paid me back after tracking footage of my cloned card being used

My bank could have helped me by The problem is they don't really care if you have no money while they sort it out , it really does cause chaos

Thank you for taking the time to read my response.

Kind regards,

19. Member of the public

Hello,

I am emailing you to respond to the Draft Contingent Reimbursement Model Code consultation paper produced by the APP Scams Steering Group. I have included my personal experience of being scammed and how I think my bank responded.

My experience of being scammed is Travelling in Scotland during May 2014 my card details were copied at one hotel.
In Oct the bank contacted me, very proudly, to day that my card had been declined in Denmark.
I pointed out that I had been at an Age UK function and never been to Denmark, ever.
I had to supply details of where I had been and what I had spent.

The bank eventually agreed that it was not me and wasn't I glad that they had refunded my money and went after the teal thieves.

My bank responded by Sending me a patronising letter telling me to take better care of my details, bank statements and personal details.
Reiterating how good they were.

My bank could have helped me by Acknowledging that I told my branch when smd where I was travelling and how one department of this circus does NOT talk to any other.
Credit card, insurance, branch and any other function does not share details. Not even with a 'front' screen that is accessible to any other.

Thank you for taking the time to read my response.

Kind regards,