

Policy statement

Fighting authorised
push payment fraud

A new reimbursement
requirement

Annex 3: Question-by-
question feedback and
response to our consultation

June 2023

Contents

| | | |
|---|--|----|
| 1 | Question-by-question feedback and response | 3 |
| | Question 1 | 3 |
| | Question 2 | 5 |
| | Question 3 | 6 |
| | Question 4 | 8 |
| | Question 5 | 11 |
| | Question 6 | 12 |
| | Question 7 | 13 |
| | Question 8 | 15 |
| | Question 9 | 16 |
| | Question 10 | 17 |
| | Question 11 | 19 |
| | Question 12 | 20 |
| | Question 13 | 21 |
| | Questions 14 and 21 | 23 |
| | Question 15 | 24 |
| | Question 16 | 25 |
| | Question 17 | 26 |
| | Questions 18, 19 and 20 | 27 |
| | Question 22 | 28 |
| | Question 23 | 29 |
| | Question 24 | 30 |
| | Question 25 | 31 |
| | Question 26 | 32 |
| | Question 27 | 33 |
| | Question 28 | 33 |
| 2 | Respondents to September 2022 consultation | 35 |

1 Question-by-question feedback and response

In this chapter, we have provided a summary of stakeholders' views and our response to each of the 28 questions in our September 2022 consultation (CP22-4).¹ Chapter 2 sets out a list of respondents.

Question 1

1.1 We asked respondents the following question:

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

Respondents' views

1.2 There were 58 responses to this question. The majority of respondents agreed with the principle that consumers should be protected from fraud and that victims should be reimbursed. However, industry and consumers group held polarised views on how the proposals would impact consumers. The majority of PSPs and their representatives (including trade bodies) argued that specific elements of our approach to introducing reimbursement could lead to a number of negative unintended consequences for consumers. Conversely, consumer groups and organisations generally strongly supported our approach because of the high level of customer protection proposed.

Positive impacts on consumers

1.3 Consumer groups argued that our approach was appropriate due to the significant impact that APP fraud has on consumers – and would continue to have even if reimbursement was more assured. Many victims struggle to recover from being victims of APP fraud, which has long-term negative impacts on their mental health, confidence, and relationships. Current pressures on the cost of living provided a further reason to reassure consumers that they were more likely to be reimbursed if they were defrauded.

1.4 Some respondents noted inconsistent consumer outcomes under the CRM Code and said firms use exceptions to the CRM Code that reinforce victim blaming. They argued that the new reimbursement requirement could lead to more consistent and fairer decision-making, and to full rather than partial reimbursement for more consumers. It was felt that our proposals would lead to greater confidence in Faster Payments – and that this would ultimately mean more competition and more choice for consumers. There was also support from consumer groups for the argument that firms would see greater incentives for preventing fraud.

¹ PSR, [Consultation CP22-4: Authorised push payment \(APP\) scams: Requiring reimbursement](#), (September 2022)

1.5 Consumer groups also welcomed the proposals on vulnerable customers.

Policy risks or negative impacts on consumers

Increased likelihood of moral hazard

1.6 Many industry respondents said our proposals would lead to a rise in the likelihood of moral hazard, arguing they do not give consumers the incentives to take sufficient care when making payments. This was felt to be especially a problem with setting the customer standard of caution at gross negligence. Certain types of APP fraud, such as purchase fraud and investment fraud, were highlighted as being at particular risk of moral hazard.

Increased risk of APP fraud

1.7 Arguments were also made by many industry respondents that reimbursement could lead to a rise in APP fraud. Reduced customer caution would increase the risk of fraud and could increase the number of criminals targeting the UK. Respondents also saw a risk of increased first-party fraud, where the prospects of financial gain would tempt consumers to become complicit in fraud.

Increased friction in the system

1.8 A number of concerns were raised by industry respondents about the direct impact on consumers. The greater liability imposed on PSPs could lead to increased friction in the payment journey with more transactions delayed or rejected. This could damage the user experience and reduce trust in account-to-account payments. Consumer groups agreed that our requirements would likely lead to greater friction in payments but saw this was necessary (where deployed effectively) to prevent fraud.

Risk that customers could be 'de-banked'

1.9 There was a concern that increased liability could lead PSPs to reduce their service offering to customers they judged to be at greater risk of fraud or more likely to be complicit as money mules. The proposal to exempt vulnerable customers from meeting the customer standard of caution could lead to more 'de-banking' of customers (full removal of their banking services) and could increase spurious claims of vulnerability by victims and claims management companies.

Impact on firms and the market

1.10 It was argued that our proposals could harm competition and customer choice, with firms either leaving the market altogether or 'de-risking' by withdrawing products and services (see 1.9). Some in industry believed our proposals would lead to an increase in claims management companies. This, they felt, would contribute to poorer consumer outcomes because reimbursements would take longer and would be reduced by fees to these companies.

Our view

- 1.11** We note that nearly all respondents recognised the need to prevent fraud and ensure victims are treated appropriately. APP fraud poses a significant threat to users of Faster Payments, with the number of APP fraud cases growing and losses totalled £485.2 million in 2022.² Besides financial losses, victims of APP fraud suffer worry, uncertainty and hardship. The government has recognised the harm caused by APP fraud through provisions in the Financial Services Market Bill (FSMB) which instructs us to introduce reimbursement. This instruction also sits within the Home Office’s Fraud Strategy which sets out a range of measures to assist fraud prevention and victim support.
- 1.12** The new reimbursement requirement will drive more consistent reimbursement for victims of APP fraud. We have designed our policy framework to be clear for customers to understand and for PSPs to operationalise. We also recognise that it will evolve and be refined over time (see policy statement, Chapter 1).
- 1.13** We are setting minimum standards, defining the outcomes we expect, and aligning financial and reputational incentives on payment firms. In adopting an outcome-based approach, we are giving payment firms the space to innovate and to choose how best to deliver the new reimbursement requirement for their customers.
- 1.14** We acknowledge the range of policy risks highlighted by respondents. We have addressed the risks thematically in the policy statement, including our mitigating actions (see Chapter 4, Table 4).

Question 2

- 1.15** We asked respondents the following question:

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

Respondents’ views

- 1.16** We received 64 responses that expressed views on the impact of our proposals on PSPs. There was a significant overlap in the issues mentioned in the responses to this question and the responses to Question 27 on the cost benefit analysis. The responses focused on eight main issues:
- a reduction in competition and innovation
 - the risk of vulnerable customers being ‘de-banked’
 - increased opportunities and risk of fraud
 - additional costs to PSPs
 - limitations on Pay.UK’s capacity to administer the system
 - increased friction in processing payments
 - the impact on PSPs of cost-sharing and payment type coverage

² In 2022, there were around 207,000 reported APP fraud cases on personal accounts (an increase of 6% on 2022). UK Finance, [Annual fraud report – The definitive overview of payment industry fraud in 2023](#) (May 2023).

- issues for PSPs around implementation of the proposal

1.17 Other views on the impact of the proposal on PSPs were expressed around wide definitions, inconsistencies in customer treatment, shifting fraud into crypto accounts and sharing accountability with social media and tech firms.

Our view

1.18 We have addressed these impacts in our updated cost benefit analysis. See the separate Annex 4.

Question 3

1.19 We asked respondents the following question:

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

Respondents' views

1.20 There were 58 responses to the question. Responses were mixed, with a wide variety of views on the scope of the proposals.

Scope of payment systems

1.21 Several PSPs agreed the focus on Faster Payments was proportionate for the proposals. However, many respondents who agreed with the principle of reimbursement felt that the proposals should be expanded to other payment systems to mitigate the risk of fraud migration. Other payment systems frequently referenced by respondents included 'on-us' payments, CHAPS and Bacs, while a smaller number of respondents called for systems such as cheques, crypto and Swift payments to be considered too.

1.22 Respondents diverged over PIS transactions. Some payment initiation service providers (PISPs) supported PIS transactions being in scope of the new reimbursement requirement (as long as the PISP was not liable to reimburse). Other PISPs argued to remain out of scope due to concerns that PSPs would place additional restrictions and friction on PIS transactions. One large PSP called for PISPs to be directly liable for any fraud incidents that took place over a PIS transaction.

Scope of APP fraud and jurisdiction

1.23 Consumer organisations agreed with the proposals for the new reimbursement requirement to include all types of APP fraud.

1.24 A significant number of PSPs called for further clarification on what qualifies as APP fraud, including which parts of a fraudulent payment journey the policy covers, and whether it would include all types of APP fraud. Respondents sought clarity over whether international payments would fall within the scope of the policy.

Scope of customers covered

1.25 The main issue raised by respondents regarding the scope of customers covered was whether the new reimbursement requirement should include microbusinesses and charities. Views were mixed. Some stakeholders, notably small business account providers, raised concerns that including microbusinesses and smaller charities could lead to a reduction in services available to these organisations. The same respondents said that these organisations are capable of bearing a higher responsibility than consumers. A minority of respondents argued for an expansion to larger businesses and/or charities.

Our view

1.26 We acknowledge that there would be benefits to expanding the scope of the new reimbursement requirement (or comparable protections) to other payments systems. It could further increase incentives for PSPs to act against fraud, lead to more consistent treatment for customers and help to level the playing field across different payment types. Any expansion would likely come with greater short-term costs for the industry and, in light of our statutory obligations to consult if we decided to include additional payment systems at this stage, could delay implementation. We are considering whether the new reimbursement requirement (or comparable protections) should apply to other payment systems. Further detail is set out in the policy statement, see Chapter 2.

1.27 All categories of APP fraud will be within the scope of the new reimbursement requirement. We have considered whether it would be appropriate to exclude specific types of APP fraud (such as purchase or investment fraud). But we concluded that this could lead to fraud migration, customer confusion and additional challenges in implementation.

1.28 With regard to additional clarity on terminology, we believe the existing definitions are sufficient. Where necessary, we have restated these in the policy statement (see glossary). We will provide further guidance on the customer standard of caution (gross negligence) as set out in Question 4.

1.29 The new reimbursement requirement applies to Faster Payments sent and received by PSPs in the UK across the Faster Payments system, including payment initiation service (PIS) transactions. The new reimbursement requirement does **not** apply to:

- civil disputes
- payments which take place across other payment systems
- international payments
- payments made for unlawful purposes

1.30 We have decided to include PIS transactions under the same obligations as other Faster Payments. We concluded that treating PIS transactions differently to other Faster Payments could create an imbalance in protections and provide a space for fraud to migrate into. We expect that this approach will provide consistent customer protections and incentivise PSPs to work with PISPs to prevent fraud. This aligns with our work on account-to-account payments and open banking.

1.31 The new reimbursement requirement covers the same types of payers as the CRM Code, to ensure consistency and build on existing customer understanding. This

includes consumers, microenterprises and charities as defined in the policy statement (see glossary). The CRM Code adds a specific exception for reimbursement for microenterprises and charities, *'where the Customer is a Micro-enterprise or Charity, it did not follow its own internal procedures for approval of payments, and those procedures would have been effective in preventing the APP scam'*.³ When developing further guidance, we will consider this exception as part of how the customer standard of caution might apply in the context of microenterprises and charities.

Question 4

1.32 We asked respondents the following question:

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**

Respondents' views

1.33 There were 48 responses to the question on whether the customer standard of caution should be gross negligence. 23 respondents (48%) agreed with this proposal.

A consumer caution exception

1.34 The majority of respondents supported the need for a consumer caution exception to reimbursement. Most stakeholders believed that all parties need to be incentivised to prevent fraud and that it is reasonable for consumers to exercise some caution when authorising payments. Some PSPs argued that this exception should vary by scam type.

1.35 A few consumer groups did not see the need for an exception, arguing that it may place too much responsibility on consumers to spot sophisticated scams and may limit the incentives on PSPs to prevent fraud.

Agreed with gross negligence standard

1.36 Most consumer groups, as well as a limited number of firms and technology providers, supported gross negligence as the customer standard of caution. Arguments included:

- Gross negligence was an appropriately high bar as the sophistication of APP fraud often left consumers with little opportunity to protect themselves.
- Consumer groups provided the example of other payment protections which shows little evidence that they cause consumers to take less care. They highlighted that TSB has reported no discernible increase in moral hazard from its Fraud Refund Guarantee.

³ LSB, [Contingent Reimbursement Model Code](#), (February 2023)

- There are already barriers to customers identifying and reporting fraud. Some consumer groups felt that PSPs could exploit any lower bar in order to deny reimbursement, and that this would further dissuade customers from reporting fraud.

Disagreed with the gross negligence standard

1.37 Most PSPs and trade bodies disagreed with setting gross negligence as the customer standard of caution. Arguments included:

- Gross negligence will remove customer caution and trigger unintended consequences, including increasing the risk of moral hazard.
- It is an exceedingly high bar and creates very significant risk of legal complexity and ambiguity.
- Gross negligence will not be simpler to introduce and requires definition to ensure consistency in application.

1.38 There were also calls for us to commission research to better understand the standard of caution acceptable to consumers.

Alternative proposals

1.39 In arguing for a different standard, several responses from industry proposed alternative models:

- Some called for a contributory negligence standard, which would place obligations on customers to take certain steps during the payment journey. If customers failed to take these steps and fell victim to APP fraud, they would not be reimbursed fully or at all.
- Some set out steps consumers should take, such as validating that a recipient is genuine, or engaging with warnings such as Confirmation of Payee (CoP) checks. Under the same heading, some called for the customer standard to vary by fraud type, complexity or customer. For example, setting a lower bar for purchase fraud.
- Some respondents felt there should be different rules for businesses, for example, if they used their accounts for non-business purposes such as sending money to a fraudster as part of a romance scam.
- One response called for an enhanced CRM Code, which would mandate the existing CRM Code's standards but include two additional exceptions – focusing on repeat victims and lying to your PSP.

Guidance on gross negligence

1.40 The majority of responses called for us to provide additional guidance on the gross negligence standard:

- Some respondents said that failure to provide guidance could lead to firms and the Financial Ombudsman Service applying the standard inconsistently and consequent delays in claim decisions. Choosing to wait for the ombudsman to establish case law may also impose time and financial costs on contesting parties. Several submissions called for us to consult further and work with the ombudsman to establish case law.

- Consumer groups expressed concerns that a lack of guidance around gross negligence would lead to PSPs setting the bar too low and abuse the exception to deny reimbursement.
- Some consumer organisations called for us at least to provide guidance on what does not count as gross negligence, to ensure consistent application.
- One consumer advocacy organisation was worried that a lack of guidance might put off consumers from claiming reimbursement due to a misunderstanding of the term.

1.41 One response noted that whether the exception was based on gross negligence or an alternative standard, static guidance can easily reflect the constantly evolving nature of fraud and social engineering.

Our view

1.42 We accept that a customer standard of caution is required to ensure customers take appropriate care when making payments. To improve customer outcomes in comparison to the existing CRM Code, a higher, clearer and more consistent bar to reimbursement is needed. Gross negligence is a high bar, which we believe would only be applied in a small number of cases. Where suspected, the burden of proof is on the PSP to prove gross negligence.

1.43 We have tested a range of alternative standards proposed in consultation responses. We see no credible alternative to gross negligence that would likely meet our stated objectives of preventing fraud, improving protections, incentivising innovation, and instilling greater confidence in Faster Payments. Gross negligence will support these objectives by ensuring a more consistent interpretation by the 1,500+ PSPs who can process Faster Payments.

1.44 Gross negligence as the customer caution of standard exception will best incentivise PSPs' efforts to prevent fraud as part of our balanced policy framework. The high bar will help ensure that firms are more proactive in assessing the risk of payments using customer analytics and shared intelligence. As the policy statement sets out (see Chapter 1), PSPs should intervene appropriately to pause, delay and stop suspicious payments where they identify high levels of risk. The government is looking at how legislation might need to change for payments to be delayed beyond the usual timescales (in a small number of cases) to better protect customers, where there are suspicions of fraud.

1.45 We also believe that setting gross negligence as a high, clear bar will help ensure that firms reimburse in the first instance. Under the CRM Code in 2020/21, the ombudsman upheld rate in customers' favour of 73% of customers' views in APP fraud cases. This rate has fallen to 50% in 2021/22.⁴ But the overturn rate remains high and too many victims of crime are waiting too long for their case to be settled and to be reimbursed.

4 Data published April 2023

Question 5

1.46 We asked respondents the following question:

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

Respondents' views

1.47 We received 45 responses to this question, with 34 stakeholders agreeing with our proposal and 11 disagreeing.

Applying the vulnerability definition

1.48 Most respondents argued that the definition should be applied where vulnerability affects the customer's susceptibility to falling victim to a specific APP fraud. One PSP highlighted the risk that if there was an exception for vulnerable customers then claims management companies may coach victims to falsely express vulnerability to 'game' the system.

Exempting vulnerable consumers

1.49 Most respondents – including PSPs, consumer groups and trade bodies – agreed with our proposal to reimburse vulnerable consumers even if they acted with gross negligence.

1.50 Respondents who disagreed with our proposal to require reimbursement of vulnerable consumers highlighted the risks of first-party fraud and moral hazard. Two trade bodies and a PSP noted how difficult it was to identify vulnerable customers. They said this raised the risk that consumers could falsely claim vulnerability to avoid being held to the gross negligence exception. Two other PSPs were concerned that the proposals would make it economically unsustainable to provide services to vulnerable customers and could lead to financial exclusion ('de-banking') of these customers.

Our view

1.51 As set out in the FCA guidance, *'consumers with some characteristics of vulnerability may be more likely to fall victim to scams'*.⁵ Some types of vulnerability can impair decision-making, putting people at greater risk from social engineering and less able to exercise caution to protect themselves from APP fraud. There is therefore a weaker case for applying exceptions designed to incentivise customer caution to these types of vulnerable customers. If a customer is deemed vulnerable for a specific APP fraud, the sending PSP must not apply the customer standard of caution (gross negligence). Gross negligence is a high bar, which we believe would only be applied in a small number of cases and therefore the exception for vulnerable customers would only impact a limited number of cases.

1.52 We acknowledge the range of policy risks highlighted by respondents. We have addressed the risks thematically in the policy statement, including our mitigating actions (see Chapter 4, Table 4).

⁵ FCA, [FG21/1 Guidance for firms on the fair treatment of vulnerable customers](#) (February 2021)

Question 6

1.53 We asked respondents the following question:

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

Respondents' views

1.54 We received 44 responses to this question, with 28 stakeholders agreeing with our proposal and 16 disagreeing.

Agreed with the use of the FCA's definition

1.55 Industry and consumer groups agreed that using the FCA's definition of a vulnerable customer would help ensure such customers were treated consistently across the UK's financial services sector. One firm stated that the definition is already recognised across the industry. Another stakeholder said the FCA definition appears to be working in relation to other types of fraud experienced by customers.

1.56 One PSP supported our proposal but argued that the FCA's definition did not provide a blanket exception to all customers with vulnerable characteristics, noting that firms are expected to assess, on a case-by-case basis, how far their vulnerability was relevant to an incident.

Disagreed with the use of the FCA's definition

1.57 The majority of the respondents who disagreed with our approach proposed that the definition should align with the one used under the CRM Code. PSPs argued the FCA definition lacks specificity, but the CRM definition allows firms to define vulnerability in the particular context of the APP fraud case and gives them more flexibility to identify vulnerable consumers.

Our view

1.58 Aligning our rules with the FCA's approach to vulnerability outlined in its guidance will help ensure consistent outcomes for customers. The fair treatment of vulnerable customers aligns with our strategic objectives of sufficiently protecting payment system users, as well as wider regulatory efforts to ensure firms are acting in the best interests of their customers, such as through the FCA's Consumer Duty.

1.59 While we recognise the arguments put forth by the respondents regarding using the CRM Code's definition, it is appropriate to align the approach to customers in vulnerable circumstances across all aspects of the financial services they use. Having PSPs operationalise a single approach will help ensure consistency of outcomes and help embed the right cultural shift within and across firms.

- 1.60** Our view is that the FCA’s approach to the fair treatment of vulnerable customers does not automatically mean that all customers with characteristics of vulnerability will be exempted from the customer standard of caution and claim excess. PSPs should evaluate each customer’s individual circumstances on a case-by-case basis to help them determine the extent to which their characteristics of vulnerability, whether temporary or enduring, led to them being defrauded, and therefore whether they meet the FCA’s definition. This is not a blanket exception for all customers who exhibit any characteristics of vulnerability.
- 1.61** Firms should take steps to encourage disclosure of vulnerable circumstances so they can best understand how to support customers and prevent harm associated with APP fraud. Staff and systems used to support victims of fraud need to ensure an appropriate level of detail is captured during assessment and reporting processes to ascertain the circumstances of the incident and the individual. This will help ensure appropriate aftercare can be provided, both to prevent fraud re-victimisation, as well as any wider support they may need when accessing products and services from the firm. Insight gained from analysis of the experiences and outcomes of vulnerable fraud victims can help ensure the needs of these customers are being met.
- 1.62** PSPs are expected to comply with the FCA’s guidance on vulnerability and be mindful of their obligations under the Consumer Duty (see policy statement, Chapter 3).

Question 7

- 1.63** We asked respondents the following questions:

Do you have comments on our proposal that sending PSPs should be allowed to apply a modest fixed ‘excess’ to reimbursement?

Do you have comments on our proposal that any ‘excess’ should be set at no more than £35?

Do you have comments on our proposal that PSPs should be able to exempt vulnerable consumers from any ‘excess’ they apply?

Respondents’ views

- 1.64** There were 61 responses to these questions. Responses were polarised, with respondents either agreeing or disagreeing with any excess. Respondents who opposed the proposed £35 suggested alternatives.

Agreed with the principle of a claim excess

- 1.65** Many respondents agreed with the principle of an excess. An excess would match with some other reimbursement protections and could mitigate the risk that the new reimbursement requirement would make moral hazard more likely. Several PSPs and trade bodies called for a claim excess to be applied consistently and uniformly across the industry to avoid confusion for customers.

Disagreed with the principle of a claim excess

- 1.66** Consumer groups were unanimously opposed to any excess. They argued that fraud is often hard to avoid (for example, many people fall victim to social engineering) and that any excess would unfairly impact victims. One respondent highlighted that the CRM Code victims are reimbursed without an excess.

Setting a claim excess at £35

- 1.67** Respondents almost universally disagreed with setting a claim excess at £35, either calling for the amount to be increased, lowered or scrapped entirely.
- 1.68** Consumer organisations generally, repeating their disagreement with the principle of a claim excess, argued that £35 was too high and that lower-value fraud has a negative impact on victims.
- 1.69** Conversely, trade bodies and PSPs generally argued for a higher claim excess. They felt that £35 would do little to encourage consumers to act with greater caution. It was also argued that a £35 excess wouldn't be applied in most cases due to the administrative burden. Alternatives included percentages, such as 5% and 10%, and higher fixed amounts, including £50 and £100.

Exemption for vulnerable customers

- 1.70** Most who responded to the question about vulnerable customers agreed they should be exempt from any excess. A few respondents suggested that a requirement to treat them differently from other customers may make PSPs less willing to provide services to vulnerable customers.

Our view

- 1.71** We have assessed the competing arguments regarding levying an excess on reimbursement. In considering the policies as part of a balanced package, we have decided to remove the minimum value threshold for claims and introduce a claim excess.
- 1.72** A single claim excess is clearer to communicate to customers (therefore better at encouraging appropriate customer caution) and easier for PSPs to administer. Set at the appropriate level, a claim excess will manage the risk of moral hazard alongside the many actions PSPs can take to prevent APP fraud.
- 1.73** We acknowledge respondents' arguments that £35 is not a suitable level of excess to address the moral hazard risk that reimbursement will reduce customer caution (particularly in higher-value payments). We will consult on a number of possible options for the claim excess in Q3 2023.

Question 8

1.74 We asked respondents the following questions:

Do you have comments on our proposal that sending PSPs should be allowed to set a minimum claim threshold?

Do you have comments on our proposal that any threshold should be set at no more than £100?

Do you have comments on our proposal that PSPs should be able to exempt vulnerable consumers from any threshold they set?

Respondents' views

1.75 There were 61 responses to the question. As with the previous question, responses were split on whether a minimum threshold should be set, with reasons presented by respondents on both sides similar to those regarding the excess.

Agreed with a minimum claim threshold

1.76 A significant number of PSPs were in favour of a minimum claim threshold. Arguments included:

- It is more difficult for PSPs to identify whether lower value payments are fraudulent – for example, determining whether a payment is a genuine purchase or a lower-value purchase fraud.
- A minimum threshold would ensure that administrative costs for PSPs are proportionate. Lower-value APP fraud makes up a significant proportion of cases and would be burdensome to assess and reimburse.

1.77 Several respondents argued that any minimum threshold must be consistent across the industry to avoid confusing consumers and complicating the 50:50 allocation of reimbursement between PSPs. Some respondents said that different thresholds across the industry could lead fraudsters to migrate to particular PSPs.

1.78 As with the claim excess, there was a general consensus vulnerable customers should be exempt from any minimum threshold implemented. A minority dissented.

Disagreed with a minimum claim threshold

1.79 A mixture of respondent types, including the majority of consumer groups, were against any threshold. Arguments included:

- PSPs would not be incentivised from stopping fraud below any minimum threshold.
- A minimum threshold could disproportionately affect the lower-income victims who are most affected by lower-value APP fraud.
- It could lead to under-reporting of APP fraud below the minimum threshold.
- There is no threshold under the CRM Code.

Setting the minimum threshold at £100

- 1.80** Respondents who agreed with the principle of a minimum threshold had mixed views on setting it at £100:
- Some agreed with the proposed £100 limit, with two stakeholders calling for it to rise in line with inflation.
 - Most PSPs in favour of a threshold called it to be set at £250, questioning whether £100 was enough to ensure that customers exercise caution. Another industry group called for a limit between £500 and £1,000.
 - Another respondent called for PSPs to be able to set their own limits based on customer and/or payment types.

Our view

- 1.81** It is an important principle for PSPs to be able to consider the risk of fraud across all payments. On reflection, we acknowledge that a minimum threshold could reduce customer reporting, reduce incentives on PSPs to act on fraud beneath that threshold, and cause fraud to migrate below it.
- 1.82** There has been some confusion over how the excess and the minimum threshold would work in practice, with two differing figures likely to confuse customers and PSPs. We have therefore removed the separate minimum threshold for claims and will consult on the appropriate level for a claim excess.
- 1.83** We acknowledge that depending on how the excess is structured (for example, as a fixed £100), it could act a de facto minimum threshold for claims. The excess will be optional, and we will require sending PSPs to report all APP fraud claims (regardless of value) to receiving PSPs. In practice, customers will know that any APP fraud claim will at least be recorded, and the receiving PSP may be able to repatriate the stolen funds.
- 1.84** The claim excess will not apply to vulnerable customers (see policy statement, Chapter 2).

Question 9

- 1.85** We asked respondents the following question:

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

Respondents' views

- 1.86** There were 36 responses to this question. Responses were generally split between consumer groups and PSPs, who held opposing views on whether a maximum threshold would be beneficial.

Agreed with no maximum threshold

- 1.87** Consumer organisations were generally against a maximum threshold, arguing that it would give PSPs the incentive to do more checking for high-value payments and would give customers the confidence that reimbursement applies to all payments. Two PSPs were also in favour of not having a maximum threshold.

Disagreed with no maximum threshold

- 1.88** A number of PSPs, including many small firms, argued that if there was no maximum threshold it would impose an 'unlimited liability' on PSPs, with potential unintended consequences. For example, several smaller PSPs warned it would increase their capital requirements, leading them to limit their potential liability by more stringently limiting the value of payments customers could make. In turn, this would mean poorer outcomes for customers.
- 1.89** Some respondents argued that a maximum threshold would protect against any abuse of the policy and ensure customers exercised appropriate caution and due diligence with higher payments.
- 1.90** Several PSPs pointed out that other customer protections within the UK payment landscape had maximum levels of reimbursement.
- 1.91** PSPs and industry groups suggested a range of figures for a suitable maximum threshold. These included £30,000 (aligning with section 75 of the 1974 Consumer Credit Act), £85,000 (like the Financial Services Compensation Scheme), and £375,000 (the Financial Ombudsman Service maximum compensation limit prior to April 2023).

Our view

- 1.92** We have assessed the varying views including those in favour of our original proposals not to have a maximum threshold.
- 1.93** After reviewing the evidence provided, we have decided to introduce a maximum level of reimbursement (by value) for individual claims as part of the balanced package of policies. This is primarily to bring the new reimbursement in line with other customer protections in the payment landscape. We also acknowledge the wider benefits, including greater clarity on the potential prudential liability for PSPs.
- 1.94** The maximum level of reimbursement will be subject to consultation in Q3 2023.
- 1.95** We have considered the potential prudential risk from introducing the new reimbursement requirement as part of our updated cost benefit analysis (see the separate Annex 4).

Question 10

- 1.96** We asked respondents the following questions:

Do you have comments on our proposal that sending PSPs should be allowed to set a time limit for claims for mandatory reimbursement?

Do you have comments on our proposal that any time limit should be set at no less than 13 months?

Respondents' views

- 1.97** There were 45 responses to this question. The vast majority of respondents agreed that a time limit for claims should be set, and they generally accepted 13 months as suitable.

Setting a time limit for claims

- 1.98** Several PSPs said a time limit was important to ensure that there would be no open-ended liability on PSPs. One consumer group added that any time limit should be reasonable and fair to customers.
- 1.99** Several respondents commented on when the time count should begin on a claim. One industry body said we should consider counting from when the customer might reasonably have realised they have fallen victim to APP fraud, rather than the first payment. PSPs and trade bodies were agreed that we should be clear when the time count begins so that all PSPs treat customers the same, ensuring clarity and consistency for customers.

13 months

- 1.100** The majority of respondents agreed with a 13-month time limit, arguing that it was sensible to follow the limits set by other protocols (for example, unauthorised fraud and direct debit).
- 1.101** Some consumer organisations argued that the time limit should be longer than 13 months. Two organisations pointed out that victims may not be aware until much later that they have fallen victim of fraud, especially in cases of romance or investment fraud. Proposals for a longer time limit included the ombudsman's limit of six years⁶, five years, and two years.
- 1.102** PSPs generally favoured a time limit of 13 months or less. It was argued that APP fraud is reported in a much shorter timeframe (for example, within three months). Two PSPs suggested six months as a suitable limit.

Our view

- 1.103** A time limit is important to ensure PSPs do not have open-ended liability but must give customers sufficient time to make a claim.
- 1.104** We have concluded that 13 months is a suitable limit for claims. This is the same as the time limit for claims for refunds of unauthorised payments under the Payment Services Regulations 2017. Sending PSPs are under no obligation to limit claims to 13 months and can voluntarily provide reimbursement on any claim.
- 1.105** An individual could claim for payments made over a longer period as part of an APP fraud as long as they submitted the claim within 13 months of the final payment. The exception to this rule will be when the new reimbursement requirement first becomes effective – the new requirement will only apply to Faster Payments made after day 1.

⁶ Customers may have the opportunity to pursue a claim via the Financial Ombudsman Service up to six years from a problem happening, or longer, if still within three years of the customer becoming aware (or of when the customer should reasonably have become aware) of the problem.

- 1.106** If the sending PSP decides to refuse a claim due to the 13-month time limit under the new reimbursement requirement, customers may have the opportunity to pursue a claim via the Financial Ombudsman Service up to six years from a problem happening, or longer, if still within three years of the customer becoming aware (or of when the customer should reasonably have become aware) of the problem. This is the same process as all other complaints between customers and businesses that provide financial services. The 13-month time limit for APP fraud claims under the new reimbursement requirement does not impact the ombudsman's scope or processes.

Question 11

- 1.107** We asked respondents the following questions:

Do you have comments on our proposal that the sending PSP is responsible for reimbursing the consumer?

Do you have comments on our proposal that reimbursement should be as soon 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?

Respondents' views

- 1.108** There were 40 responses to this question. The vast majority of respondents agreed that the sending PSP should be responsible for reimbursement. However, most respondents were opposed to the 48 hour time limit to reimburse customers.

Sending PSP responsible for reimbursing the customer

- 1.109** Only one respondent, a PSP, was against making the sending PSP responsible for reimbursing their customer.

48-hour time limit to reimburse the customer

- 1.110** The majority of respondents said 48 hours gave too little time to reimburse the customer. Arguments included:
- 48 hours would not always be enough time to complete an accurate assessment and would place undue burden on staff to assess claims at speed. Several PSPs suggested that first-party fraud could increase as a result. Noting that claims to the ombudsman takes several months, one consumer organisation said that customers would benefit if PSPs had longer time to make better decisions.
 - A number of smaller banks and building societies pointed to the operational difficulties of reimbursing customers within this timeframe. Many PSPs are not open seven days a week, or 24 hours a day, making it difficult to fulfil the 48-hour requirement consistently.
- 1.111** Alternative time limits to reimburse customers included 15 days (as mandated by the CRM Code), 5 days or 7 days. One large PSP suggested an annual review of timescales.
- 1.112** Consumer organisations generally (but not unanimously) supported a 48 hour time limit to reimburse victims, saying this would ensure they suffer as little detriment as possible. One consumer organisation was concerned that 48 hours would not be adequate time for PSPs to reach the right outcome for victims.

Our view

- 1.113** We will require sending PSPs to assess claims and reimburse the customer. The fraudulent payment has been made using their systems and they are best placed to assess the information their customer provides.
- 1.114** We will extend the time limit for reimbursing customers to five business days. On assessing the evidence provided, we acknowledge that the proposed 48-hour time limit to reimburse victims would be too operationally challenging for many PSPs. This is especially so for smaller banks and building societies that do not have 24/7 operations. This will also mitigate the risk of PSPs making poor or automated decisions to achieve the time limit. As the median ombudsman case takes approximately six months to conclude, and generally longer for fraud cases, we want PSPs to make good decisions in the first place. PSPs will therefore also have the option to 'stop the clock' for specific actions. The policy statement sets out further details (see Chapter 5, Box 5).

Question 12

- 1.115** We asked respondents the following questions:

What standard of evidence for gross negligence or first-party fraud would be sufficient to enable a PSP to take more time to investigate?

How long should the PSP have to investigate in those circumstances?

Respondents' views

- 1.116** There were 29 responses to this question. There were a mixed responses on how high the standard of evidence should be, and many PSPs called for alignment with the CRM Code on the length of time to investigate.

Standard of evidence

- 1.117** Consumer groups were in favour of a high standard of evidence to determine gross negligence. Respondents argued that PSPs should not take undue time investigating a victim's claim, and that the burden of proof should be on PSPs to establish gross negligence, rather than the customers proving they have taken appropriate caution. Another organisation said that the use of warnings, or Confirmation of Payee (CoP), represents too low a standard of evidence for gross negligence suggesting that the assessment should instead consider the victim's reasonable basis for belief.
- 1.118** A number of PSPs suggested that a lower standard of evidence for gross negligence should be used to investigate claims further, or suggested examples of where gross negligence should be applicable. Suggestions of sufficient evidence included ignoring warnings during a payment journey (including CoP mismatches and targeted warnings), PSPs having a reasonable belief that fraud has taken place, and misstatements during customer due diligence. One PSP disagreed with the fact that current provisions in the CRM Code for customer standards of care, such as ignoring effective warnings and CoP, are not considered gross negligence under the Code and are not currently considered a high enough standard of evidence.

Time to investigate

- 1.119** Many respondents agreed that the time the PSP should take to investigate should align with the CRM Code (15 days). Some respondents, including many PSPs and one trade body, called for a longer limit of 30 to 35 days, as investigations may be more complex or require engagement with a number of institutions. One respondent suggested three months for first-party fraud, and 21 days to investigate gross negligence. A further respondent suggested alignment with card transaction dispute limits of 120 days.

Our view

- 1.120** Sending PSPs must reimburse customers within five business days. In certain circumstances, PSPs will have the option to ‘stop the clock’ on any reimbursement so they can gather information. Under this mechanism, the five business days will pause while the PSP gathers the information, with the time resuming once this has been completed. The policy statement sets out further details (see Chapter 5, Box 5).
- 1.121** We agree that, where suspected, the burden of proof is on the PSP to prove gross negligence. This aligns with the treatment of customers involved in unauthorised payment transactions as set out in the FCA’s approach to payment services and electronic money.⁷
- 1.122** Information should be gathered as soon as possible after an incident. PSPs will need to engage with their customers as the first touchpoint, because they are likely to have the most meaningful evidence. PSPs should capture the chronology, what the customer saw, did and thought, and whether they were coached through stages of the payment journey. PSPs should strive to have open-ended reporting processes which give staff the flexibility to ask the questions they feel are important to capturing the right details. Digital reporting systems could provide free-text options rather than just prescriptive prompts.
- 1.123** Firms must be responsive to customers’ needs and understand that fraud incidents will impact people in different ways, possibly affecting how they engage with their PSP. Where possible, firms should use a ‘tell us once’ approach so customers do not have to go over their story repeatedly with different staff.

Question 13

- 1.124** We asked respondents the following question:

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

Respondents’ views

- 1.125** We received 53 responses to this question. Most respondents agreed with the principle of sharing reimbursement costs between sending and receiving PSPs, but some raised concerns over how it would apply in practice and whether a more refined allocation of costs would be a better approach.

⁷ FCA, [Payment Services and Electronic Money – Our Approach](#) (November 2021)

- 1.126** A few consumer groups responded to the question. They were supportive in principle so long as the policy promoted fair outcomes for consumers.

Applying the 50:50 default allocation in practice

- 1.127** Several PSPs and trade bodies requested further information on the mechanics of the policy including how (and when) the sending PSP would be reimbursed by the receiving PSP. They asked for guidance including timelines on reimbursement from the receiving PSP to the sending PSP and clarity on whether reimbursement would be accrued and settled over a fixed time period.
- 1.128** Some firms asked for further information on how a 50:50 split would work with the optional excess. For example, would a receiving PSP have to reimburse a sending PSP for 50% of the total APP fraud claim amount or could they reduce this by 50% of the excess.

Alternative options to the 50:50 default allocation

- 1.129** Some respondents disagreed with the proposed 50:50 default allocation and suggested alternative options:
- Several PSPs advocated a risk-based allocation between PSPs, to reward strong fraud prevention. Some recognised that this would take time to implement as data would have to be gathered, possibly including the data from the PSR's Measure 1 initiative (see the policy statement, Chapter 3).
 - A few respondents suggested different fixed options such as assigning fixed reimbursement percentages at different levels, or all costs of reimbursement to a single party who was demonstrably at fault, or full liability by default to either sending or receiving PSP.
- 1.130** Some respondents included views on allocating part of the reimbursement costs to PISPs or to parties in other sectors, such as social media firms. We have considered these arguments as part of our response to Question 17.

Our view

- 1.131** The 50:50 split of the cost of reimbursement between sending and receiving PSPs is not an attempt at a fine-tuned allocation. It is intended to provide for adequate incentives on both sending and receiving PSPs as part of our balanced package of policies to quickly increase protection for customers and meet legislative deadlines.
- 1.132** There could be additional benefits with a more refined cost allocation model which recognises the relative efforts of PSPs in preventing APP fraud to determine the allocation of reimbursement costs. Currently, insufficient data is available to support a more refined reimbursement cost allocation model; however, Pay.UK will lead work to consider how a more refined reimbursement cost allocation model could be developed.
- 1.133** We have considered the other alternatives presented by respondents. However, it would be challenging to determine different reimbursement percentages for sending and receiving PSPs (for example, 70% for the receiving PSP). Different percentages would also give PSPs different incentives to tackle fraud. We have considered assigning allocation to one party, but the CRM Code has shown that this also creates inconsistent incentives across the industry.

1.134 If the sending PSP voluntarily provides reimbursement outside of the new reimbursement requirement, then they can only require 50% of the in-scope reimbursement paid to the customer. Further details are provided in the policy statement (see Chapter 5).

1.135 Pay.UK will be responsible for defining the operational guidance and processes for the reimbursement process between sending and receiving PSPs. We expect Pay.UK to set a reasonable time period for this reimbursement. An ultimate backstop period will apply to prevent receiving PSPs avoiding their obligation to reimburse sending PSPs.

Questions 14 and 21

1.136 We asked respondents the following questions:

Do you have views on our proposal that PSPs are able to 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?

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

Respondents' views

1.137 This section summarises the responses to Questions 14 and 21 because they overlapped. We received 41 responses to these questions.

Agreed with the option to depart from 50:50

1.138 Most respondents, both PSPs and consumer groups, agreed with the principle of PSPs being able to depart from the 50:50 allocation, but many raised concerns that this could add complexity, while negotiation and mediation would make the process longer.

1.139 Some PSPs agreed with the principle of giving PSPs freedom to depart from the 50:50 default allocation. But they said the practicalities of implementing such a system meant it should be a medium-term rather than short-term aim.

Disagreed with the option to depart from 50:50

1.140 A few, particularly smaller firms, disagreed with PSPs being able to depart from the 50:50 default allocation. Arguments included:

- Smaller PSPs would not have the capability to deal with the potential number of cases that might be disputed.
- Any negotiation, mediation or dispute resolution would likely benefit larger PSPs.
- It would be difficult to implement this proposal without delaying the introduction of the new reimbursement requirement.

1.141 A few consumer groups also raised concerns with the proposal for PSPs to depart from the 50:50 default allocation:

- Customers might face delay receiving their reimbursement while PSPs negotiated their split of liability.

- PSPs should focus on reducing fraud activity to protect customers, rather than putting resources into minimising and negotiating liability.

1.142 Some respondents also observed that the CRM Code's existing mechanism for this has not been used. They cited the complexities and costs of adopting the current dispute provisions under the Code.

Additional complexity

1.143 Several firms and trade bodies stated that to ensure consistency and fairness, any deviation from the 50:50 split would require clear guidance on when this can happen. Some firms suggested that Pay.UK should develop and set out the terms for any arbitration and negotiation, including minimum reimbursement amounts and set criteria for determining liability.

Our view

1.144 We will not introduce a process on day 1 for PSPs to be able to depart from the 50:50 default allocation, recognising stakeholder views that it could increase bureaucracy, operational costs, complexity and time to reimburse customers, and might also favour larger PSPs. If additional processes were introduced before anyone knew how the new reimbursement requirement worked in practice, it could complicate and distract from initial implementation.

1.145 As set out in Question 13, Pay.UK will lead work to consider how a more refined reimbursement cost allocation model could be developed in future.

1.146 If disputes arise from the new reimbursement requirement, PSPs are best placed to determine the best way to resolve these. For example, agreeing to use independent external arbitration or other existing mechanisms. This policy does not prevent Pay.UK from introducing any additional dispute resolution processes if they judge this to be appropriate as the PSO.

1.147 We will consider whether any further action is needed as part of the post-implementation review.

Question 15

1.148 We asked respondents the following question:

Do you have views on how scheme rules could implement our proposed 50:50 default allocation to multi-generational⁸ scams?

Respondents' views

1.149 We received 33 responses to this question. Most respondents disagreed with the principle of multiple generations of payments being within the scope of the new reimbursement requirement. They argued that only the final payment from the PSP to the criminal's account should be considered.

⁸ For clarity, we now refer to multi-generational scams as multi-step APP fraud (see policy statement, Chapter 2).

Multiple generations of payments should be out of scope

- 1.150** Several PSPs stated that managing fraud across multiple generations of payments would place a significant operational and financial burden on PSPs. Respondents argued that it would be nearly impossible to distinguish genuine payments between a customer's own accounts at two PSPs (for example, from a savings account to a current account) and transfers of funds into fraudsters' hands many transactions later. Extending liability to earlier stages in a multi-step APP fraud case would result in the regular blocking or delay of legitimate payments and transactions, to customers' detriment.
- 1.151** Some trade bodies and firms stated that the current legislative framework does not allow for the level of data sharing between PSPs that would be needed to identify the earlier transactions in multi-generational fraud cases.

Multiple generations of payments should be in scope

- 1.152** A few firms and consumer groups suggested that multiple generations of payments should be within the scope of the new reimbursement requirement. They argued that more organisations, such as crypto exchanges, should be brought within its scope. A few firms also suggested that focus should broaden on the wider fraud landscape and social media firms should share some of the liability for APP fraud.

Our view

- 1.153** We have concluded that the new reimbursement requirement should apply to a payment to an account controlled by a person other than the customer, where the customer has been deceived into granting that authorisation for the payment as part of an APP fraud. This will give PSPs a significant incentive to prevent transactions to accounts controlled or owned by fraudsters, while reducing the impact on genuine non-fraudulent transactions.
- 1.154** We acknowledge that expanding the scope of the policy to include earlier transactions (for example, between an individual's savings and current accounts) would be impractical for PSPs. We want to focus PSPs' efforts on preventing funds from leaving the control of the victim as part of an APP fraud.

Question 16

We asked respondents the following question:

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

Respondents' views

- 1.155** We received 31 responses to this question. Most respondents agreed with the principle of sharing repatriation funds between sending and receiving PSPs, as long as this 50:50 split aligned with the original split of reimbursement costs. If the split of liability changes, they argued, the repatriation funds split should also change.

- 1.156** A few firms disagreed with the proposed approach and suggested alternative options. One proposal was that the PSP responsible for securing the repatriation should be entitled to a greater proportion, but not above their reimbursement costs. One firm suggested that receiving PSPs are usually less at fault and should keep a greater percentage in the case of repatriated funds.
- 1.157** Several firms and trade bodies called for this process to be standardised across the industry, including with expected timeframes for funds to be split between the sending and receiving PSPs after repatriation.

Our view

- 1.158** We agree with the principle of sharing repatriated funds following the cost of the reimbursement. We have reviewed the alternative options presented (including first fully reimbursing the receiving PSP to encourage repatriation efforts). But we conclude that following the cost of reimbursement is the fairest and simplest solution.
- 1.159** Any repatriated funds remaining after the PSPs have fully covered their reimbursement costs must go to the victim. For example, if 100% of funds are recovered, the victim should be reimbursed their claim excess by the sending PSP. There should not be any cases where victims receive more than 100% of their original claim.

Question 17

- 1.160** We asked respondents the following question:

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

Respondents' views

- 1.161** We received 31 responses to this question, with the majority coming from industry stakeholders. Most agreed with our proposals in principle and thought that the cost of reimbursement should be allocated to all direct and indirect Faster Payments participants. Respondents argued this would help to ensure a consistent approach across the industry.
- 1.162** A minority of respondents from the industry pointed out that a 50:50 cost reimbursement model between sending and receiving PSPs would provide no incentives for other firms within the payment chain (like PISPs, EMIs and payment institutions, as well as unregulated firms like crypto exchanges). They recommended we broaden our proposals to include these types of firms.

Our view

- 1.163** All PSPs should have incentives to detect and prevent APP fraud. We have seen a trend of fraudsters migrating to receiving PSPs that do not participate in existing safeguards including the CRM Code and CoP (introduced under our Specific Direction 10, hereafter 'SD10'). For example, non-SD10 PSPs accounted for 20% of Faster Payments transactions in 2021 but received 50% of APP fraud payments sent from SD10 PSPs.⁹

⁹ Based on quarterly CoP data received from SD10 PSPs and industry Faster Payments data from Pay.UK in 2021, covering 2021 and the first quarter of 2022.

- 1.164** We have considered the proposal that firms elsewhere in the payment chain should be included in the allocation of costs. But this would be operationally complex and there is insufficient data to decide how to allocate costs. PSPs that operate the sending or receiving payment account for a transaction have access to the data relevant for informed decisions. As set out in Question 3, we have decided to include PIS transactions and apply the same obligations as other Faster Payments (see policy statement, Annex 2 for further details).

Questions 18, 19 and 20

- 1.165** We asked respondents the following questions:

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

Do you have comments on the minimum initial set of Faster Payments scheme rules needed to implement our mandatory reimbursement proposals?

Do you have any views on how we should exercise our powers under Financial Services (Banking Reform) Act 2013 (FSBRA) to implement our requirements?

Respondents' views

- 1.166** This section summarises the answers to Questions 18, 19 and 20, as most respondents combined their answers to all three under Question 18.
- 1.167** We had 43 responses to these questions. Most agreed with at least the key aspects of our long-term vision, with many saying that Pay.UK, the payment system operator (PSO), should be the rule-setter responsible for mitigating fraud. Arguments included:
- Scheme rules are more flexible compared to regulation.
 - The PSO can feed insight into continuous development of the rules.
 - APP fraud could be a significant driver of payment system changes that the PSO should respond to.
- 1.168** A minority of respondents disagreed with our long-term vision. Several responses across firms, trade bodies and consumer groups stated that the PSR was the more appropriate entity for rule setting and enforcement. Some respondents also said the liability framework for reimbursement should be set in legislation in the longer term, like the arrangements for unauthorised fraud. In the meantime, they proposed we should impose the requirements through regulatory directions.
- 1.169** Almost all respondents (including those that agreed with our long-term vision) said that Pay.UK currently lacks the capacity to take on the role we outlined. They pointed especially to its current lack of enforcing powers, and the fact that the rules do not cover indirect PSPs. There were mixed views on how far change might be possible.

Our view

- 1.170** Our view is the PSO is the appropriate body, in the long term, to make, maintain, refine, monitor and enforce compliance with comprehensive scheme rules that address fraud risks in the system. This is consistent with our strategic priority to act to ensure the

interbank systems provide the infrastructure, rules and incentives that foster innovation and competition in payments. Compared to legislation, Faster Payments rules are more adaptable to the quickly evolving threat from APP (and other) fraud.

- 1.171** However, this represents a change to Pay.UK's role in Faster Payments and there are currently factors limiting Pay.UK's ability to fully take on this role. In particular, Pay.UK's scheme rules only apply to direct participants, and Pay.UK has limited tools to enforce compliance with its rules. Although Pay.UK is already doing work to consider how it can change these constraints as it progresses delivery of the NPA, relying exclusively on scheme rules at this stage poses risks to timely and effective implementation.
- 1.172** We are therefore introducing some safeguards into the day-one arrangements to mitigate those risks. We will overlay the scheme rule requirements with a general direction requiring all Faster Payments participants to comply with those rules. This will bring all Faster Payments participants into the scope of the requirements and will give PSR a role in enforcement to support Pay.UK. We will retain responsibility for some of the key requirements, including the underlying requirement to reimburse victims of APP fraud. We will look to hand over responsibility for some of these requirements to Pay.UK in the future as it develops the capabilities required to achieve our long-term vision. Before doing so, we will review and consult on any subsequent changes to Pay.UK's role and implement these changes through appropriate legal instruments.
- 1.173** The minimum initial set of Faster Payments scheme rules strikes a balance between clarity for both PSPs and their customers and efficient implementation within Pay.UK's capacity. Pay.UK's enforcement structure already includes referral to us where there is a lack of compliance; we do not envisage this changing. The PSO's relative flexibility to update the rules in response to new challenges, coupled with a regulatory backstop in cases of non-compliance, will mean it can effectively oversee the rules for mitigating fraud. We recognise that this would only be a starting point and the rules would evolve over time to remain relevant in the ever-changing landscape of fraud.
- 1.174** We have considered the respondents' concerns over the potential for misinterpreting the customer standard of caution. We will set this standard to ensure clarity and consistency of application.

Question 22

- 1.175** We asked respondents the following question:

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?

Respondents' views

- 1.176** We had 49 responses to this question. Of those, the majority agreed a compliance monitoring regime was crucial.
- 1.177** There were concerns around Pay.UK's capacity to take on the role, but also agreement that it should do so in order for the regime to start immediately. Several respondents, while agreeing, wanted to ensure that the reporting requirement was not overly burdensome and said that ideally it should be automated.

- 1.178** Several respondents disagreed with Pay.UK taking on a monitoring role. They noted that the PSO's role is not quasi-regulatory and that the Financial Conduct Authority (FCA) currently collects fraud data. They expressed a preference for normal supervision of compliance by the FCA, with the Financial Ombudsman Service arbitrating in disputes.
- 1.179** Many respondents, both for and against the proposal, saw the UK Finance Best Practice Standards as a good long-term solution for implementation. However, they also noted that the standards would need to be developed further to meet the monitoring requirements.

Our view

- 1.180** Pay.UK will create and implement a compliance monitoring regime for all requirements across all in-scope PSPs (including indirect participants). This approach acknowledges that Pay.UK is best positioned to assess the most effective and efficient monitoring mechanism (in conjunction with industry). The general direction we give will require all in-scope PSPs to provide data to Pay.UK. The high-level areas we expect Pay.UK to gather and analyse data on are:

- number of APP fraud claims reported by customers
- number of APP fraud claims rejected by PSPs (and reasons)
- time taken to reimburse APP fraud victims
- use of exceptions by PSPs
- reimbursement rate of customers by sending PSPs
- reimbursement rate of sending PSPs by receiving PSPs
- time taken for receiving PSPs to reimburse sending PSPs
- rate of repatriation of stolen APP fraud funds

- 1.181** We are also working with Pay.UK to agree a high-level approach and principles for how it will monitor compliance.

- 1.182** We have considered the concerns around Pay.UK's capacity. To provide support, our section 54 direction will direct PSPs within the scope of the policy to report data to Pay.UK. This will ensure the compliance monitoring regime operates in the short term. At the same time, Pay.UK can consider, alongside industry, the best long-term model for compliance monitoring.

Question 23

- 1.183** We asked respondents the following question:

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

Respondents' views

- 1.184** We received 24 responses to this question. An important theme across respondents was that the cost and operational impact to PSPs would need to be further considered.

- 1.185** Most responses agreed that a real-time compliance monitoring system would be an effective and beneficial tool. Some respondents suggested that the tool could be built on further for risk identification and mitigation.
- 1.186** Several dissenting respondents suggested there was no need for a real-time compliance monitoring system and its costs would outweigh its benefits. The main reason for this was that there did not seem to be a requirement for real-time monitoring based on the nature of fraud – with firms already uploading case information within a couple of hours of case reporting, and more complex cases taking a long time to resolve. Therefore, periodic reporting seemed more appropriate. Other dissenting responses said that we should cooperate with the FCA, which already collects fraud data.

Our view

- 1.187** As the PSO, Pay.UK is best placed to work with industry and create a suitable compliance monitoring system that strikes a balance between efficacy and operational burden. Given our decision to require Pay.UK to create and implement the regime, we do not feel it appropriate for us to mandate any particular method of monitoring.

Question 24

- 1.188** We asked respondents the following question:

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

Respondents' views

- 1.189** We received 16 responses to this question. Most responses disagreed with Pay.UK being responsible for enforcement of the reimbursement requirements. Arguments included:
- Pay.UK currently has limited enforcement powers for direct participants and no enforcement powers for indirect participants.
 - Enforcement is the role of the regulator, not of the PSO.
 - Pay.UK currently lacks capacity to take on this role, especially where non-compliance is as a result of the complexity of cases.
- 1.190** There were further concerns around the different routes to enforcement between direct and indirect participants.

Our view

- 1.191** We recognise some of the constraints on Pay.UK's current ability to enforce compliance across all participants. The general direction on Faster Payments participants will give us an enforcement role to support Pay.UK.
- 1.192** We are responsible for enforcing the general direction on Faster Payments participants and the specific direction and section 55 rule change requirement placed on Pay.UK. We will use enforcement powers we judge to be appropriate, using our assessment of Pay.UK's performance in implementing and monitoring the reimbursement requirements and PSPs' performance in complying with the requirements.

- 1.193** Pay.UK will follow its enforcement procedures for direct Faster Payments participants. This process includes referring to the PSR if PSPs do not take corrective steps following Pay.UK's initial steps. Examples of where we would expect Pay.UK to refer a case to us include:
- **Consistent failure by a PSP to abide by the new reimbursement requirement and underlying policies.** For example, where a PSP has failed over a sustained period to improve timeliness of reimbursement.
 - **An extreme compliance failure by a PSP to abide by the new reimbursement requirement.** For example, where a PSP refuses to implement the new reimbursement requirement.
- 1.194** For any cases referred to the PSR, we use our enforcement powers as we judge appropriate, taking account of our administrative priority framework.¹⁰
- 1.195** Only direct Faster Payments participants are subject to Pay.UK rules and enforcement. We will be responsible for enforcing compliance of in-scope indirect Faster Payments participants.

Question 25

- 1.196** We asked respondents the following question:

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

Respondents' views

- 1.197** There were 33 responses to this question. There were a mixture of responses and preferred options, but the majority of respondents called for the PSR to give a direction to indirect PSPs to comply with the reimbursement rules in Faster Payments.

Giving a direction to indirect participants

- 1.198** Calls for us to give a direction came largely from PSPs. Respondents argued that it is the best way to ensure that the cost of reimbursement liability lies with the indirect PSP. They also argued that a direction would ensure a consistent approach across all PSPs within the scope of the policy.

Applying the rules on reimbursement via IAPs

- 1.199** PSPs who act as Indirect Access Providers (IAPs) raised the issue of risk. One IAP cited how many PSPs it has as customers and suggested that to mitigate any new liability, it would have to reconsider the terms and conditions for sponsoring any new PSPs. Another large PSP argued that these proposals could present an undefined credit and operational risk if they required IAPs to refund payments on behalf of indirect PSPs or bear any cost, risk or administrative burden on their behalf.

¹⁰ PSR, [Administrative Priority Framework](#) (March 2015).

Extending Faster Payments rules to indirect participants

1.200 A small number of respondents suggested that applying the rules on reimbursement to indirect participants through the Faster Payments rules would be the simplest solution. The issue of Pay.UK amending scheme rules to extend to indirect participants was raised. One respondent argued that amending any rules could take time, potentially impacting the delivery of reimbursement requirements in the short term.

Our view

1.201 We believe that it is fair that only the PSPs involved in an APP fraud should be responsible for reimbursement, rather than their access provider.

1.202 We will direct Pay.UK to put the new reimbursement requirement into Faster Payments rules, using our powers under section 55 of the FSBRA. This will be supported by a general direction under section 54 on all in-scope PSPs, which will place a regulatory obligation on these firms to comply with the relevant Faster Payments rules.

1.203 The direction will apply the requirements to both direct and indirect participants, whilst maintaining responsibility with Pay.UK. We believe that ensuring consistency across the industry by directing all participants in scope, including indirect PSPs, is key, and will put the onus on PSPs to improve fraud prevention.

Question 26

1.204 We asked respondents the following question:

If it was necessary for us to give a direction, what are your views on whether we should direct indirect PSPs or Indirect Access Providers (IAPs)?

Respondents' views

1.205 There were 29 responses to this question. The vast majority of respondents (including larger PSPs) called for us to give direction to indirect PSPs rather than IAPs. Arguments included:

- It would align with the approach used for Confirmation of Payee.
- It would ensure consistency across the reimbursement scheme.
- IAPs do not have a relationship with fraud victims.
- Giving a direction to IAPs would adversely affect their risk appetite and have a negative impact on smaller PSPs' ability to access Faster Payments.

1.206 Only one respondent, a small PSP, suggested that IAPs should be directed, arguing that it was the only realistic way to reach the significant number of PSPs involved.

Our view

1.207 We agree that there could be negative impacts on the indirect access market if IAPs were held accountable for the liability of their indirect PSPs. In addition, we want to see consistent action among PSPs in combatting fraud and producing timely reimbursement.

- 1.208** Our general direction will place the obligation to reimburse directly on indirect Faster Payments scheme participants within the scope of the policy. This mitigates the risk that if IAPs were made responsible for indirect PSP reimbursement they would restrict access for indirect Faster Payments scheme participants.

Question 27

- 1.209** We asked respondents the following question:

Do you have comments on our cost benefit analysis at Annex 2 or any additional evidence relevant to the analysis?

Respondents' views

- 1.210** We received 45 responses that expressed a view on the cost benefit analysis. Of these, eight agreed with our approach and assessment of the relevant costs and benefits; 31 thought the costs were understated; 5 questioned the scale of the expected benefits; and 6 expressed concerns with the approach used in the analysis. Among respondents who argued that our assessment had understated the costs, six main issues were raised:

- the risk of increased friction in the payment system
- a reduction in competition and innovation
- increased administrative costs for PSPs
- the risk of vulnerable customers being 'de-banked'
- cost increases on PSPs being passed on to all customers
- increased risk of first-party fraud

Our view

- 1.211** We have addressed these views in our updated cost benefit analysis. See the separate Annex 4.

Question 28

- 1.212** We asked respondents the following question:

Do you have any other comments on the proposals in this consultation?

Respondents' views

- 1.213** We received 14 responses to this question, mostly from industry participants. The majority related to one or more of the proposals mentioned in the consultation or reiterated views related to other questions in the consultation. However, three main topics were recurrent:

- **Increasing intelligence sharing:** Several comments from PSPs referred to work around our Measure 2, noting that intelligence and data sharing among industry participants must increase to enable the reimbursement policy. Respondents highlighted problems of communication between institutions (with smaller PSPs

reporting they had historically been left out of some industry initiatives). Concerns were expressed that our reimbursement proposals would adversely affect the industry's capacity to deliver increased intelligence sharing.

- **The wider fraud ecosystem:** Some PSPs called for more work to be done on the role of big tech, social media and telecoms in facilitating fraudulent activity. However, they recognised the limits on our jurisdiction in this area.
- **Delay of payments:** Some respondents from the industry would welcome changes to allow PSPs to further delay certain high-risk payments.

1.214 Additional comments included:

- Some respondents welcomed our proposed post-implementation review to consider the success of the proposals.
- One respondent noted that fraudsters sometime pose as legitimate traders, and then fail to deliver a service, blurring the line between fraud and civil disputes.
- One consumer organisation encouraged greater customer education especially for certain groups more susceptible to falling victim to fraud.
- A few respondents from the industry called for a more detailed analysis to ensure that any significant costs to industry or customers are recognised and assessed relative to the benefits of reimbursement.
- One respondent argued that our proposals did not adequately reflect the views of all participants and that there is insufficient evidence and data to support the changes we propose.

Our view

1.215 On the three recurrent topics, we generally agree with the points raised by stakeholders, noting:

- **Increasing intelligence sharing:** This remains a priority for us, and we are working closely with industry to consider payments risks and improve fraud prevention (see policy statement, Chapter 3).
- **The wider fraud ecosystem:** We are not acting alone in fighting APP fraud. PSPs play a pivotal role in designing fraud out of the system, but there is also a critical role for the wider fraud ecosystem (see policy statement, Chapter 3).
- **Delaying payments to prevent fraud:** Where high levels of risk are identified, PSPs should deploy appropriate interventions to pause, delay and stop suspicious payments. The Treasury is examining the best way to allow PSPs to adopt a risk-based approach to inbound and outbound payment processing.

1.216 We have considered the additional comments in developing the policy statement and provided our view where appropriate.

2 Respondents to September 2022 consultation

We have included a list of the 71 written responses to the consultation at Table 1. Where a public response has been provided, this is available on our website.

Table 1: Respondents to the consultation

| Respondent group | Organisation |
|--|---|
| Consumer Organisations and Groups | Citizens Advice Scotland |
| | Consumer Council |
| | Money Advice Trust |
| | The Money Charity |
| | National Trading Standards |
| | Money Saving Expert |
| | Victim Support |
| | Age UK |
| | Which? |
| | Financial Services Consumer Panel |
| PSPs – CRM Code signatories | Starling |
| | Lloyds Banking Group |
| | Nationwide |
| | Santander |
| | HSBC UK – <i>no public response received to publish</i> |
| | Barclays |
| | HSBC – <i>no public response received to publish</i> |
| | NatWest |
| | Virgin Money UK |

| Respondent group | Organisation |
|---|--|
| PSPs – Not CRM Code signatories: Banks and building societies | Stafford Railway Building Society |
| | Coventry Building Society |
| | TSB |
| | Leeds Building Society |
| | Unity Trust Bank |
| | Investec |
| | Revolut – <i>no public response received to publish</i> |
| | Counting Up |
| | Monzo – <i>no public response received to publish</i> |
| | PSPs – Others including EMLs, PISPs and Service Providers |
| Ordo Pay | |
| Clear Junction | |
| PockIt – <i>no public response received to publish</i> | |
| EML Payments / PrePaid Financial Services – <i>no public response received to publish</i> | |
| Hargreaves Lansdown | |
| Transpact | |
| Fire | |
| Token | |
| ClearBank | |
| Modulr FS Limited | |
| Prepay Technologies (PPS) | |
| Truelayer | |
| Wise – <i>no public response received to publish</i> | |
| CreDec – <i>no public response received to publish</i> | |
| Investec | |
| Experian | |

| Respondent group | Organisation |
|---|---|
| Trade bodies and industry groups | LSB |
| | Payments Innovation Forum |
| | BSA |
| | EMA |
| | Innovate Finance |
| | The Payments Association |
| | Stop Scams |
| | Open Finance Association |
| | UK Finance |
| PSO | Pay.UK |
| Government | Government Banking and its customers (HMRC) – <i>no public response received to publish</i> |
| Other stakeholders including individuals | Cyber Defence Alliance |
| | Lyddon Consulting |
| | ISPAY Limited |
| | Bob Ford and John Betrand |
| | 4KEYS International |
| | Adam Kramer |
| | Law Society of Scotland |
| | Larkfleet Group |
| | Fintail & RUSI |
| | Fraud Advisory Panel |
| | Transparency Task Force – <i>no public response received to publish</i> |
| | Steven Murdoch |
| | FeatureSpace |
| | CallSign |
| Cybera | |

PUB REF: PS23/3 Annex 3

© The Payment Systems Regulator Limited 2023

12 Endeavour Square

London E20 1JN

Telephone: 0300 456 3677

Website: www.psr.org.uk

All rights reserved