Consultation Response

Ref 0218

Submission to the Payment Systems Regulator consultation on authorised push payment scams

January 2018

All rights reserved. Third parties may only reproduce this paper or parts of it for academic, educational or research purposes or where the prior consent of Age UK has been obtained for influencing or developing policy and practice.

Phil Mawhinney
phil.mawhinney@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 this consultation

In November 2017, the Payment Systems Regulator (PSR), the economic regulator for the payment systems industry, published a consultation paper on authorised push payment scams – where people are tricked into sending money to a fraudster.[1] This sets out the PSR's ongoing programme of work to mitigate the impact of such scams, including consultation on a proposed 'contingent reimbursement model'.

Age UK is the country's largest charity dedicated to helping everyone make the most of later life. We help more than 5 million people every year, providing support, advice and companionship for older people who need it most.

We welcome the opportunity to respond to this consultation. We respond only to the relevant questions, use the terms 'scams' and 'fraud' interchangeably for authorised push payment scams, and generally refer to banks rather than 'PSPs'.

Key points and recommendations

1. We welcome the best practice standards for how banks should respond to a reported scam. Banks must keep customers well informed about progress. However, we are unclear how customers will know if banks have followed the standards.
2. We welcome the proposed contingent reimbursement model. The impact of scams can be devastating for older people, and consumers need better protection.
3. We broadly support the principles outlined but cannot fully support the model until we see further detail on the requisite standards of care for banks and customers.
4. The customer requisite level of care should only be breached by a high threshold of gross negligence. It should reflect consumers' 'real world behaviour' rather than theoretical, unrealistic expectations.
5. Banks are in a better position than consumers to spot and design out fraud, so should bear the balance of liability for reimbursement, and be incentivised to improve security.
6. The 'no blame' scenario is challenging but we support victim reimbursement. This will protect consumers and incentivise banks to prevent scams and repatriate lost money.
7. In a 'shared blame' scenario, banks should be liable, as their duty to protect their customers outweighs an individual customer's duty (and ability) to protect themselves.
8. Customer vulnerability – such as dementia and bereavement – should shift the liability balance away from the customer, regardless of whether the bank identifies the vulnerability or not.
9. The scam report response standards should be part of the bank standards. Transaction data analytics and confirmation of payee should be introduced as soon as possible.
10. UK Finance may be in a good position to implement but should not design the model. The PSR should design it, with input from consumer bodies.
11. All banks should adopt the reimbursement model for it to be effective.
12. We broadly agree with the model's scope but are concerned that excluding overseas accounts could severely limit its impact.
13. Banks should have clear audit trails to help solve disputes. Bank communications to victims should explain how they can access dispute resolution and of their recourse to the Financial Ombudsman Service.
14. We support the introduction of the model by September 2018. A phased approach would allow development of the model and additions to the standards.
15. The PSR should carry out further analysis of the risks associated with Open Banking.

Q1: In your view, will the best practice standards developed by UK Finance be effective in improving the way PSPs respond to reported APP scams? Please provide reasons.

We welcome the proposed best practice reporting standards, although we have not seen them in detail.

In particular, we welcome the proposal for customers to have a single point of contact through their bank. This is consistent with other areas of consumer law (e.g. retailer liability for defective products) and recognises the unfairness and inefficiency that would arise if consumers had to complain directly to the faulty part of the supply chain. However, even with this single point of contact, customers may be stressed, confused and unsure whether they have in fact been scammed, so it is vital they can easily and quickly find the contact details for contacting their bank 24-7. We welcome the proposal for specialist bank staff to be dedicated to dealing with fraud, and suggest their training includes how to deal sensitively and effectively with customers who may be vulnerable. Ideally, the customer would speak to the same staff member as much as possible.

This is important because some customers have poor interactions with bank staff when worried about a scam. One older woman told us how she suspected she had received a scam call from someone impersonating her bank, but when she called her bank to discuss it she felt the call handler did not take her concerns seriously:

> *So, I rang [my bank] last week and… and they said 'Well, I don't know anything about the phone call but we wouldn't ask for your bank details if we had rang you', but they were flippant, they were flippant about 'Well, it might have been a scam', they weren't that interested... No, they weren't bothered.*[2]

We also welcome the intention for banks to keep the customer informed about their response to the reported scam. Banks should anticipate and design out 'fraud recovery fraud' risks, where fraudsters impersonate the bank to the customer during this phase.

Many scam victims do not report the incident, because they are embarrassed, don't know who to report to, or don't think anything can be done.[3] For the standards to have impact, banks should encourage their customers to report a suspected scam to them. They should encourage customers not to feel embarrassed, by showing that scams are a common occurrence.

Our biggest concern is that it is unclear if or how a customer will know whether their bank has met the standards, following them reporting a scam. Similarly, it is unclear if or how banks will demonstrate compliance with the standards. We ask for clarity on these points.

It is in banks' best interests that the standards work and are seen to work by consumers, given the high levels of mistrust of banks – for example, recent YouGov polling found that 'just 36% of British consumers trust banks to work in their customers' best interests, while more than half (55%) don't.'[4]

We welcome the proposal for the PSR to monitor progress of the package of initiatives through 6-monthly reporting, and the option for regulatory action if progress is slow. We ask the PSR to make public as much reporting information as possible, including on which

banks have and have not adopted the standards. We would like to see the PSR liaising regularly with consumer groups on a 6-monthly basis to discuss progress.

Q2: Should a contingent reimbursement model be introduced? Please provide reasons.
Yes. We welcome the proposed model and pay tribute to Which? for drawing attention to this issue through its 2016 super-complaint.[5]

As we have outlined elsewhere,[6] the financial and health impacts of being scammed can be devastating for older people. Some have suffered serious losses from their life savings, including tens or even hundreds of thousands of pounds. Relatively small losses can still have serious impacts. Older victims' health deteriorates more quickly, and being a victim of a scam increases the chance of going into residential care.[7]

It is not reasonable in every case to expect a customer to spot a scam and shoulder the liability if they don't; many scams are highly sophisticated, perpetrated by criminal gangs. Banks have a unique position and key role to play in preventing scams, such as through spotting suspicious account activity, warning a customer mid-payment in an accurate and effective way, being aware of a customer's vulnerabilities, preventing scammers from opening accounts and identifying mule accounts.

For example, in a case where a customer phoned her bank, concerned she might be a victim of a phone scam, the Financial Ombudsman Service found the bank had missed opportunities to prevent the scam. The bank had inaccurately described the customer's concerns to its internal fraud team, gave inadequate warnings and false assurances that a scam was not occurring, and did not sound sympathetic to the worried customer.[8]

So, given the impact on victims, the sophistication of some scams, and the fact that banks are in a position to prevent scams but do not always do so, we support the introduction of a contingent reimbursement model.

Q3: Do you agree with our high-level principles for a contingent reimbursement model? Please provide reasons.
We are broadly supportive of the model as outlined. We support the principle that banks should be incentivised to prevent scams, and that victims should be compensated where their bank has not met agreed standards.

However, we cannot fully support the model until more detail is given on 1) the agreed standards for banks, and 2) the requisite level of customer care. If the bank standards are set too low – where many banks already meet them through their current practices – we think this will provide insufficient protection for customers.

On the requisite level of customer care, we look forward to seeing more detail on the proposed level of care. Analysis of real examples of common scams and the customer pathways we might expect to see in response, may help to develop expectations of care that are fair and practical. In the meantime, we make the following points.

Firstly, where a bank warns a customer mid-payment about the risk of being scammed, through an online message or verbal warning, this should not automatically discharge the bank's liability. Generic and/or frequently shown warnings may not register with the customer, for example because it becomes normalised ('part of the wallpaper') or is insufficiently specific, targeted or timely. Scammers often account for bank warnings, building them into their story and instructing the victim on how to respond.

Secondly, in some cases the vulnerability experienced by a customer at the time of being scammed may impair their ability to take reasonable care to protect themselves and therefore reduce their liability. We expand this argument in Q9.

Thirdly, a valid example of customer negligence might be if the customer ignores a mismatch from a confirmation of payee query. However, this requires the bank to provide this service in the first place, and in a way that a wide range of consumers – including those in vulnerable circumstances – can easily understand and act upon. Lack of accessible provision of this tool should represent negligence on the part of the bank, assuming the tool would have highlighted a risk for that particular scam type.

Lastly, given the importance and sensitivity of this issue, the PSR should develop the bank and customer care standards in an open and transparent way, consulting a wide range of stakeholders.

Q4: In your view, what are the relative advantages and disadvantages of each alternative outcome for a 'no blame' situation (the victim is reimbursed by PSPs, or the victim bears the loss)? Please provide reasons.

The 'no blame' situation is a challenge. Our final view will depend on the detail of the PSP standards. We would not support standards that provide inadequate protection for customers. On the basis of the detail available, we do not support option 2 ('focus on incentives'), under which consumers who have not acted in a negligent way and who may be the victims of a sophisticated scam could still lose potentially life-saving amounts.

Going further, and again depending on the final detail, we think in the 'no blame' situation the victim should be reimbursed. This would provide strong incentives for banks to repatriate lost money to the victim, and to prevent money being sent as part of a scam in the first place, for example by clamping down on criminal use of bank accounts. Where this reimbursement liability falls on the bank and funds are not repatriated, these costs will effectively be shared among all customers, who benefit from a form of risk pooling. Given the catastrophic nature of the impact of many scams compared to the additional cost per customer, this could represent a fair balance of risks and costs.

Another major issue to be clarified is where liability lies in a 'shared blame' scenario, where both the bank and customer fail to act according to agreed standards. Banks have a fundamental duty to protect their customers' money, especially large amounts accrued over decades that older people especially cannot replace (i.e. people's life savings). Therefore, the balance should be towards reimbursing the customer where the bank has failed to meet the agreed standards, irrespective of the customer's actions. On this basis, our initial view is to support reimbursement for victims in a shared blame scenario. This chimes with the principle underlying the PSR's view stated –

Regardless of whether the victim has taken the requisite level of care, in any scenario where a PSP has not met their required standards, it might be appropriate that the model includes some form of fine or penalty on the PSP to ensure it is appropriately incentivised. The funds could potentially be put into a central fund for reimbursing victims such as in the 'no blame' scenario. (para 6.12)

As suggested in this quote, reimbursement in the 'shared blame' and 'no blame' scenarios could potentially be from a central fund, built up either from penalties or indeed an industry levy, or other source.

Further, we are not convinced reimbursing victims in this scenario, when they have not met the standards of care, would necessarily result in many consumers becoming more negligent. While it makes sense in theory that knowing they will be reimbursed regardless of their behaviour means consumers will act with less care, in real life we think 1) not everyone will be aware of where liability lies, and 2) the prospect of going through a stressful and uncertain process to reclaim life-changing amounts of money is such that consumer will continue to take as much care as possible.

We appreciate these are difficult judgements and that we need a model that maintains long-term incentives for banks to prevent scams, while ensuring they do not withdraw their services from customers. The PSR should consider whether a central pot from which reimbursement is made, and the possibility of partial reimbursement, can help balance incentives in particularly challenging cases.

Table 1. Liability in different scenarios

		CUSTOMER	
		Did meet standards ✓	**Did not meet standards x**
BANK	**Did meet standards ✓**	**No blame** • We support **reimbursement**. • This would incentivise banks to meaningfully improve security. • Risk would be pooled among all customers.	**Bank meets standards** **Customer negligent** • Customer is liable – **no reimbursement**, unless the funds can be recovered through repatriation. • But vital that the requisite level of customer care is set at a fair and realistic level.
	Did not meet standards x	**Bank negligent** **Customer not negligent** • Bank is liable – **reimbursement**.	**Shared blame** • We support **reimbursement**. • Bank did not reach the standards; customer behaviour is irrelevant.

Q5: Do you agree that the measures being developed by industry (specifically UK Finance and the Forum) should be included as the required standards of the contingent reimbursement model that PSPs should meet? Please explain your reasons.

Yes. The APP claim reporting standards have a key role and should be included in the in the PSP standards. This should mean more reimbursement occurs through better repatriation of a customer's money. Even where a customer has failed to take the requisite level of care, this should be irrelevant if the bank has failed to meet these reporting standards, and has not done all it can to rescue the customer's money.

In terms of the process, banks should automatically reimburse victims as soon as possible after the scam has been discovered (unless it is clear the customer has been grossly negligent), rather than waiting to see if, for example, the funds can be recovered. This would give banks a meaningful incentive to recover the funds. We think it would also be simpler than keeping customers in limbo and requiring regular updates.

As noted above (Q3), confirmation of payee has the potential to prevent certain scams. Failure by a bank to offer it to all customers, through a range of channels (not just online) and accessible to people in vulnerable circumstances, could constitute failure to meet acceptable PSP standards.

The transaction data analytics measure is key, as it can help banks spot, disrupt and prevent scam payments. For banks to avoid liability, banks should be required to implement an effective transaction data analytics solution.

Finally, we agree with the PSR that the standards should include measures leading to 'better identifying mule accounts used by scammers' (6.8).

We appreciate that these (and other) measures may need time to be developed and tested before being included as required standards in the model. They should be added to the standards as soon as possible at various points after the Sept 2018 starting date.

Q6: If a contingent reimbursement model is introduced, which organisation should design and implement it? Please provide reasons.

UK Finance may be able to implement the model, but should not design it. It is not appropriate for an industry representative body to design expectations of consumer behaviour. The PSR could design the model, with meaningful representation from consumer bodies. It is in a better position to make balanced judgements to protect consumers.

We are anxious that the organisation implementing the model should be seen to be independent in checking whether bank and customer standards of care have been met. This organisation should publish regular reports, including on the number of scams in each of the four categories listed in table 1 (i.e. customer/bank negligence, shared/no blame).

Q9: Are there any factors that should be considered when defining the requisite level of care victims should meet?

When defining the level of care victims should meet, it is important to look at consumers' 'real world' behaviour. This will help avoid making unrealistic assumptions about what is reasonable and fair to expect customers to do to protect themselves. This is in line with the FCA's aim to 'regulate for the real world and wherever possible our approach will be based on what we know about how consumers really behave'.[9]

As discussed above, we do not think if a bank warns a customer mid-payment about the risk of being scammed, through an online message or verbal warning, this should automatically discharge the bank's liability. Generic or frequently shown warnings may not register with the customer, for example because it becomes normalised ('part of the wallpaper') or is insufficiently specific, targeted or timely.

In the Financial Ombudsman Service (FOS) case study discussed above (Q2), the telephone scam victim's bank argued it had displayed scam warnings when the customer logged in to online banking. However, FOS found in favour of the customer, noting that the bank did not correctly register the customer's concerns or offer accurate advice. This exemplifies how it is easy for a bank to attempt to discharge its responsibilities by giving a generic warning but without effectively engaging with a customer's concerns, picking up on the signs of specific scams, and offering timely and accurate advice and protection.[10]

Similarly, banks making available 'scam checker'-type tools is welcome but should not constitute a discharging of liability. Such tools may not be accessible, useable or effective for customers, including people in vulnerable circumstances (discussed below) or those who don't use the internet. Such real-life barriers mean non-use of such tools should not be considered gross negligence. Ultimately, the onus should remain on the bank, which is better-placed than the customer to spot and stop fraud.

Further, through social engineering, scammers often account for bank warnings, building them into their story and instructing the victim on how to respond. This means that in the 'real world', customers may be convinced that by ignoring a bank's warning they are in fact taking the requisite level of care.

We do agree that 'vulnerability may play a role in defining the requisite level of care from consumers, and so the level could vary' (6.38). We see a number of key vulnerabilities in the scam cases brought to our information and advice service –

- Dementia or other cognitive impairment – see case study 1 in Table 2.
- Loneliness and/or social isolation – see case study 2.
- Recent bereavement – see case study 3.

Other research and practice echoes these as being key vulnerability risk factors.[11]

Table 2. Customer vulnerability examples[i]

Case study 1: Dementia A caller told Age UK about their father, who is around 80. He has dementia, which is worsening. He recently signed up for a 'protective asset trust' from a cold caller, paying around £1,000. The caller says their father is vulnerable and has been pressurised by cold callers.
Case study 2: Loneliness and isolation A caller told Age UK about their mother, who lives in France and has dementia. She was scammed through an online dating agency and has lost more than £10k. They have tried to address this but the mother denies there is a problem. They want her to return to the UK but she doesn't want to, despite being very isolated.
Case study 3: Bereavement A caller told Age UK their mother had fallen victim to a scam. She is over 90 years old and recently bereaved. She has convinced herself that she is in line to win a large amount of money. The mother won't listen when they try to explain that it's a scam. She is fiercely independent.

We welcome the recent progress made in understanding and identifying consumer vulnerability, including the FCA occasional paper on the subject.[12] Banks are in a good position to be aware of vulnerabilities their customers are facing. We note that the recent BSI code of practice on protecting customers from financial harm includes a section outlining how banks should understand and spot customer vulnerability. It states –

> *Frontline staff should be trained to look out for potential indicators of customers being in vulnerable circumstances… which can make them more susceptible to fraud or financial abuse, and more likely to suffer financial harm as a result.*[13]

While we welcome this approach to spotting vulnerabilities that can put people at extra risk, not all such vulnerabilities are easily identifiable. Customer vulnerability should nevertheless shift the liability balance away from the customer, regardless of whether the bank identifies it or not.

Further, many scam victims are made vulnerable in the moment of being defrauded, through the deliberate use by fraudsters of pressure, panic, grooming and other psychological tactics. That is why the requisite level of customer care for *all* customers should only be breached by a high level of gross negligence.

Where a bank is aware that a customer has previously been a victim of a (attempted) scam, it should act on this information and take extra precautions. This should shift the liability towards the bank if a further scam incident occurs.

[i] Cases taken from Age UK's information and advice helpline. Some details changed to preserve anonymity.

Some customers may want to tell their bank they feel especially vulnerable to scams, and ask it to note this and take extra precautions. We are aware of at least one bank already accepting a short document to that effect from customers. We also note that the BSI code of practice includes a requirement for banks to 'have a process in place to ensure that frontline staff respond consistently and appropriately to customers that wish to make a self-declaration of vulnerability'.[14] Where a customer has made such a declaration, we would expect the balance of liability to shift towards the bank.

While not a vulnerability as such, many older people do not use the internet – 6 in 10 (59%) people aged 75+ are not online.[15] They have less ready access to online information that may help them verify a payee, such as a doorstep trader or financial firm, e.g. the FCA Financial Services Register. This could be a consideration in any judgement about whether or not a customer has met the requisite level of care.

Q10: Do you think it is necessary for a significant majority of, if not all, PSPs that provide push payment services to consumers to adopt the contingent reimbursement model for it to be effective? If yes, please explain if you think the model would need to be mandatory for PSPs.
Yes, we think it is necessary that all banks providing push payment services to consumers adopt the model for it to be effective. Given the scale of scams and the harm they cause, it should be a basic duty and expectation on banks to do all they can to prevent scams and reimburse customers where they have not done so. We agree with the PSR that fraudsters may target banks that do not adopt the model, seeing them as a weakness in the system. It would also distort competition to have some PSPs outside the model, and potentially lead to a 'race to the bottom'.

Q11: What are your views on the scope we have outlined for the model? Please describe any other factors you think we should consider.
We agree with the scope as outlined, with one exception. While we appreciate that including payments to or from overseas accounts would add complexity, we are concerned that excluding such payments could severely limit its impact. It would also incentivise fraudsters to move offshore, if they are not already operating from overseas.

We are not in a position to know what proportion of scams involve overseas payments, and ask the PSR to investigate this question. If the proportion is high, we would have major concerns about proceeding with the model without including overseas payments. This could potentially be tackled through a phased approach (see Q14).

Q12: In your view, how should the dispute resolution mechanism work and which organisation should oversee this? Please provide reasons.
The organisation overseeing the dispute resolution mechanism should share with the PSR and consumer bodies regular reports to review outcomes and make improvements.

Banks systems should allow clear audit trails to help solve disputes. During dispute resolution, customers should be able to see the steps their bank took to protect them.

The mechanism should be accessible to all customers and well publicised. Bank correspondence with scam victims should explain how to access dispute resolution mechanisms, and remind them of their recourse to the Financial Ombudsman Service.

Q13: Do you agree with our view that a contingent reimbursement model, if introduced, should be in place by the end of September 2018? Please explain.
Yes, we agree. We want the model to be in place quickly, to prevent life-changing losses and harm for older people. However, we understand the need to take time to design and implement the model in a way that will effective in the long term so suggest a process of regular reviews or staged implementation, as set out in Q14.

Q14: Should a phased or transition approach be used to implement a contingent reimbursement model? Please explain.
A phased approach could allow the model to be set up quickly, followed by subsequent phases during which more challenging issues could be resolved. This could include introducing wider industry measures, such as confirmation of payee and transaction data analytics, and including payments to or from overseas accounts.

Additional comments
We note the lack of reference in the consultation document to Open Banking. We are concerned about the risk of impersonation by fraudsters, which too often accompanies new regulatory change (as happened, for example, with pension scams following the 2015 pension freedoms). The PSR should carry out further analysis of the associated risks, including whether new payment initiation providers may be included in the reimbursement model, and whether legislation is needed to forestall any problems

[1] https://www.psr.org.uk/sites/default/files/media/PDF/PSR-APP-Scams-report-consultation_1.pdf
[2] Participant of Age UK workshop, 2016
[3] https://www.citizensadvice.org.uk/Global/CitizensAdvice/Consumer%20publications/Scams%20report%20-%20final.pdf
[4] https://yougov.co.uk/news/2017/05/19/most-brits-trust-banks-dont-think-they-work-custom/
[5] https://www.which.co.uk/policy/consumers/347/consumer-safeguards-in-the-market-for-push-payments-which-super-complaint
[6] https://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true
[7] According to the National Trading Standards Scams Team, people defrauded in their own homes are 2.5 times more likely to either die or go into residential care within a year.
See also Age UK's report Only the Tip of the Iceberg, https://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true
[8] http://www.financial-ombudsman.org.uk/publications/ombudsman-news/135/135-case-studies-about-scams.html
[9] https://www.fca.org.uk/publication/corporate/our-future-approach-consumers.pdf
[10] Case 135/3 http://www.financial-ombudsman.org.uk/publications/ombudsman-news/135/135-case-studies-about-scams.html
[11] According to the National Trading Standards Scams Team, people defrauded in their own homes are 2.5 times more likely to either die or go into residential care within a year.
See also Age UK's report Only the Tip of the Iceberg, https://www.ageuk.org.uk/documents/en-gb/for-professionals/consumer-issues/age%20uk%20only%20the%20tip%20of%20the%20iceberg%20april%202015.pdf?dtrk=true and
ACTSO (2014) *Summary of Doorstep Crime Report to National Tasking Group, May 2014*. Ruth Andrews.
[12] https://www.fca.org.uk/publications/occasional-papers/occasional-paper-no-8-consumer-vulnerability
[13] PAS 17271:2017, Protecting customers from financial harm as a result of fraud or financial abuse – Code of practice, section 7.1.2.1
[14] Ibid., section 7.1.3.3
[15] *Internet Users in the UK 2017*, ONS