Consultation Response

Authorised push payment (APP) scams: Requiring reimbursement consultation.

Payment Systems Regulator (PSR)

November 2022

Contact: john.kamoto@ageuk.org.uk

Age UK
7th Floor, One America Square
17 Crosswall
London
EC3N 2LB
T 0800 169 87 87 **F** 020 3033 1000
E policy@ageuk.org.uk
www.ageuk.org.uk

About this consultation

The Payment Systems Regulator (PSR) is aiming to reduce Authorised Push Payment (APP) scams significantly by introducing mandatory reimbursement for victims in all but exceptional cases. This consultation asks for views on proposed measures to: Require reimbursement in all but exceptional cases; improve and make consistent the levels of protection; incentivise banks and building societies to prevent APP scams. The PSR will consider responses in developing its policy decisions on pertinent regulatory requirements in the first quarter of next year. The Regulator will also publish a policy statement on mandatory reimbursement and draft regulatory requirements in line with statutory deadlines. In the second quarter, the PSR will publish the final regulatory requirements.

Key points and recommendations

- Age UK welcomes the introduction of the reimbursement requirement after APP fraud has occurred.
- We encourage the regulator to work with firms, the Government, the third sector, and the police to develop a comprehensive preventative strategy to sit alongside these proposals.
- Age UK strongly agrees with the proposal to require reimbursement of vulnerable consumers and those with protected characteristics even if they acted with gross negligence.
- The broadest definition of vulnerability should be consistently applied by all Payment System Providers (PSPs) when assessing liability to APP scams,
- We are concerned firms may be less likely to continue providing services to those at higher risk of scams – the Government, Financial Conduct Authority and PSR must monitor this and ensure equal access to payment systems.
- PSPs must provide offline routes (e.g., in a bank branch or over the phone) for consumers to manage payments, demonstrate the legitimacy of transactions, report fraud, and access an APP refund.
- PSPs should comprehensively promote the reimbursement scheme via both online and offline routes – this must include print media, mail drops, and community and voluntary organisations.
- Firms and PSPs must ensure the mechanism for accessing the new reimbursement scheme is intuitive and accessible for digitally excluded older people and those with only low-level digital skills.

- The PSR should investigate extending mandatory reimbursement to include victims defrauded via wider payment systems (e.g., BACS transfers and cryptocurrency platforms).

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 this consultation[1] on improving redress for victims of Authorised Push Payment (APP) scams. APP fraud involves criminals tricking people into transferring money to them by posing as legitimate payees or socially engineering reasons for payment. This type of fraud has increased substantially in recent years and remains the most significant type of payment fraud in the UK. 2021 saw losses of £583.2m – an increase of 39% from the previous year.[2] In the first half of 2022, compared to the same period in 2021, APP fraud fell by 17 per cent,[3] but it is still higher than in the same period in 2020. Many cases go unreported, so actual figures are likely to be higher.

Fraudsters continue to devastate the lives of older people – annually, around one in twelve (940,000) will fall victim to a scam[4]. APP scams can be highly insidious as victims can lose their life savings in a matter of just seconds, suffering catastrophic, life-changing losses. This can destroy not just their finances but their physical, mental, and emotional well-being. As a result, Age UK warmly welcomes the PSR's mandatory reimbursement proposals.

Implementing the Contingent Reimbursement Model (CRM) Code in 2019 represented a significant leap forward in protecting consumers, but some victims were denied protection because the Code was not mandatory. In the first six months of 2022, 56% of APP scam victims had their funds returned.[5] Although this is an improvement, Financial Ombudsman

Service (FOS) complaints about banks' handling of authorised fraud – the majority of which are APP – increased in the 2021-22 financial year, from 7,700 to 9,370.[6]

We welcome the PSR's proposed scheme to make reimbursement mandatory, as this will ensure the vast majority of APP scam victims receive financial compensation regardless of who they bank with. While we have specific recommendations for maximising the success of the PSR's proposals, we want to make it clear that we strongly support the principle of mandatory reimbursement and are keen to see these proposals implemented as swiftly as possible.

Our extensive experience delivering support to vulnerable older people has given us unique insight into the devastating impact fraudsters have on the lives of older victims. Alongside the PSR's proposals, we want all banks, building societies and other payment providers to do more to prevent APP scams from occurring in the first place. UK Finance has warned that the level of fraud in the UK has reached a point where it must be considered a national security threat,[7] a sentiment we strongly share.

While enforcing the liability of Payment Systems Providers (PSPs) for fraudulent transactions is a welcome development, prevention of scams is also key. Even after the PSR implements its proposals, the benefits will only be felt by older people who have already been victimised, with all the stress and strain this entails. We believe that alongside these proposals, there needs to be a renewed focus on preventing fraud. This will require the Government, police, regulators, industry bodies, payment service providers and the community and voluntary sector to work collaboratively to shut down the scammers and reduce the wider risk of fraud.

1. Do you have views on the impact of our proposals on consumers?

These proposals will be of tremendous benefit to older consumers. Fraud affects people of all ages and backgrounds, but older people can be particularly vulnerable to certain scams – often leading to severe emotional and financial harm. One in 12 older people (eight per cent) – around 940,000 – are victims of scams each year.[8] A recent survey by Which? found fraud victims aged 65 and over reported losing more money than any other age group (an average of £2,697 compared with £1,731 overall).[9] Women aged 65 and over lost twice as much as male victims of the same age. Older people may be specifically targeted for scams because of their age. Some may be particularly vulnerable due to ill health, dementia, social isolation, digital skill needs, and a perception of increased wealth.[10] With this in mind, Age UK warmly welcomes the regulator's proposal to impose mandatory reimbursement for all APP scams to benefit older consumers by substantially increasing the proportion of victims reimbursed by PSPs.

However, there is a risk that mandatory reimbursement proposals could incentivise some PSPs to apply stringent criteria when deciding whether to allow a customer to open an account. We are concerned that firms may be less likely to continue providing services to those at higher risk of falling victim to scams – including many older people. This would be a patently unacceptable outcome at odds with PSR and Government efforts to improve financial inclusion.

Although we want firms to refuse atypical transactions to deter fraudsters, we do not want aggressive warnings geared specifically towards demonstrating gross negligence on the consumer's part if they proceed. Our concern is that this may create an unwelcome environment for consumers, with PSPs trying to use disclaimers to get around the rules and make it increasingly difficult to access a legitimate reimbursement claim. This approach could also result in lengthy battles through the Ombudsman or the courts to resolve who is at fault in different scenarios. This should not be confused with a clear warning of a potential scam which is of course an essential preventative measure.

Older people also face increased rates of digital exclusion, with two-fifths of those aged 75+ not using the internet. Age UK is aware that some older people are increasingly reluctant to use online payment services because of greater awareness and fear of scams, with 39% saying they don't trust the internet.[11] Santander data shows that the number of those over 55s who continue to avoid using digital banking has remained roughly the same since the pandemic, with around one in six (16%) choosing not to use their bank's digital services to manage their money. Among those over 55s who don't bank online, 64% blame concerns over security.[12]

PSPs must be mindful of consumers facing barriers to getting online and those who are reluctant to undertake day-to-day transactions or manage their money over the internet. PSPs must provide offline routes (e.g., in a bank branch or over the phone) for consumers to manage payments, demonstrate the legitimacy of a transaction, report suspected fraud, access an APP refund, and speak with their provider about any concerns. PSPs should be mandated to comprehensively promote the reimbursement scheme via online and offline routes. The PSR should also arrange the promotion of the scheme through various sources, including print media, mail drops, and community and voluntary organisations.

2. Do you have views on the impact of our proposals on PSPs?

The proposed measures will significantly impact the PSPs' reimbursement requirements and public image, incentivising firms to focus on their communication and education strategies. Only 51% of APP scam losses were reimbursed to the victim under the Voluntary Code in 2021, creating a reimbursement lottery depending on who you bank with.[13] As mentioned, complaints to the FOS about banks' handling of authorised fraud cases – the majority of which are APP – have increased. And three-quarters (73%) of these were upheld in favour of the customer, so banks often get it wrong. These proposals will compel PSPs to do better.

3. Do you have views on the scope we propose for our requirements on reimbursement?

Age UK welcomes the introduction of the reimbursement requirement after APP fraud has occurred, but it is also important that more action is taken to prevent APP scams in the first place. We would encourage the regulator to work with firms, the Government, the third sector, and the police to develop a comprehensive preventative strategy. Reimbursement is a critical component of ensuring consumer redress after a scam, but by the time this occurs many of the negative consequences of being targeted have already taken their toll on the victim.

From experience, we know that for many older victims, this creates a sense of panic at the prospect that they may have been defrauded out of life-changing amounts of money. Needless to say, the impact on their mental and physical well-being can be truly devastating, often leaving them fearful and isolated. While the PSR's proposals will doubtlessly bring much-needed relief to many more victims, it is important comprehensive preventative measures are put in place alongside these proposals.

Technology and telecoms firms, which are part of the APP scams ecosystem, also need to do more to stop scams at source before they adversely impact consumers. UK Finance analysis has shown that seven in 10 (70%) of APP scam cases originate through search engines, social media, and fake websites.[14] We welcome the Government's intention to combat scam advertisements in the Online Safety Bill and hope to see this carried out.

4. Do you have comments on our proposals:

• that there should be a consumer caution exception to mandatory reimbursement
• to use gross negligence as the consumer caution exception
• not to provide additional guidance on gross negligence?

The regulator is proposing an exception to mandatory reimbursement if a consumer is grossly negligent, which aims to incentivise customers to take care. This is designed to limit any disproportionate costs to PSPs if customers were to exercise less caution following the implementation of mandatory reimbursement. However, there is no evidence to show that consumers will act with less caution following implementation. If the regulator goes ahead with this, they should require PSPs to provide consumers with clear guidance on what they expect of their customers. The regulator should be clear what constitutes gross negligence and take legal advice to ensure that it aligns with a consistent definition. Without a robust regime from the outset, we can expect years of legal challenges.

We note that TSB bank exemplifies gross negligence as repeatedly ignoring safety advice. This has resulted in a 98% reimbursement rate due to scams under their fraud refund guarantee. In contrast, at other banks, on average, only 47% of stolen money is refunded to victims.[15] We want a robust and consistent definition of gross negligence policies similar to TSB's determination of gross negligence applied by other PSPs to achieve similar reimbursement rates. The regulator should consider committing to TSB's fraud refund guarantee as additional guidance for gross negligence to cover consumers against honest mistakes.[16]

5. Do you have comments on our proposal to require reimbursement of vulnerable consumers even if they acted with gross negligence?

Age UK strongly agrees with the proposal to require reimbursement of vulnerable consumers and those with protected characteristics even if they acted with gross negligence. As the regulator rightly points out, there is evidence that older consumers are more likely to be victims of APP scams.[17] Some older people are especially at risk, either because scammers target them or because their circumstances make them vulnerable to scams, for example, if they are recently bereaved, lonely, or mentally or physically ill. Evidence also shows that there is a correlation between ageing and the likelihood of falling victim to a scam.[18] For older people experiencing mental health problems, it can mean they are less likely to get their money back and are more than twice as likely to fall into debt because of fraud.[19]

To advance equality of opportunity, the regulator should implement this requirement within its powers to require mandatory reimbursement in cases of APP scams. The regulator might consider utilising centralised records of vulnerability across the payment system to ensure consistency of approach for all PSPs' customers. The Lending Standards Board has highlighted that when disclosure of a vulnerability is not apparent or forthcoming from customers, firms tend to struggle to identify vulnerable cases.[20] This can happen at a firm and employee level due to poor questioning of customers and the need for awareness training on vulnerability to scams.

Although we are supportive, an existing vulnerability or protected characteristic must not be used to discriminate against consumers when it comes to accessing payment services. PSPs should review their vulnerability training to ensure that customer circumstance is fully considered. This could lead to more specialised teams that comprehensively account for consumer vulnerability and determine a customer's circumstances so as to understand how this has impacted them when being scammed. We urge the regulator to ensure PSPs improve their vulnerability training, so that customer circumstance is fully considered.

6. Do you have comments on our proposal to use the FCA's definition of a vulnerable customer?

While it is important that older age is not automatically equated with vulnerability, Age UK is acutely aware that people in later life are more likely to be exposed to the circumstances (e.g. social isolation, digital exclusion, poor health) which make them more vulnerable to exploitation by fraudsters. We would therefore welcome a definition of vulnerability which comprehensively encompasses at-risk older people. This will better reflect the threat they face from fraudsters, particularly given that they generally suffer higher losses[21], while mitigating the risk of them missing out on reimbursement due to issues such as digital exclusion.

The Financial Conduct Authority's (FCA) definition of a vulnerable customer as "someone who, due to their circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care" serves as an appropriate definition, particularly as some PSPs and the FOS have applied this concept previously.[22] We welcome the PSR using this definition, particularly as customers identified as vulnerable via this approach will be exempt from claims of gross negligence. However, we wish to reinforce that this definition must be interpreted in a consistent way with a focus on ensuring the broadest range of vulnerable customers are included within the scope.

The FCA views vulnerability as a spectrum of risk, which we agree with. All consumers are potentially vulnerable to APP scams, but this risk is increased by certain characteristics such as mental health problems, physical disability, and low income. Many other factors, such as 'time poverty', confidence in using the internet, and educational attainment, are likely to affect consumers' ability to engage in specific markets.[23]

Recently, a Pay.UK poll found that 54% of UK adults had at least one characteristic of financial vulnerability[24] – in line with the FCA's most recent survey (53%, as of October 2020).[25] Indeed, there are specific market contexts in which all of us can experience a degree of vulnerability – for example, when we need to purchase at a stressful time. Vulnerability is also known to arise when assessing the value of a product, where it involves complex estimations of risk or probability. UK Finance highlighted this year that more than half of the public (56%) said they are likely to look for opportunities to make extra money in the coming months due to the rising cost of living. And one in six (16 per cent) Britons said the increasing cost of living meant they were more likely to respond to an unprompted approach from someone offering an investment opportunity or a loan.[26] This could leave many people more susceptible to fraud. Therefore, we would like to see the broadest definition of vulnerability applied by all PSPs when assessing liability to APP scams, which we believe the FCA's above definition should cover.

7. Do you have comments on our proposals that:

• sending PSPs should be allowed to apply a modest fixed 'excess' to reimbursement
• any 'excess' should be set at no more than £35
• PSPs should be able to exempt vulnerable consumers from any 'excess' they apply?

We understand the rationale behind the proposal to allow sending PSPs to apply a fixed 'excess' of £35 to reimbursement as an incentive for smaller PSPs to use preventative measures and deal with administration costs. However, currently under the CRM Code, victims of APP fraud get all their money back if the customer has taken all the steps set out in the code.[27] When there is an increase in the cost of living, applying an excess to individuals who have reasonably done all they can to protect themselves is not practicable. PSPs should consider an individual's financial circumstances when assessing if they should implement the excess of £35. We therefore call for an exception for vulnerable customers from the £35 excess.

8. Do you have comments on our proposals that:
• sending PSPs should be allowed to set a minimum claim threshold
• any threshold should be set at no more than £100
• PSPs should be able to exempt vulnerable consumers from any threshold they set.

We know there will be a post-implementation review of the minimum claim threshold to see if it needs to be reduced or eliminated. Age UK's view is that within the context of a cost-of-living crisis it would be better to instead trial the mandatory reimbursement scheme without the £100 minimum and then consider if this needs to be added later.

While we understand the rationale for the proposal that the sending PSPs should be allowed to set a minimum claim threshold of no more than £100, we are concerned about the impact this might have on those struggling to balance their household budgets. While

APP scams under £1000 represent just 8% of losses by value[28] the PSR must be mindful that for many of those reliant on the State Pension as their sole source of income a hit of less than £100 to their bank balance can still prove a devastating blow to their finances. Our view is that it is often less about the volume of money taken and more about the impact this has based on the specific circumstances of the victim.

Furthermore, we can envisage scenarios where scammers target victims to make small payments over a period. As we know, victims often end up on lists passed around by criminal groups perpetrating scams. In these circumstances, we do not want the discretion to be up to PSPs to determine if these victims should be reimbursed – instead, we want these transactions to be counted cumulatively instead of being treated in isolation. It is crucial that if scammers target victims multiple times over separate transactions for less than £100 at a time, that any minimum claim threshold cumulatively accounts for this rather than treating them as separate incidents.

We would also warmly welcome a minimum claims threshold exemption for vulnerable consumers. We strongly encourage the PSR to go further than its proposals and make this vulnerability exemption mandatory across all PSPs.

9. Do you have comments on our proposal not to have a maximum threshold?

We strongly agree with the proposal not to have a maximum threshold. Increasing numbers of older people risk losing truly staggering sums of money through APP scams. Given this, we agree that if a PSP allows a substantial fraudulent payment, it should be liable for victim reimbursement regardless of the value of the transaction. This will ensure protection for those who might otherwise lose their life savings through no fault of their own.

10. Do you have comments on our proposals that:

• sending PSPs should be allowed to set a time-limit for claims for mandatory reimbursement
• any time limit should be set at no less than 13 months?

We understand the reasoning for allowing sending PSPs to set a time-limit for mandatory reimbursement, as we acknowledge this is the same limit set for claims for refunds of unauthorised payments under the Payments Systems Regulations 2017.[29] However, there is an issue where some payment instructions will be large amounts from fictional investment and pensions schemes (or romance fraud), and it may not be apparent that these payments have been fraudulent for many years.

Indeed, as part of its latest quarterly data publication, the Financial Ombudsman has found that investment scams have seen the most considerable increase in the proportion of “authorised” scam complaints, despite the number of “authorised” scam complaints decreasing overall.[30] In such scenarios, a 13-month time limit is not realistic. Granted, the regulator has noted that consumers may appeal to the Financial Ombudsman Service (FOS) up to six years from a problem occurring, or longer, if still within three years of the consumer becoming aware (or when the consumer should have reasonably become aware) of the scam.

However, our concern is the extent to which the 13-month time limit would curtail the powers of the FOS and prohibit victims from accessing reimbursement. We encourage the PSR to implement a more flexible approach, avoiding setting a hard deadline regardless of circumstances. This would ensure that victims of particularly insidious scams, such as romance fraud, who may not have been aware that they were scammed until much later than 13 months, can still come forward and access reimbursement from PSPs.

11. Do you have comments on our proposals that:

• the sending PSP is responsible for reimbursing the consumer
• reimbursement should be as soon as possible and no later than 48 hours after a claim is made unless the PSP can evidence suspicions of first-party fraud or gross negligence.

We agree with this approach. The Lending Standards Board (LSB) has reported that nearly all PSPs’ processes of assessing reimbursement claims focus their investigation on the repatriation of funds from the receiving bank. Conversations with customers tend to allude to the fact that reimbursement would only be successful if the receiving bank had managed to freeze and return the funds to the sending bank.[31]

By compelling the sending PSP to reimburse victims of APP fraud as soon as possible and no later than 48 hours, we hope this will deter firms from giving victims incorrect information of placing reimbursement solely on recovery of funds from the receiving firms. Ultimately, we hope this will put less onus on the victim to prove themselves by jumping through standard-of-care tests, which require consumers to meet a disparate set of standards imposed by different PSPs before being reimbursed.

12. What standard of evidence for gross negligence or first-party fraud would be sufficient to enable a PSP to take more time to investigate, and how long should the PSP have to investigate in those circumstances?

The provision of a warning should not be used as evidence for gross negligence or first-party fraud or as a strict measure of liability for declining reimbursement. Nor do we believe Confirmation of Payee (CoP) should be used by PSPs as a rigorous measure of liability in declining reimbursement. All considerations concerning the scam should be deliberated to assess the victim's reasonable basis for belief and inform the PSPs' cause for investigation.

As mentioned above, PSPs may try and gear their warnings toward proving gross negligence which consumers may not pay mind to as they believe the transaction to be legitimate (as such is the reality of being scammed). Therefore, using such warnings and CoP may allow situations where PSPs treat legitimate victims negatively.

13. Do you have comments on our proposal for a 50:50 default allocation of reimbursement costs between sending and receiving PSPs?

Ultimately, we would like to see a system where the reimbursement levels are split 50:50 at the outset. Current data shows that receiving PSPs are not doing enough to reimburse victims (contributing less than 5% on average to reimbursement costs) even though the fraudster banks with them.[32] Receiving PSPs must do better in vetting their clients and ensuring a stable financial ecosystem that avoids harm to UK consumers, especially those at risk or vulnerable to becoming victims.

While we are cognisant that this may disadvantage new market entrants[33] we don't want a situation where smaller PSPs are freely onboarding customers and not doing their due diligence in the name of competition. We believe smaller PSPs and new entrants should respond by developing more effective fraud controls. Granted, such advanced controls would also come at a cost. Nevertheless, smaller PSPs and new entrants should now start considering how this proposed model might affect them and what improvements they can make to their system to disrupt scammers and create a more secure financial ecosystem.

A 50:50 default allocation of reimbursement costs between sending and receiving PSPs will enable cross-sector data-sharing to better prevent and detect APP scams. Data and information sharing will be crucial to dealing with APP fraud. By incentivising both the sending and receiving PSPs to share data through a default allocation of reimbursement costs, the regulator will ensure industry pursues preventative measures to tackle APP fraud. Moreover, since better information sharing is one of the Strategic Objectives of the UK Government's current Economic Crime Plan (and is likely to underpin the upcoming second iteration), we believe this proposal aligns with the Government's sentiment that prevention is better than cure.[34]

14. Do you have views on our proposal that PSPs can choose to depart from the 50:50 default allocation by negotiation, mediation or dispute resolution based on a designated set of more tailored allocation criteria?

We fear that departing from the 50:50 default allocation by negotiation, mediation, or dispute resolution based on a designated set of more tailored allocation criteria will lead to tension between PSPs. We can envisage situations where PSPs differ in opinion in developing and implementing such arrangements. For example, the Lending Standards Board indicates a need to draw out expectations more clearly for receiving firms. After all, a PSP has helped scammers collect their money. It is not right that receiving PSPs do not contribute enough to reimbursement costs. Receiving PSPs must do better to vet their customers and ensure a stable financial system. Therefore, we do not support the proposals to depart from the 50:50 default allocation. We prefer if they both automatically send 50% to the victim. Then they can depart from the 50:50 allocation if they have repatriated the funds. If banks are compelled to each send 50% of the stolen money, then all PSPs will do more to communicate quickly and effectively work with one another to detect and freeze fraudulent funds. This should allow for all PSPs to implement stringent preventative mechanisms that deter APP scams from happening in the first place.

15. Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational scams?

Multi-generational scams are where the end-to-end journey involves more than one payment. For example, fraudsters may ‘socially engineer’ a consumer to transfer money from their bank account to the account they hold at a different PSP (or perhaps persuade them to open a new account in their own name). The fraudster then persuades the consumer to transfer the money from that account into the account under the fraudster’s control. Sometimes, that second payment may be a transfer using Faster Payments to an account held at a PSP. In other cases, the second payment may be to a different type of account, such as a crypto wallet, which does not happen over Faster Payments, but uses an alternative method (e.g., a card or crypto-based payment system). An increasing proportion of scams involve consumers being convinced to move payments from their bank accounts to accounts in their name with legitimate cryptocurrency platforms, with converted cryptocurrency then transferred to the scammer. The funds remain in the consumer’s control after the initial transfers from the account with the PSP, and the scam takes place from the cryptocurrency wallet (and not by Faster Payment). It is not clear if such scenarios of multi-generational fraud are intended to be covered by the mandatory reimbursement proposal. Which? have warned that there is limited legal protection for such losses with their research finding that 20% of fraud victims tricked into sending money to criminals in the past two years used cryptocurrency, and 17% used digital wallets such as Apple Pay.[35] It remains unclear how the proposed 50:50 default allocation can be applied in these instances. This represents a potential gap in the PSR’s proposals as cryptocurrency exchanges cannot, as it stands, be required to refund their customers.

The regulator must analyse these situations further to determine the liability of mandatory reimbursement. Age UK would encourage an approach which extends reimbursement to include victims defrauded via cryptocurrency platforms.

16. Do you have comments on our proposal for a 50:50 default allocation of repatriated funds between sending and receiving PSPs?

Repatriation of APP scam losses occurs when the receiving PSP can detect, freeze, and return funds stolen as part of an APP scam. Fast and effective communication from the sending PSP may aid receiving PSPs in detecting and freezing fraudulent funds. Data from UK Finance show that there are currently very low repatriation rates. In 2021, £12.4 million was returned to victims through repatriation, accounting for just 5% of the total reimbursed to victims by CRM Code signatories.[36]

Scammers often quickly transfer stolen money to other accounts and jurisdictions, making it hard for PSPs to trace and return. However, there is also a lack of incentive for receiving PSPs to try increasing repatriation rates. Age UK believes that a 50:50 default allocation of repatriated funds between sending and receiving PSPs is the right way to incentivise all PSPs to prevent APP scams from happening in the first place. Nevertheless, this will only work if the mandatory reimbursement is split 50:50 between the sending and receiving banks as a default – if banks are compelled to each send 50% of the stolen money, then all PSPs will do more to communicate quickly and effectively with one another in order to detect and freeze fraudulent funds.

17. Do you have views on the scope we propose for rules on allocating the costs of mandatory reimbursement?

We welcome the proposal that the rules on allocating reimbursement costs apply to all directly connected PSP participants sending and receiving payments over Faster Payments and PSPs indirectly sending and receiving payments. Trends show scammers are migrating to receiving PSPs who are not participating in existing safeguards such as the CRM Code and CoP. For example, PSPs that were not given Specific Direction 10 (SD 10)[37], requiring the UK's six largest banking groups and building societies to provide CoP checks for Faster Payments, accounted for 20% of Faster Payment transactions in 2021 but received 50% of APP scam payments sent from SD 10 PSPs. Applying the allocation of costs of reimbursement to all directly connected PSPS and indirect PSPs sending and receiving payments would allow for a consistent model and incentivise all PSPs to detect and prevent APP scams.

18. Do you have views on our long-term vision and our rationale for the PSO being the rule-setter responsible for mitigating fraud?

We cautiously welcome the call for the Payment Systems Operator (Pay.UK) to introduce new rules to provide better governance of the payment systems under its control. We are cautious in supporting this expanded role for Pay.UK because it has so far failed to implement fraud mitigation measures in its ruleset without intervention from the PSR.

Currently, Pay.UK's existing constraints do not allow for implementing the proposals set out. However, in the long term, after developing the resources and arrangements it requires, Pay.UK may be the appropriate body to undertake the role of maintaining, refining, monitoring, and enforcing compliance that addresses fraud risk in the system. We would welcome ongoing consultation on what arrangements for the monitoring and assurance of implementing the regulator's requirements are needed for Pay.UK to carry out this role adequately.

21. Do you have views on how we propose that allocation criteria and dispute resolution arrangements are developed and implemented?

We cannot foresee a scenario where dispute resolution arrangements for allocating reimbursement liabilities are developed and implemented in the short term. The regulator posited a system where this arrangement could be implemented after asking the industry to develop and implement the agreements. However, this scenario would most likely return a varied response from PSPs and push such arrangements back into the long term.

If the regulator does choose to impose a dispute resolution arrangement, it would be better if a body such as the LSB maintained such arrangements. The LSB already oversees, monitors, and enforces the CRM Code and has made significant progress in identifying a set of standards for preventing and detecting APP scams and linking these to the allocation of reimbursement liabilities. Such future arrangements would therefore be better built on the achievements of the LSB by designating them to oversee the allocation of reimbursement liabilities.

22. Do you have comments on our preferred short-term implementation approach of requiring Pay.UK to implement an effective compliance monitoring regime, including a reporting requirement on PSPs?

One of the key challenges of the mandatory reimbursement proposal is ensuring PSPs follow the rules. The PSR will need comprehensive and timely information on compliance to pursue any necessary enforcement action or provide regulatory updates if required. A clear and rigorous compliance assessment framework is essential to achieving this goal. This monitoring regime must be implemented from the outset of the mandatory reimbursement scheme. PSPs should be required to report regularly to Pay.UK on their performance. This will ensure that regulators, consumer groups, and the Government can assess the Scheme and, if necessary, recommend changes.

23. Do you have views on the costs and benefits of Pay.UK implementing a real-time compliance monitoring system, and when could it be introduced?

As outlined in response to question 22, the PSR must ensure that a monitoring regime is implemented from the outset of the mandatory reimbursement scheme. This should include a real-time compliance monitoring system as early as possible.

24. Do you have views on the best option for short-term enforcement arrangements?

The best option for short-term enforcement would be for the regulator to apply fines and penalties on any PSP that fails to comply with scheme rules on reimbursement within the set timescale. If these measures fail to ensure the rules are followed in the short term, the regulator should escalate action against non-compliant PSPs. Any proceeds from fines or penalties should also be redirected towards scam victims.

This would give Pay.UK time to develop and improve its enforcement regime. Longer term, we would like to see Pay.UK apply its enforcement regime as the Payment Systems Operator, but with escalation to the PSR as one of the steps in that regime.

25. Do you have views on the best way to apply the rules on reimbursement to indirect participants?

The Faster Payment System allows all participants to connect safely and securely, directly or indirectly, to the Faster Payment System central infrastructure to facilitate real-time payments. However, presently, Faster Payment rules only apply directly to direct participants. The regulator has posited that if it were to initially implement reimbursement requirements on PSPs through a direction, with Pay.UK operationalising those requirements, the regulator's direction would apply to direct and indirect participants.

Although this is not the PSR's preferred option, this option would enforce reimbursement rules for all Faster Payments. We suggest such rules apply initially so that older consumers are protected before, longer term, the New Payments Architecture (NPA) rules on reimbursement apply to all NPA participants (direct and indirect participants of Faster Payments).

---

[1] : CP22/4: Authorised push payment (APP) scams: Requiring reimbursement | Payment Systems Regulator (psr.org.uk)
[2] Fraud The Facts 2021- FINAL.pdf (ukfinance.org.uk)
[3] APP fraud - less talking, more acting | Insights | UK Finance
[4] Age UK analysis of data from the Crime Survey for England and Wales 2018-19, scaled up to the England and Wales aged 65+ population using ONS midyear population estimates for 2020.
[5] Half year fraud update 2022.pdf (ukfinance.org.uk)
[6] Annual complaints data and insight 2021/22 (financial-ombudsman.org.uk)
[7] UK Finance: Scale of fraud a 'national security threat' | This is Money
[8] OLDER PERSON BECOMES FRAUD VICTIM EVERY 40 SECONDS| PRESS RELEASE | AGE UK
[9] One in five fraud victims send money to criminals via cryptocurrency - Which? News
[10] age_uk_briefing_fraud_and_scams_sept_2016.pdf (ageuk.org.uk)
[11] Age UK, 2021. *Briefing Paper: Digital inclusion and older people – how have things changed in a Covid-19 world?*. Age UK. [Online]. Available at: https://www.ageuk.org.uk/globalassets/age-uk/documents/reports-and-publications/reports-and-briefings/active-communities/digital-inclusion-in-the-pandemic-final-march-2021.pdf. [Accessed 05/08/21].
[12] Over 55s Flock Online during Coronavirus Pandemic but Miss Out on Digital Banking Opportunity | Santander UK

[13] Annual Fraud Report 2022_FINAL_.pdf (ukfinance.org.uk)
[14] 70% of APP scam cases start online, UK Finance study reveals - Money Age
[15] Annual Fraud Report 2022_FINAL_.pdf (ukfinance.org.uk)
[16] Fraud Refund Guarantee | TSB Bank
[17] Most vulnerable in society are more at risk of falling victim to fraudsters | Action Fraud
[18] Correlates of Susceptibility to Scams in Older Adults Without Dementia - PMC (nih.gov)
[19] Fraud victims experiencing mental health problems are twice as likely to fall into debt - Which? News
[20] CRM-Review-R21c-Follow-Up-Summary-Report.pdf (lendingstandardsboard.org.uk)
[21] One in five fraud victims send money to criminals via cryptocurrency - Which? News
[22] Guidance for firms on the fair treatment of vulnerable customers | FCA
[23] Consumer vulnerability: challenges and potential solutions - GOV.UK (www.gov.uk)
[24] Internal Longform (wearepay.uk)
[25] Financial Lives 2020 survey: the impact of coronavirus (fca.org.uk)
[26] Public are warned to stay alert to fraud as a result of the rise in the cost of living | Insights | UK Finance
[27] Information-for-customers-CRM.pdf (lendingstandardsboard.org.uk)
[28] Annual Fraud Report 2022 | Policy and Guidance | UK Finance
[29] The Payment Services Regulations 2017 (legislation.gov.uk)
[30] Consumers warned about rise in investment scams (financial-ombudsman.org.uk)
[31] CRM-Review-R21c-Follow-Up-Summary-Report.pdf (lendingstandardsboard.org.uk)
[32] CP21/10 Authorised push payment (APP) scams consultation paper | Payment Systems Regulator (psr.org.uk)
[33] New market entrants may argue that this approach could reduce competition because of the potentially significant cost implications for them as a new firm.
[34] [Title] (publishing.service.gov.uk)
[35] One in five fraud victims send money to criminals via cryptocurrency - Which? News
[36] Annual Fraud Report 2022_FINAL_.pdf (ukfinance.org.uk)
[37] PS19/4 - Specific Direction 10 (Confirmation of Payee) | Payment Systems Regulator (psr.org.uk)