September 2018

APP Scams Steering Group

Draft Contingent Reimbursement Model Code

CONSULTATION PAPER

Non confidential responses

Part 2

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

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

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

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

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

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

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

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

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

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

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

Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.
If the customer has been negligent, no refunds should be made. It will be hard to prove negligence during the payment flow, so PSPs will not be incentivised to weaken their warnings or controls based on any insight into the customers due diligence levels. The aim is to incentivise both PSPs and users to implement better controls before putting money in the hands of scammers.

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

Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?
The vulnerability criteria bears no relation to the information PSPs have access to. PSPs cannot assess customers health records, any information regarding balances held with other institutions, or personal information such as family situation. The criteria is only helpful for retroactively determining reimbursement eligibility by an independent body to judge a customers vulnerability. Any request for this kind of information after an APP scam by a PSP is invasive in the extreme. This may also mean that any claim to reimbursement on vulnerability grounds would need to be done retroactively (i.e. after the PSP has decided whether or not to reimburse as they cannot judge - unless in extreme circumstances - whether a customer is vulnerable).

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

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

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

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

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

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

Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?
Yes, but if the ASSG is looking to secure as many PSPS as possible to sign up to the code, they should acknowledge that many of the potential funding sources identified in no blame scenarios, the PSP will be paying to reimburse victims. It is not possible for smaller PSPs or challenger banks to absorb this cost, when there is no fault.

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

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

Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?
Yes but there needs to be a prompt time frame to decide blame apportionment and timely refunding for the sending PSPs if they are not to blame.

Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?
Please see our response to Q8.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Creu Cymru oed gyfeillgar
Creating an age friendly Wales

15 November 2018

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

Dear Sir,

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

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

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

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

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

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

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

FRSB FundRaising Standards Board

Creu Cymru oed gyfeillgar
Creating an age friendly Wales

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

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

We welcome the recognition in the consultation that

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

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

Yours sincerely

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

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

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

Consultation

APP Scams Steering Group: Draft Contingent Reimbursement Model Code

November 2018 Ref:

Policy@ageuk.org.uk

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

About Age UK

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

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

About this consultation

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

Key points

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

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

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

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

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

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

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

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

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

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

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

Age UK Response

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

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

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

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

Sending Firm – specific comments

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

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

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

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

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

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

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

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

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

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

SF1(2) Prevention

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

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

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

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

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

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

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

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

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

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

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

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

Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims.
Whilst we understand the desire for a provision along these lines in order to assist in apportioning responsibility between Firms we are concerned that there may be some unintended consequences from the current position and wording of the provision.

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

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

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

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

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

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

Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care?
We are confused by this question as the provisions seem to operate by assuming that the Sending Firm has met its level of care. If it has not, then on our reading of the Code R2(1)(a) and (b) would not be relevant.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Additional Questions
Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?
The impacts of fraud can be shattering. Some older people lose their life savings, which they worked decades for and which were meant to provide for their retirement. Even relatively small losses can be devastating to the victim. In our polling, around 1 in 8 of those who lost money (13%) lost more than £1,000, while a quarter (23%) lost less than £100. In the case of older people in vulnerable circumstances, the impacts can go beyond money, affecting their physical and mental health too. This can even mean that someone who was living at home independently is no longer able to. On top of the personal harm caused, this increases demand on under-pressure public services like the NHS and social care. People defrauded in their own homes are 2.5 times more likely either to die or go into residential care within a year.[2] Any progress the Code makes towards reducing the incidence and impact of APP fraud is therefore extremely welcome.

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

Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?
We expect that Firms will also benefit from a reduced incidence of fraud. If the Code is introduced and implemented well then we would expect to see a significant increase in trust in Firms, particularly those that fully embrace it and provide notably improved protection for their customers. We expect that Firms may also benefit from development of the Effective Warning system to improve communications with their Customers in other areas.

Q23 How should the effectiveness of the code be measured?

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

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

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

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

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

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

15 November 2018

1. Introduction

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

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

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

2. Background data on Northern Ireland

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

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

---

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

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

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

[4] The Consumer Council – Vulnerable Consumers 2017

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

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

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

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

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

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

3. Main body of response to questions

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

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

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

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

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

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

Q3: We welcome views on how these provisions (R2 (1) (a) and (b)) might apply in a scenario where none of the parties have met their levels of care &
Q4: Do you agree with the steps customers should take to protect themselves?

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

---

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

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

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

4. Other issues

4.1 Cross Border payments

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

4.2 Small to Medium sized Enterprises (SMEs)

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

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

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

5. Conclusion

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

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

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

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

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

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

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

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

Yours sincerely

[✂]

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

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

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

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

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

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

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

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

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

13 November 2018

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

Dear Sir / Madam

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

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

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

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

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

Yours faithfully,

Financial Services Consumer Panel

ANSWERS TO CONSULTATION QUESTIONS

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

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

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

For 'sending' firms:

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

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

For 'receiving' firms:

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

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

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

We find it difficult to envisage circumstances where this might apply.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Transpact – Response to APP scams Steering Group consultation

Dear Authorised Push Payment Scams (APP) Steering Group,

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Best Regards,

Transpact.com

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

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

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

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

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

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

Yes. We have no recommendations for other issues.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

No comment.

Additional Questions

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

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

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

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

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

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

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

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

Q23 How should the effectiveness of the Code be measured?

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

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

15 November 2018

Contingent Reimbursement Model Consultation Response

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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