September 2018

APP Scams Steering Group

Draft Contingent Reimbursement Model Code

CONSULTATION PAPER

Non confidential responses

Part 3

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

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

UK FINANCE

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,

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.