Consultation

APP Scams Steering Group: Draft Contingent Reimbursement Model Code

November 2018 Ref:

Policy@ageuk.org.uk

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

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

About Age UK

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

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

About this consultation

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

Key points

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

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

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

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

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

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

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

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

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

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

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

Age UK Response

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

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

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

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

Sending Firm – specific comments

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

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

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

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

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

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

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

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

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

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

SF1(2) Prevention

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Q23 How should the effectiveness of the code be measured?

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

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

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

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

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