

Consultation Response

Authorised Push Payment (APP) Scams – Call for Views

Payment Systems Regulator (PSR)

April 2021

Contact: joel.lewis@ageuk.org.uk

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.

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

Authorised Push Payment (APP) fraud, when criminals trick people into transferring money to them by posing as a legitimate payee or constructing fraudulent reasons for a payment, are a significant and growing problem. The scammers are clever, organised criminals and people have lost life-changing sums of money. In the first half of 2020, losses due to APP scams totalled £208 million (although this is likely to be an underestimate, due to under reporting of APP scams).

The Payment Systems Regulator's (PSR) aim is to significantly reduce APP scam losses incurred by payment system users, through improved prevention and reimbursement. The consultation asks respondents for their views on three measures the regulator believes could help to reduce APP scam losses.

Key points and recommendations

- Age UK supports decisive action taken by the regulator to address the persistent harm posed by APP fraud.
- The implementation of the Contingent Reimbursement model (CRM) Code in 2019 represented a significant leap forward in protecting consumers against APP scams, however, far too many victims are not receiving a consistent standard of care.
- A lack of transparency around Payment System Providers' (PSPs) decision-making process has led to serious inconsistencies in the number and level of APP fraud reimbursements to victims.
- In the current absence of a statutory duty to protect consumers, the PSR must now take decisive action - by extending the obligation of reimbursement to all PSPs - to prevent further harm.

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.

Introduction

We welcome the opportunity to respond to the consultation on improving redress for victims of APP fraud. Given the persistent and increasing threat of fraud, and APP scams in particular, it is right that the PSR, is proposing these measures to protect consumers against the significant impacts that these crimes have on thousands of victims every year.

The implementation of CRM Code in 2019 represented a significant leap forward for consumer protection against scams. Signatories of the Code recognised that in nearly all cases, consumers, micro-enterprises, and charities, should not be held responsible for an incidence of APP fraud against them. The Code established a presumption that any financial losses sustained as part of an APP fraud would be reimbursed in full.

Whilst important progress and improving rates of reimbursement have been made since the CRM Code's introduction, it is clear that far too many people are bearing the responsibility for being the victim of a crime. The non-mandatory adoption of the Code means that some victims are denied

protections simply on the basis of who they bank with. A lack transparency around its application, has meant that consumer outcomes are far from consistent – whether it be across the sector, and potentially even across individual Payment System Providers (PSPs). In the current absence of a statutory duty to protect consumers, the PSR must now take appropriate action, by extending the obligation of reimbursement to all PSPs through the inclusion of a reimbursement requirement in payment system rules.

Question 1: Do you have any comments on the data presented above? Do you have any supplementary information on customer outcomes under the CRM Code?

The CRM Code's introduction was a great leap forward in creating a framework to assess and refund victims of APP fraud. The Code represents a significant improvement on what existed before. However, this must be regarded as the starting point, not the end, of a journey to improve outcomes for victims of APP fraud. The proposals outlined by the PSR are another stop on this road to ensuring that victims of fraud receive an adequate and consistent level of protection and that all consumers can have a greater degree of confidence when making payments.

The increases in reimbursement rates since its implementation show that signatory firms may be starting to standardise decision-making and improve understanding about how it can be used to protect consumers. However, it is clear from the data provided that action to prevent these scams and support victims needs to move stronger and faster. The ongoing, persistent, and increasing threat of APP fraud to consumers, means mandatory protection is needed to improve the number and level of reimbursements. This should be on the same basis as for unauthorised fraud, with victims reimbursed except for cases of gross negligence or first party fraud. We support the PSR's view that a lack of a standardised definition around what constitutes 'gross negligence' is leading to inconsistent decision-making and therefore ultimately leading to serious harm for consumers who are not reimbursed.

In light of the impact of the pandemic on changing consumer behaviour and accelerating previous trends for more of us to shop, bank and manage our money online, consumers need to have the confidence and reassurance that they are being protected. This can be particularly true for those in vulnerable circumstances due to their isolation, mental capacity, or digital skills. All consumers can be one decision and one life event away from becoming vulnerable themselves. It is crucial that the regulator takes action to prevent further resulting harm to health, wellbeing, confidence, and relationships, from incidences of APP fraud.

Question 2: Do you have any comments on the appropriate balance of liability for APP scams costs between individuals and PSPs?

Age UK strongly supports the principle that PSPs and the wider banking, technology, and telecoms systems, are often far better equipped to better protect against scams than individual consumers. PSPs are able to employ analytics and machine learning to identify and act on suspicious transaction history and account management. Despite the ability of firms to detect and prevent fraud, consumers are still shouldering the responsibility for losses. The PSR estimates that approximately half of all victims of APP fraud are not being refunded. The Code was designed and implemented to shift liability from individual consumers and onto the payments system as a whole. It is unacceptable that customers who have met the appropriate level of care should not expect to be reimbursed.

Age UK works alongside many other organisations across the third sector, law enforcement, banking, technology, and telecoms to provide clear and consistent practical information and advice to protect the public against fraud. However, criminals carrying out APP frauds are increasingly using highly sophisticated tactics - such as employing the language of the police and bank staff - in

order to trick people into transferring or sending them money. Alongside well-honed techniques of social engineering, it can become extremely difficult, for the average person to appropriately challenge a fraud attempt. Whilst consumers and organisations that support them are taking appropriate action to safeguard against sophisticated fraud attempts, there must also be greater onus and incentive for PSPs to adequately protect them and stop them being victimised in the first place.

Question 3: Do you have any comments on our analysis of what is driving the Code outcomes we're seeing?

Age UK shares the view of the PSR that the current structure and implementation of the Code, alongside a lack of transparency and perhaps understanding from staff, has led to too many inconsistent interpretations of how it should be applied. If the Code's implementation 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'.

Regulations state that the consumer must have acted fraudulently, with intent, or with "gross negligence" in order to fail to qualify for a refund. The Financial Ombudsman Service (FOS) states "we take the view that "gross negligence" is a suitably high bar that goes well beyond ordinary carelessness" – the lenders should not take their customer's authorisation at face-value. However, this seems to be precisely what is happening in a number of instances.

It is the responsibility of multiple stakeholders across the industry to ensure that there is greater public awareness and understanding about the Code. To build and maintain public trust in the payments system, consumers will expect to receive consistent treatment and outcomes under an industry-wide code. When customers in 'no blame' situations are not being reimbursed then it shows the Code is not working as it was intended. Those who due to their circumstances are less able to effectively advocate for themselves either to their PSP or to the FOS, need an improved and consistent level of protection.

Question 5: Are there any other issues with the CRM Code you would like to tell us about?

'Vulnerable' is not a term many people would use to describe themselves, particularly those who may be most at risk of the serious harm of an APP fraud. Many victims of scams blame themselves and feel ashamed when reporting an incident, even when they would not be reasonably expected to be able to challenge an attempted fraud. Firms should be employing a consistent process to assess levels of vulnerability; in the same way they would do for other issues to do with account opening and management. Firms should consider 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).

Firms are failing to appropriately assess vulnerability properly which can lead to people not being reimbursed. Whilst the FOS has a responsibility to deliberate on cases of disagreement between two parties, it is not beneficial for any party, the individual, PSP, or FOS themselves to have to deliberate cases where victims should have been refunded in the first instance.

The PSR should also consider the impact of the pandemic on how people bank and manage their money. Many banks have temporarily shut, and a large number of branches have permanently closed, continuing long-running trends that reduce face-to-face interactions when people are managing their money. This will disproportionately impact certain groups such as older people and

those living with disabilities. The banking protocol has been a largely successful initiative designed to train staff to spot signs of fraud and abuse. However, if this 'friction' of trained staff able to prevent fraud is reduced, then it creates opportunities for criminals to exploit the deficit. This move away from in-person banking, with consumers now expected to manage their money online, could be fraught with risk for those that don't have the skills, confidence, and equipment to safely do so. If PSPs are fundamentally changing the way millions of consumers manage their money, then due consideration and action must be taken to ensuring they are appropriately protected from fraud and abuse.

Question 6: Do you have any comments on this measure, or its effectiveness and proportionality? For example, do you have feedback on the information we propose for publication outlined above, or on who should publish the data?

We support this measure to help improve the consistency of decision-making processes. Improved information sharing and scrutiny by consumers and regulators will help improve choice and competition and should lead to better consumer outcomes. It is also important for best practice to be shared amongst the wider industry. Greater transparency around case reviews, the consistent application of the Code, and how expectations on customers are reasonably applied to real life cases should all be made publicly available. We would also be very interested to see examples of cases where firms have decided that consumers did not act with appropriate levels or care and could have done more to prevent the scam.

All stakeholders will value improved evidence about what customers need to do to protect themselves from APP fraud. Overtime we would expect to see reductions in cases referred to the FOS, who should also publish data on the APP cases it receives for each provider.

We note that the following measures taken out of context could be misleading e.g., there could be an increase in APP fraud. However, publishing of the following metrics should help improve understanding of the Code's effectiveness.

- Total value of APP fraud in the reporting period
- 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
- Information around what constitutes an effective warning

Question 8: Do you have any comments on Measure 3A? For example, do you have feedback on the design, or its effectiveness and proportionality?

We support this option as it provides a simple and consistent system for victims. The current approach through the CRM Code is an improvement but it has not worked as intended. It should cover all types of APP scams and if a simpler standard of care is required then this should be based on the same legal basis that is used for unauthorised fraud, with victims reimbursed except for cases of gross negligence or first party fraud.

Question 9: Do you have any comments on Measure 3B? For example, do you have feedback on the design, or its effectiveness and proportionality?

We do not believe this measure, effectively an industry written code, will improve consistency and could cause confusion for victims with multiple codes existing across different PSPs. We do not

believe it is realistic for a new PSR Code approved by all sectors in a timely manner. TSB's fraud guarantee has shown that there are alternative models to the way the Code currently operates, and that the vast majority of consumers should expect to be reimbursed.

Question 10: Do you have any comments on these issues? For example, do you have feedback on whether we should use a direction or a rule change to pursue these measures, or whether Bacs should be included?

Important that as many APP scams are as included as possible and stay within the scope of a reformed mandatory Code.

Question 11: Do you have any comments on our proposal to conduct an equality impact assessment for any measures developed following this call for views?

We would support an equality impact assessment which could be based on the FCA's drivers of vulnerability and protected characteristics under the Equality Act.