PSR Payment Systems Regulator

Policy statement

Fighting authorised push payment fraud: a new reimbursement requirement

Response to September 2022 consultation (CP22/4)

June 2023

PS23/3

Contents

Foreword

Today, there are more incidents of fraud than any other crime in the UK. Authorised push payment (APP) fraud has quickly become one of the most significant types of payment fraud globally. Once a victim realises they have been scammed, it's often too late to stop it and it can have a devastating impact on their life or business.

Criminals are becoming more sophisticated every day. We need to act in bold new ways to change the payment industry culture to improve fraud prevention and focus firms on protecting consumers and businesses.

The Payment Systems Regulator (PSR) is committed to fighting APP fraud and, in a world first, we are introducing a new reimbursement requirement. We are:

- incentivising the payment industry to invest further in end-to-end fraud prevention by making every payment firm meet the cost of reimbursing
- increasing customer protections so most victims of APP fraud are swiftly reimbursed, boosting confidence in the UK payment ecosystem
- pursuing our long-term ambition for Pay.UK to take on a broader role and actively improve the rules governing Faster Payments to tackle fraud

Alongside the new requirement to reimburse victims, we are increasing transparency with a new balanced scorecard of APP fraud data, promoting intelligence sharing and expanding the rollout of the name-checking service Confirmation of Payee. These measures are already prompting positive change in the industry with increased efforts by firms to tighten up controls and share more data than ever before. We expect industry to continue these initiatives and adopt new, innovative approaches to prevent APP fraud.

We have engaged extensively in developing the new reimbursement requirement and heard a wide range of views. We have listened carefully and created a balanced, proportional approach to reimbursement. This package is a major step forward, but it will evolve and be refined over time with better data and as lessons are learnt through implementation.

We are not acting alone in fighting APP fraud. Fraud does not respect the boundaries of any one organisation, or industry, nor the differences between the private and public sector. To tackle this problem effectively, collaboration is critical. We are engaging extensively with the Financial Conduct Authority, the Treasury, the Home Office, Ofcom, the Department for Digital, Culture, Media and Sport, police forces and other public bodies to stop fraudsters operating in the UK.

We want to implement the new reimbursement requirement as soon as practically possible. Every day, there are new victims of APP fraud but the payment industry's approach will not change overnight. In the short term, the new reimbursement requirement will be challenging for some firms. But in the longer term, it will consistently raise standards, increase safety and security for customers and help maintain the UK's position as a global leader in payments. We will work closely with Pay.UK and industry to drive effective, timely implementation backed by our regulatory oversight and powers. We are grateful to everyone who contributed and responded to our consultations, and we are delighted to put this policy in place.

Aidene Walsh Chair, PSR

Chris Hemsley Managing Director, PSR

1 Executive summary

1.1 We are introducing a new reimbursement requirement for APP fraud within the Faster Payments system. APP fraud happens a when fraudster tricks someone into sending a payment to an account outside of their control.[1] In 2022, there were around 207,000 reported APP fraud cases on personal accounts (an increase of 6% on 2021) and losses totalled £485.2 million.[2] These figures cover only a subset of payment firms, and many cases go unreported, so the real figures are likely to be higher. Besides financial losses, victims of APP fraud suffer worry, uncertainty and hardship.

1.2 The last three years has seen considerable progress in improving reimbursement for victims. The Contingent Reimbursement Model (CRM) Code was launched in 2019 as good industry practice to prevent APP fraud and respond to its growth. In 2022, 66% of APP fraud losses within scope of the CRM Code were reimbursed to the victim.[3] The CRM Code has been supported by some examples of industry innovation (see Box 1). We have seen the start of a positive cultural shift across the payment sector in anticipation of the requirement to reimburse victims of APP fraud.

1.3 For the first time, the new reimbursement requirement will introduce consistent minimum standards to reimburse victims of APP fraud. The new reimbursement requirement is underpinned by ten key policies (see Table 1). Essentially it will:

- Require payment firms to reimburse all in-scope customers who fall victim to APP fraud in most cases
- Share the cost of reimbursing victims 50:50 between sending and receiving payment firms
- Provide additional protections for vulnerable customers

1.4 We are increasing protections within Faster Payments because currently the majority of APP fraud is enacted with a Faster Payment. The new reimbursement requirement will apply to all Payment Service Providers (PSPs)[4] within the scope of the policy, this includes high-street banks and building societies but also smaller payment firms (see Chapter 2). Criminals operate across payment systems, and work is underway to consider whether the new reimbursement requirement (or equivalent protections) should apply to other payment systems. The Bank of England, as the operator of the CHAPS system, is committed to achieving comparable outcomes of consumer protection for CHAPS transactions (see Chapter 2).

1 In our September 2022 consultation, PSR, *Authorised push payment scams: requiring reimbursement* (September 2022), we referred to our work on APP scams. We have updated our terminology to APP fraud to align with the government's Fraud Strategy, Home Office, *Fraud strategy* (May 2023)

2 UK Finance, *Annual fraud report – The definitive overview of payment industry fraud in 2023* (May 2023).

3 66% of losses in cases reported under the CRM Code. UK Finance, *Annual fraud report – The definitive overview of payment industry fraud in 2023* (May 2023).

4 This document also refers to Payment Service Providers as payment firms.

1.5 The new reimbursement requirement will come into force in 2024. We will consult on a specific start date alongside our draft legal instruments in early Q3 2023. We expect industry to start work now to implement the new reimbursement requirement (see Chapter 7).

Incentives to innovate

1.6 We are setting minimum standards, defining the outcomes we expect (see 1.12 and Figure 2), and aligning financial and reputational incentives on payment firms.

1.7 We want payment firms to take responsibility for protecting their customers at the point a payment is made. In doing so, we expect the new reimbursement requirement to lead firms to innovate and develop effective, data-driven interventions to change customer behaviour. This includes adopting a risk-based approach to payments with firms making better decisions on when to intervene and hold or stop a payment. 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.

1.8 In adopting an outcome-based approach, we are giving Pay.UK and the industry the space to innovate and to choose how best to deliver the new reimbursement requirement, including defining the operational processes. We will play a key role in monitoring and enforcing the effectiveness of these processes to deliver the new reimbursement requirement.

1.9 The new reimbursement requirement and underlying policies are proportionate in relation to the expected benefits (see Box 2).

Box 1: Examples of industry innovation to reimburse APP fraud victims

- Since 2019, TSB has offered a fraud refund guarantee. The bank fully reimburses all APP fraud losses unless the customer has been involved in committing the fraud or has abused the guarantee. TSB reports that 98% of all fraud claims are refunded.[5]
- Since 2021, Nationwide has provided a scam checker service. Customers can talk to Nationwide when they are not sure about a payment they are about to make. If the service reviews a transaction that turns out to be fraudulent, Nationwide fully reimburses the customer unless the service advised them not to make the payment.[6]

5 TSB, *Fraud Refund Guarantee*

6 Nationwide, *Scam Checker Service*

Key policies

Table 1: The new reimbursement requirement is underpinned by ten key policies, designed as a balanced package to set out the framework of the policy

Key policy	Aligns with our September 2022 consultation?[7]
1 **Reimbursement requirement for APP fraud within Faster Payments**. Sending PSPs must reimburse all customers who fall victim to APP fraud (noting the exceptions and limits set out in policies 3 to 10). See Chapter 2 for the scope of the policy. The reimbursement requirement does not apply to: • civil disputes • payments which take place across other payment systems • international payments • payments made for unlawful purposes	**Yes**
2 **Sharing the cost of reimbursement.** Receiving PSPs must pay sending PSPs 50% of the reimbursement that the sending PSP paid to the customer. A time period will be set by Pay.UK with an ultimate backstop to ensure receiving PSPs reimburse sending PSPs.	**Yes**
3 **Exceptions for APP fraud claims**. There are two exceptions to reimbursement (noting the other policies) under the new reimbursement requirement: Where the customer has acted fraudulently ('first-party fraud') Where the customer has acted with gross negligence. This is the customer standard of caution for APP fraud claims.[8]	**Yes**
4 **Time limit to reimburse**. Sending PSPs must reimburse customers within five business days under the new reimbursement requirement. For specific actions, the sending PSP can 'stop the clock' (see Box 5, Chapter 5).	**Yes.** However, this has been extended from the proposed 48-hour time limit to reimburse.
5 **Claim excess.** Sending PSPs have the option to apply a claim excess under the new reimbursement requirement. *We will consult on the appropriate level for this and publish the maximum excess in PSR guidance in Q4 2023.*	Subject to consultation

7 PSR, *Consultation CP22-4: Authorised push payment (APP) scams: Requiring reimbursement*, (September 2022)

8 There is a potential risk that, if customers are more confident of being reimbursed, they will take less care in ensuring that their payee is not a fraudster (the risk of moral hazard). Since we cannot, at present, rule out this risk, as part of our mitigations we have considered an exception to reimbursement to incentivise customers to continue to exercise caution (see Chapter 4, Table 4). This is the customer standard of caution. Gross negligence is a high bar and, where suspected, the burden of proof is on the PSP (see Chapter 5).

	Key policy	Aligns with our September 2022 consultation?[7]
6	**Minimum threshold.** There is no separate minimum value threshold for APP fraud claims under the new reimbursement requirement.[9]	**No.** We have removed the £100 minimum threshold for claims
7	**Maximum level of reimbursement.** There is a maximum level of reimbursement for APP fraud claims (by value) under the new reimbursement requirement. *We will consult on the appropriate maximum value for APP fraud claims and publish this in PSR guidance in Q4 2023.*	**No.** We did not consult on a maximum level of reimbursement.
8	**Time limit to claim.** Sending PSPs have the option to deny APP fraud claims submitted more than 13 months after the final payment to the fraudster.	**Yes**
9	**Treatment of vulnerable customers.** The customer standard of caution and claim excess must not be applied to vulnerable customers.	**Yes.** We have now mandated the exception to the claim excess for vulnerable customers
10	**Approach to 'multi-step' fraud cases.** The new reimbursement requirement applies to the Faster 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 (see Chapter 2).	**Yes**

Implementing reimbursement

1.10 We want Pay.UK, as the independent payment system operator (PSO), to run Faster Payments in a way that ensures that customers are protected, and fraud is prevented from entering the system. In 2022, our five-year Strategy set out that we want to give Pay.UK a stronger role to lead the development of protections for payment system users.

1.11 Our view is that 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. 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. We have been working closely with Pay.UK to design arrangements for reimbursement that are effective from the outset. We will therefore implement the new reimbursement requirement through a combination of Faster Payments rules and PSR directions.

9 We will consult on the appropriate level for the claim excess and acknowledge that this could act as a de facto minimum threshold depending on how it is structured and implemented.

1.12 We will direct Pay.UK to put the new reimbursement requirement into Faster Payments rules using our powers under section 55 of the Financial Services (Banking Reform) Act 2013 (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. Our expectation is that this approach to implementation will evolve over time as we look to Pay.UK to introduce the changes necessary to reach all participants and enforce the requirements.[10]

Table 2: Implementation approach

Instrument(s)	What key policies and/or tasks will be covered by the instrument?
Rule change requirement (FSBRA section 55) for Pay.UK to amend Faster Payments rules	**All policies will be put into the Faster Payments rules, with additional guidance and detail provided by us for some policies (see 'PSR Guidance' and 'PSR Publication' below).** Specifically, the Faster Payments rules will include: • **reimbursement requirement and its scope (see Chapter 2)** • **sharing the cost of reimbursement** • **time limit to reimburse victims** • **claim excess** • **maximum level of reimbursement** • **time limit for victims to claim**
Directions (FSBRA section 54) *one general direction for all in-scope PSPs and one specific direction for Pay.UK*	**General direction setting out the reimbursement requirement and who it applies to, and to requiring all PSPs within the scope of the policy (including indirect participants) to comply with the relevant Faster Payments rules** and report data to Pay.UK. **Specific direction on Pay.UK to create and implement effective monitoring of PSPs in line with the rule change requirement and general direction.** Pay.UK to provide compliance data to us – this will inform any enforcement we may take and allow us to assess the effectiveness of the policy.
PSR guidance	• **guidance on the customer standard of caution (gross negligence)**
PSR publication (e.g., online notice)	• **maximum level of claim excess** • **maximum level of reimbursement**

10 We will consult on the structure and wording of the legal instruments in early Q3 2023

Expected policy outcomes

1.13 The new reimbursement requirement is a significant step to drive better fraud prevention and focus payment firms on protecting consumers and businesses**.** By implementing the new reimbursement requirement and delivering our wider measures (see Chapter 3), we expect to see:

1. **Less APP fraud**: The best result for everyone is a decrease in the level of APP fraud. This avoids distress, disruption and financial loss for all involved. It also stops money ending up in the hands of criminals.

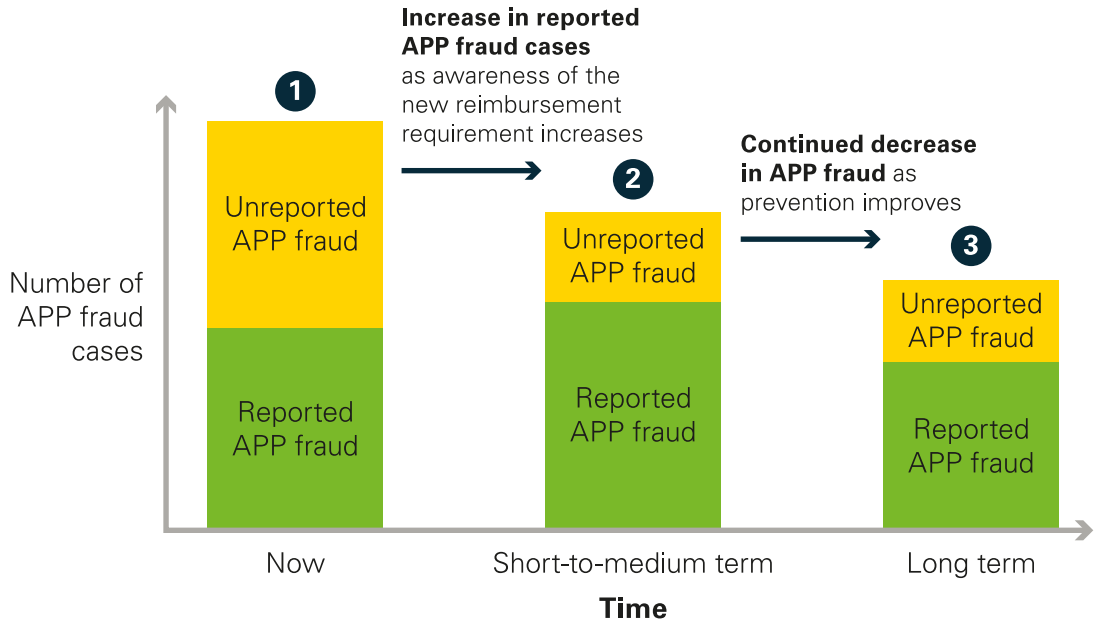
   In the short to medium term, we expect reported APP fraud cases to increase as victims become aware of the new reimbursement requirement and more payment firms report APP fraud. Over time, we expect total APP fraud incidents to decrease (see Figure 1).

2. **Improved protection for victims**: We want more victims of APP fraud consistently reimbursed for their losses.

3. **Effective incentives for payment firms**: We want payment firms to have financial and reputational incentives to further focus resources on preventing APP fraud.

4. **Increased confidence in Faster Payments**: Through better prevention and protection, we want to give users greater confidence to use account-to-account payments, helping them to be more competitive with card payments.

Figure 1: Expected changes in the level of APP fraud over time



Putting in place prevention

1.14 We recognise the critical role of the wider fraud ecosystem (see Chapter 3), and fraud must be tackled both 'upstream' and 'downstream'. However, payment firms play a pivotal role in designing fraud out of the system. For the first time, this policy will

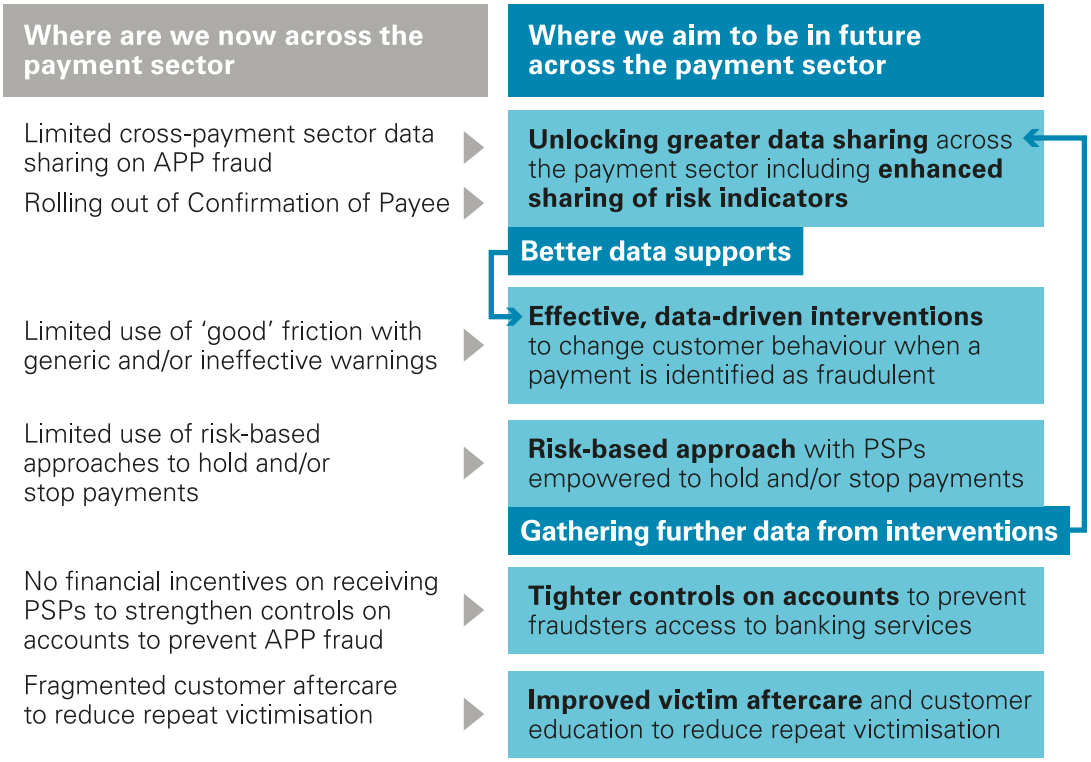
create consistent financial incentives for the whole Faster Payments industry to invest in more effective prevention of APP fraud, with payment firms sharing the cost of reimbursement.

1.15 Fraud is complex and continually evolving. There is no simple checklist approach to successful prevention, but we expect this policy to incentivise critical changes that improve prevention across the payment industry (see Figure 2).

1.16 Positive change is already underway. We expect it to accelerate and deepen across the sector in preparation for the introduction of the new reimbursement requirement and then to continue to be refined over time. We also acknowledge that payment firms will need support to achieve some of these outcomes (see Chapter 7).

1.17 Change began with the CRM Code, leading several signatory payment firms to innovate and then refine their approach to tackling APP fraud. We now expect to see much wider and more significant change for all payment firms as the industry moves to better protect customers and the UK payment ecosystem from fraudsters. This culture change will not happen overnight. We remain committed to playing our role in supporting Pay.UK and industry through timely, effective implementation (see Chapters 6 and 7).

Figure 2: Outcomes we expect the new reimbursement requirement to incentivise



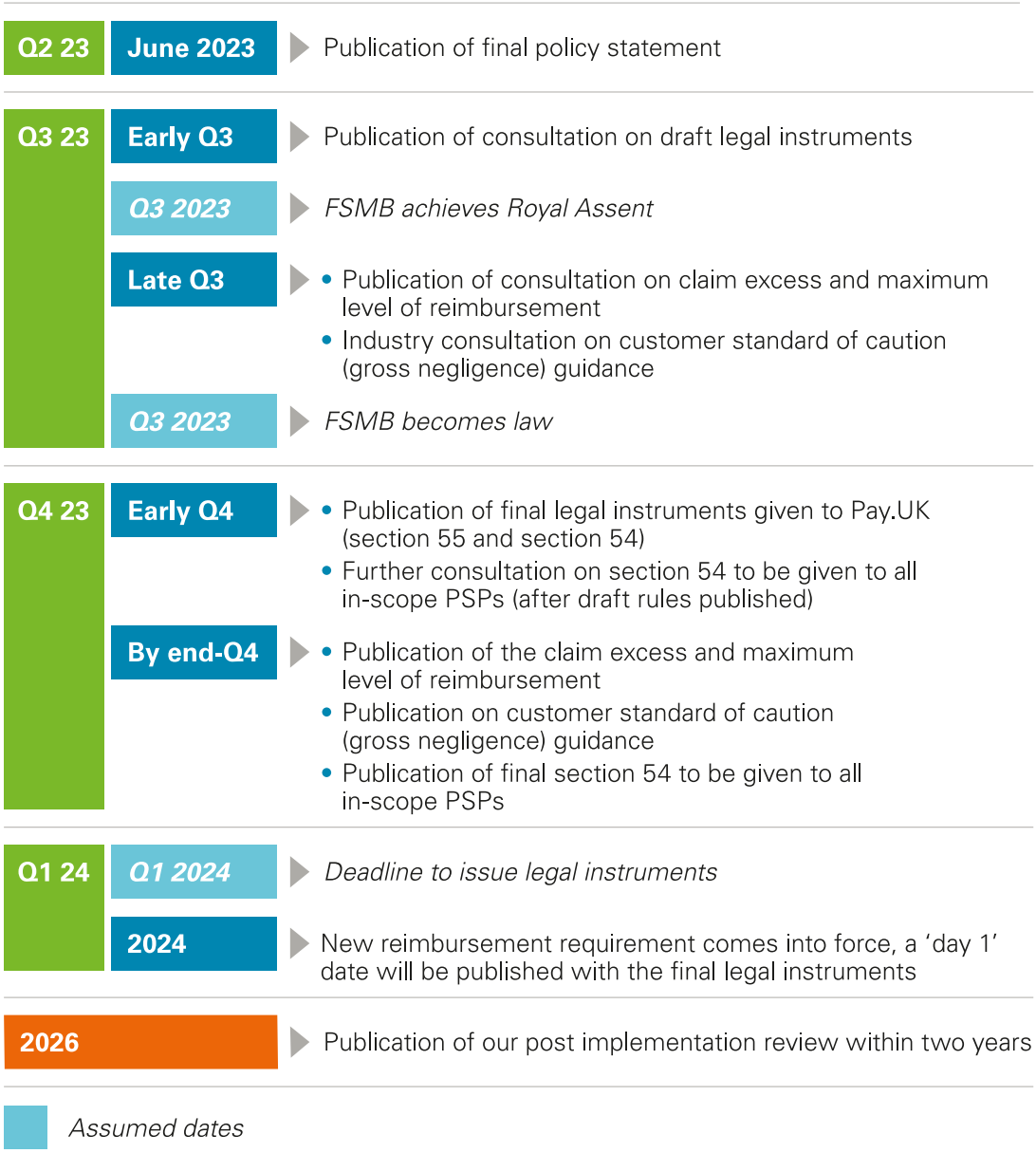
Next steps, refinement and future review

1.18 We will continue to engage and collaborate with a wide range of stakeholders as we progress to implementation. Figure 3 shows a high-level timeline with key milestones. Figure 8 in Chapter 6 sets out an engagement roadmap, with further detail on how we will engage stakeholders through 2023.

1.19 Pay.UK has started to consider what it will need to do for implementation, and we now expect that it will work with industry to accelerate implementation planning ahead of the new reimbursement requirement coming into force in 2024.

1.20 The fight against APP fraud is a long-term effort. We will review the effectiveness of the new reimbursement requirement within two years, taking in the lessons learned during implementation. The UK is the first country in the world to implement consistent standards to reimburse victims of APP fraud, and other jurisdictions are watching closely in considering their own approaches. The post-implementation review will be one step in refining our approach. With better data and a richer understanding of fraud, we will continue to evolve this policy framework to drive APP fraud out of UK payments.

Figure 3: High-level timeline for the new reimbursement requirement



Box 2: Proportionality and cost benefit analysis

The new reimbursement requirement and specific policies are proportionate to the expected benefits. We completed a proportionality assessment which found:

- APP fraud poses a significant threat to users of Faster Payments, with the number of APP fraud cases growing. We are focusing on Faster Payments because it is it is the type of payment which is most frequently requested by fraudsters for APP fraud. Fraudulent payments make up a very small proportion (less than 0.1% in 2021) of overall Faster Payments volumes but the harm they create is significant enough for the PSR to act.
- 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.
- Many APP frauds originate online or via call or text. But PSPs play a critical role as APP fraud can only be successful if facilitated via a payment. It is sufficiently in the public interest to require PSPs to reimburse victims of APP fraud in most cases. Our approach is proportionate as it shares the costs of reimbursement between PSPs, recognising that sending and receiving firms can take steps to detect potential frauds and refuse payment orders or block accounts if they suspect fraud.
- We have a strategic priority of ensuring payment system users are sufficiently protected. We need to use our powers under FSBRA to direct PSPs to act and reimburse their customers because not all PSPs are taking sufficient action. Greater investment and innovation in fraud prevention will reduce fraud and harm to customers.
- The CRM Code has improved customer outcomes and fraud prevention efforts but there is still a lack of consistent customer protection for Faster Payments. For example, the Financial Ombudsman Service (FOS) is upholding a high proportion of APP fraud complaints in customers' favour. Over the last 12 months, the FOS has upheld rates around 50% of APP fraud cases.
- The new reimbursement requirement will only work effectively if we use our powers to direct all relevant PSPs to take the required action to systemically tackle APP fraud. Effective reimbursement requires collaboration and co-ordination across a payment system. For this reason, phasing implementation would not be appropriate.

We have analysed the cost and benefits of our policy. The separate Annex 4 sets out our updated cost benefit analysis.

Guide to the policy statement

This sets out a high-level guide to the rest of the policy statement to help direct readers to relevant material:

Chapter 2: Scope of the new reimbursement requirement	Sets out the scope of the new reimbursement requirement.
Chapter 3: Wider action to fight fraud	Sets out how the new reimbursement requirement is part of a wider package of measures to reduce fraud.
Chapter 4: Summary of feedback to our consultation	Sets out a summary of stakeholders' views and our response to key themes identified through our September 2022 consultation.
Chapter 5: Key policies in practice	Sets out the ten key policies into the context of an illustrative APP fraud reimbursement journey to provide clarity on how we expect the new reimbursement requirement to work in practice.
Chapter 6: Putting in place reimbursement	Sets out how we will implement the new reimbursement requirement through a combination of Faster Payments rules and PSR directions.
Chapter 7: Achieving successful implementation	Sets out the key actions which industry will need to complete to comply with the new Faster Payments rules and PSR directions.
Chapter 8: Evaluating policy effectiveness	Sets out how we will monitor the effectiveness of the new reimbursement requirement and publish a post-implementation review within two years.
Annex 1: Equality impact assessment	Sets out our assessment of the equality impacts and rationale for the new reimbursement requirement, in line with our public sector equality duty under the Equality Act.
Annex 2: Payment initiation service transactions	Sets out how the new reimbursement requirement applies to payment initiation service transactions.

There are two additional annexes published separately to this policy statement:

Annex 3: Question-by-question feedback and response to our consultation	Sets out a summary of stakeholders' views and our response to each of the 28 questions in our September 2022 consultation. This includes a list of respondents to the September 2022 consultation.
Annex 4: Cost benefit analysis	Sets out our cost benefit analysis of the new reimbursement requirement.

2 Scope of the new reimbursement requirement

APP fraud cases covered by the new reimbursement requirement

2.1 Section 68 (1) of the Financial Services and Markets Bill (FSMB) instructs us to 'prepare and publish a draft of a relevant requirement for reimbursement in such qualifying cases of payment orders as the Regulator considers should be eligible for reimbursement'. Section 68(2), adds that 'a 'qualifying case'' is where '(a) the case relates to a payment order executed over the Faster Payments Scheme, and (b) the payment order was executed subsequent to fraud or dishonesty'.

2.2 The new reimbursement requirement applies to payments – executed by the sending PSP in accordance with an authorisation given by its customer – to an account controlled by a person other than the customer, where the customer has been deceived into granting that authorisation as part of an APP fraud case. This includes where:

- the payer intends to transfer the funds to a person other than the recipient, but is deceived into transferring the funds to the recipient
- the payer intends to transfer the funds to the recipient but is deceived as to the purposes for which they are transferring the funds

2.3 All types of APP fraud are within the scope of the new reimbursement requirement.[11]

Examples of APP fraud

Example 1	A customer sees a holiday advertisement on a social media platform. They click the link on the advert taking them to a website that appears completely legitimate. The customer decides to purchase a holiday and does so via a bank transfer. A few days later, after not receiving much information and becoming increasingly concerned, they realise they have been a victim of fraud. The customer suffers a loss of £4,500.
Example 2	Through a dating app, a customer is befriended by an individual who lives in a different part of the UK. Over a few months, they build what appears to be a genuine relationship. In time, the individual says they have fallen ill, and they are struggling to cover their living costs. Concerned, the customer sends multiple payments to help pay these costs. Requests then follow for money to fund a visit to the customer. After sending numerous payments, the customer realises they are never going to see the individual, who is a fraudster. The customer suffers a loss of over £10,000.

11 APP fraud types can include (but are not limited to) impersonation, investment, romance, purchase, invoice and mandate, CEO fraud and advance fee. UK Finance, *Fraud – The Facts 2021* (March 2021).

Transactions covered by the new reimbursement requirement

2.4 We are focusing on Faster Payments because it is the type of payment which is most frequently requested by fraudsters for APP fraud. Though payments resulting from APP fraud represented less than 0.1% of overall Faster Payments volumes in 2021, Faster Payments were used for 97% of APP fraud payments.

2.5 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 (see 2.18 to 2.19). The new reimbursement requirement does **not** apply to:

- payments which take place across other payment systems – for example, if a customer sends funds to their account at a crypto exchange and then pays a fraudster via a crypto currency (see Figure 4)
- international payments
- payments made for unlawful purposes
- civil disputes, such as where a customer has paid a legitimate supplier for goods or services but has not received them, they are defective in some way, or the customer is otherwise dissatisfied with the supplier.

2.6 Civil disputes do not meet our definition of an APP fraud as the customer has not been deceived (see 2.2). The law protects consumer rights when purchasing goods and services, including through the Consumer Rights Act[12]. A sending PSP should be able to determine whether a claim is a civil dispute through communication with the customer and the receiving PSP.

Start date for the new reimbursement requirement

2.7 The new reimbursement requirement will apply to Faster Payments authorised after the regulatory requirement comes into force in 2024. We will consult upon and then publish the start date alongside the draft and final legal instruments in Q4 2023.

2.8 The start date ('day one') does not prevent PSPs from voluntarily reimbursing victims of APP fraud now, including providing reimbursement under the CRM Code. We expect the CRM Code requirements to stay in place until the new reimbursement requirement comes into force (see 3.9 to 3.11).

12 GOV.UK, *Consumer protection rights*

Customers covered by the new reimbursement requirement

2.9 The new reimbursement requirement applies to consumers, microenterprises and charities (defined in the glossary). This policy statement refers to payers within the scope of the requirement collectively as 'customers'. This is the same coverage of payers as in the CRM Code.

Vulnerable customers

2.10 We have considered the potential impacts of the new reimbursement requirement on vulnerable customers, including as part of our Equality Impact Assessment (see Annex 1). The sending PSP processing an APP fraud claim (see Chapter 5) should assess the customer's situation and any potential vulnerability in line with the Financial Conduct Authority's (FCA) guidance for PSPs on the fair treatment of vulnerable customers: 'Firms should consider consumers' vulnerability and capacity to make decisions when deciding how to treat consumers who have been victims of scams or fraud'.[13]

2.11 As set out in the FCA guidance, 'consumers with some characteristics of vulnerability may be more likely to fall victim to scams'.[14] 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 (applying the definition in paragraph 2.12), the sending PSP must notapply the customer standard of caution (gross negligence) or claim excess. In Q3 2023, we will consult on whether the maximum level of reimbursement will apply to vulnerable customers.

2.12 For the new reimbursement requirement, all firms should consistently apply the FCA's definition in order to identify customers vulnerable to APP fraud: 'A vulnerable customer is someone who, due to their personal circumstances, is especially susceptible to harm, particularly when a firm is not acting with appropriate levels of care'.[15] This means, in relation to regulatory requirements, firms are working to a single definition of vulnerability.

2.13 PSPs should evaluate each customer's circumstances on a case-by-case basis to help determine the extent to which their characteristics of vulnerability, whether temporary or enduring, led them to be defrauded, and therefore whether they meet the definition of vulnerability set out in paragraph 2.12. This is not a blanket exception for all customers who exhibit any characteristics of vulnerability. PSPs are expected to comply with the FCA's guidance on vulnerability and be mindful of their obligations under the Consumer Duty (see 3.12 to 3.14).

13 FCA, *FG21/1 Guidance for firms on the fair treatment of vulnerable customers* (February 2021)

14 FCA, *FG21/1 Guidance for firms on the fair treatment of vulnerable customers* (February 2021)

15 FCA, *FG21/1 Guidance for firms on the fair treatment of vulnerable customers* (February 2021)

PSPs covered by the new reimbursement requirement

2.14 PSPs that operate the sending or receiving payment account for a qualifying transaction (see 2.5) are within the scope of the new reimbursement requirement. This includes direct and indirect Faster Payments participants (see Glossary). For the avoidance of doubt, PSPs that do not operate the sending or receiving payment account are out of scope. Further detail on how the new reimbursement requirement applies to payment initiation services providers (PISPs) is at 2.18 to 2.19, and Annex 2.

Protecting users of the UK's payment systems

2.15 Ensuring end users are sufficiently protected when using the UK's payment systems is a strategic priority for us. As set out in Chapter 1, we are increasing protections within Faster Payments because Faster Payments are being used in the majority of APP fraud cases. But criminals operate across payment systems, so we are considering whether the new reimbursement requirement should apply to other payment systems.

2.16 We will consider risks across different payment systems and, where necessary, address them with future action. In applying this principle, the new reimbursement requirement will apply to PIS transactions, see 2.18 to 2.19. The Bank of England, as the operator of the CHAPS system, is committed to achieving comparable protections for CHAPS transactions, see 2.20.

2.17 We are also looking forward to new payment systems and, in parallel to implementing the new reimbursement requirement, Pay.UK are delivering the New Payments Architecture (NPA). The requirement to reimburse victims of APP fraud will carry over into the NPA. We have set a deadline to complete migration to the new, competitively procured infrastructure by 1 July 2026.

Open banking payments (PIS transactions)

2.18 Payment initiation service (PIS) transactions are in scope of the requirements. Open banking and other innovations are improving opportunities for interbank retail payments. To enable PIS transactions to grow significantly requires greater trust in these payments. This aligns with our work on account-to-account payments and open banking.

2.19 We apply the new reimbursement requirement to PIS transactions in the same way as with other types of Faster Payments. The obligations on sending and receiving PSPs are unchanged, including that sending and receiving PSPs must share the cost of the new reimbursement requirement 50:50. Annex 2 gives further detail, including examples of how this will work in practice.

CHAPS

2.20 The Bank of England, as the operator of the CHAPS system, is committed to achieving comparable outcomes of consumer protection regardless of the payment system the consumer uses. We are working with the Bank of England to define a model for reimbursement which reflects the unique characteristics of CHAPS, is simple to operationalise, and creates comparable protections for customers. We expect to adopt a similar approach, giving a direction under section 54 of the Financial Services (Banking Reform) Act 2013 (FSBRA) to require scheme participants to comply with relevant requirements set out in the scheme rules.[16] We will announce timings for consultation and implementation alongside our consultation on the draft legal instruments for Faster Payments participants and Pay.UK in early Q3 2023.

'On us' payments

2.21 We are engaging the FCA on the application of the reimbursement requirement to 'on us' payments, where the fraudster uses an account provided by the victim's own PSP. Our powers do not extend to regulating 'on us' payments because they are not transferred via a payment system designated to us under FSBRA. PSPs should reimburse 'on us' APP fraud in the same way as Faster Payments and communicate to their customers if they handle 'on us' APP fraud differently. Victims are impacted in the same way, and they should have the same right to reimbursement.

Other payment systems

2.22 APP fraud also impacts users of Bacs. As set out at 2.16, we will consider risks across different payment systems and, where necessary, address them with future action. Although it is not a type of push payment fraud, the same principle applies to authorised card fraud.

Multi-step fraud cases (also known as 'multi-hop' or 'multi-generational' fraud)

2.23 Some APP fraud cases involve more than one payment. For example, the fraudster may 'socially engineer' a victim to transfer money from their bank account to an account they hold at a different PSP. The fraudster then manipulates the victim to transfer the money from that account to one outside the victim's control. These fraud cases can be referred to as 'multi-hop', 'multi-step' or 'multi-generational'. This document refers to them as multi-step fraud cases.

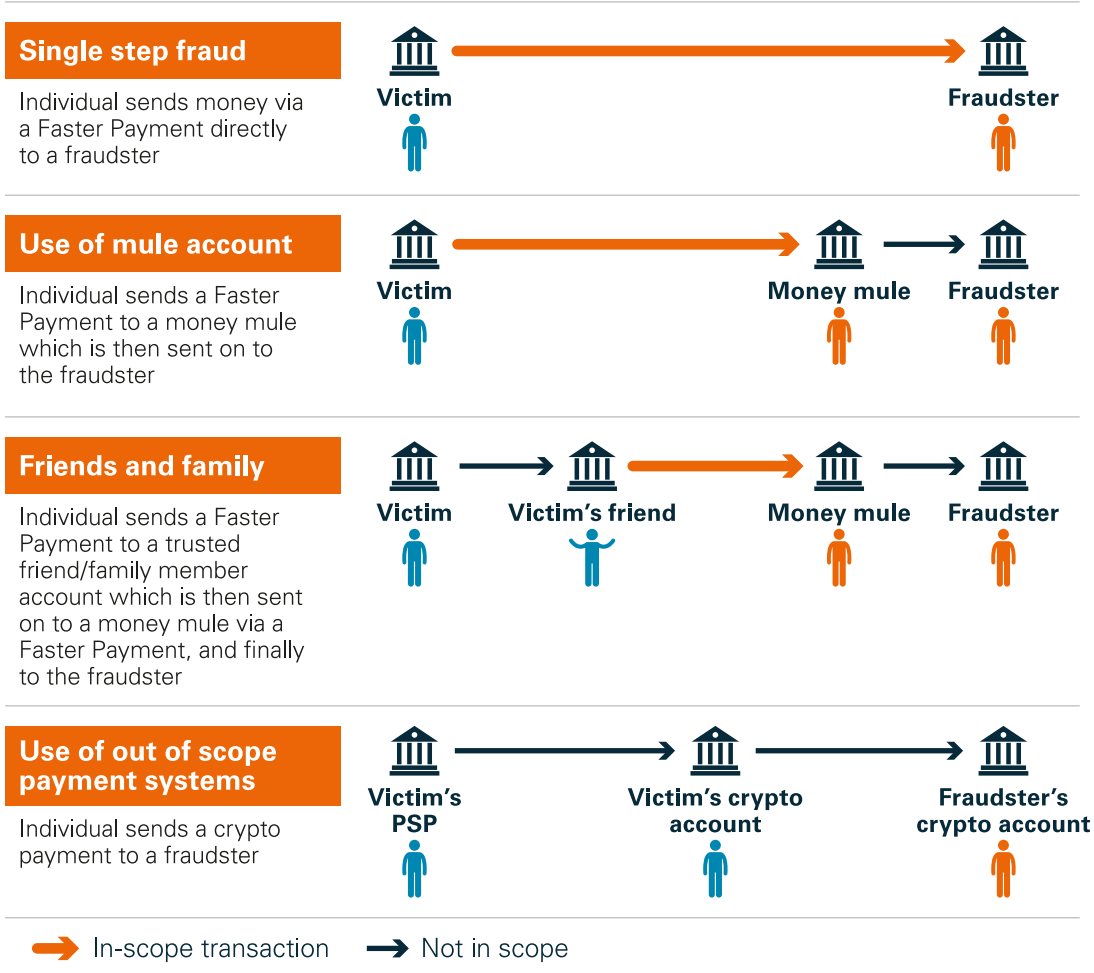
2.24 The new reimbursement requirement applies to the Faster Payment to an account controlled by a person other than the customer, where the customer has been deceived into granting that authorisation as part of an APP fraud case.

16 This may exclude some types of CHAPS participants.

2.25 When we refer to multi-step fraud cases, we are not referring to fraud across different payment systems, such as where a victim sends a crypto transaction to a fraudster. Figure 4 sets out potential examples of multi-step APP fraud cases. There are many more types of multi-step fraud, for which we expect Pay.UK to work with industry to develop further guidance to support implementation.

2.26 We will consider whether any further guidance is required on the scope of our requirements as we develop the legal instruments to implement our policy.

Figure 4: Multi-step APP fraud examples, showing which transaction is within the scope of the new reimbursement requirement



3 Wider action to fight fraud

Reimbursement will create a clear financial incentive for payment firms to do everything they can to limit a fraudster's ability to access the UK banking system, and their ability to move money into their control.

The better PSPs get at this, the closer we will get to the ultimate objective of limiting criminals' ability to use the UK's banking and payments systems to commit fraud, but this policy is just one part of a wider package of measures to reduce fraud.

Our objectives and priorities

3.1 Our statutory objectives underpin everything we do. In summary, these are:

- to ensure that payment systems are operated and developed in a way that considers and promotes the interests of all the businesses and consumers that use them
- to promote effective competition in the markets for payment systems and services – between operators, PSPs and infrastructure providers
- to promote the development of and innovation in payment systems, in particular the infrastructure used to operate those systems

3.2 In 2022, we set out four strategic priorities for the PSR linked to our statutory objectives[17]. The new reimbursement requirement aligns with our statutory and strategic objectives. It furthers our commitment to ensure that users are sufficiently protected when using the UK's payment systems and, in the longer term, it will promote competition through creating a more efficient payments market based on clearer standards for preventing fraud (see our updated cost benefit analysis at Annex 4).

3.3 In acting against fraud across Faster Payments, we are working towards our strategic goals by strengthening customer protections in account-to-account payments to build customer trust and positively position them as a safe and secure payment method.

17 PSR, *The PSR Strategy*, (January 2022)

PSR's action against APP fraud

3.4 Through a multi-pronged approach, we are pushing hard to make sure that all PSPs take all appropriate steps they can to limit fraudsters' ability to access the UK banking system and their ability to move money into their control. We are:

1. **Publishing a balanced scorecard of APP fraud data (Measure 1):** In March 2023, we directed 14 PSPs to provide six-monthly data showing how effectively firms are handling APP fraud. This is a crucial step towards greater transparency in the fight against fraud. Across the payments industry, the largest sending PSPs and all receiving PSPs will be accountable for their own performance and will be encouraged to do more to prevent fraud and look after victims.

   This action will also put more power in the hands of the customer, enabling them to see how well their bank or building society will protect them if they fall victim to fraud. This will provide a significant boost to the information customers have when choosing who to bank with.

2. **Increasing intelligence sharing (Measure 2):** In our drive for greater data sharing, we have tasked industry with developing a data and intelligence sharing tool to consider the riskiness of payments and improve fraud prevention. The industry supports this initiative and agrees that Enhanced Fraud Data (EFD) will help prevent fraud. A UK Finance pilot last year showed that EFD sharing between sending and receiving firms can significantly improve fraud detection.

   Pay.UK, with the support of UK Finance, is now taking forward a project to deliver EFD. Pay.UK has consulted on the first iteration of data standards to support this information sharing and is working towards building an application programming interface (API) solution through which standardised customer data will be sent. We expect PSPs to start implementing aspects of the system by the end of 2023.

3. **Expanding the rollout of Confirmation of Payee (CoP):** In October 2022, we published the final policy statement and direction on 400 new PSPs to expand CoP, a name-checking service for UK-based payments. CoP helps to reduce accidentally misdirected payments and APP fraud – for example, impersonation scams.

Wider fraud ecosystem

3.5 As the gatekeepers to the financial system, PSPs have a critical role in the fight against fraud. With the right tools – and the incentive of the new reimbursement requirement – they can stop a payment they suspect could be fraudulent. In Chapter 1, we set out further detail on the outcomes we expect these incentives will drive in changing PSPs' approaches towards APP fraud. While these measures mark a significant step towards designing fraud out of the financial system, they do not address the whole picture. Almost all respondents to our consultation agreed that further action was needed across the wider fraud ecosystem – from fraud origination to enforcement and repatriation of funds.

3.6 Fighting APP fraud requires coordinated action by the public and private sector, right across the fraud journey. This starts when the payment account is set up or the victim is first recruited. It continues with the transaction being initiated, and then it is received into an account controlled by the fraudster, followed by the movement of money into other accounts.

3.7 In May 2023, the Home Office published its Fraud Strategy, setting out actions to tackle the growing incidence of fraud. We have identified the key actions from the strategy that reflect the priorities identified by stakeholders during our consultation. These actions – led by the government, other regulators and key actors within the wider fraud ecosystem – are set out in Figure 5, which divides them into four themes:

- **Legislation**: Creating a wider statutory framework to support the new reimbursement requirement, from tackling online advertising to the Treasury's commitment to examining the best way of letting PSPs adopt a risk-based approach to inbound and outbound payment processing.
- **Data sharing**: Increasing the flow of information across the payment sector and wider ecosystem to stop potential fraud before it happens.
- **Customer education and victim support**: Raising awareness to help prevent customers become victims in the first place, and providing appropriate support and education when they do.
- **Law enforcement**: Disrupting APP fraud to stop fraudsters capitalising on their crimes and prosecuting them to bring them to justice.

Box 3: Action to stop the recruitment of fraud victims

We have seen positive action taken to stop victims being recruited. In the case of investment fraud, the FCA established a voluntary agreement with Google to change their advertising policies to only allow financial services adverts from FCA-authorised firms.[18] We have also seen Fraud Sector Charters developed between the Home Office and accountancy,[19] telecommunications[20] and retail banking[21] firms to help address specific risks within those sectors.

Fraud origination data

3.8 To support action across the wider fraud ecosystem, reports on fraud data should record where APP fraud originates, such as in social media or telecommunication firms. We are in the early stages of considering what data could be collected on APP fraud origination. We are aware that some PSPs are already capturing some of this data when recording instances of fraud. Over the coming months, we will engage with relevant stakeholders, including industry, government, regulators, and consumer organisations.

18 Google, *Further measures to help fight financial fraud in the UK* (June 2021)
19 Home Office, *Fraud sector charter: accountancy* (October 2021)
20 Home Office, *Fraud sector charter: telecommunications* (October 2022)
21 Home Office, *Fraud sector charter: retail banking* (October 2021)

We will consider the policy options and the channels available to us to collect this data and how we might best utilise it.[22]

The CRM Code

3.9 We expect PSPs to reimburse their customers when they are victims of APP fraud. PSPs should act now to prepare for the new reimbursement requirement to come into force in 2024 (see Chapter 7). Ten PSPs (representing 19 consumer brands and over 90% of authorised push payments) have already started this journey by signing up to the CRM Code.

3.10 The new reimbursement requirement provides a consistent set of minimum standards reaching over 1,500 PSPs, which provides significantly wider coverage with Faster Payments in comparison to the CRM Code. There are some additional benefits enshrined within the CRM Code. For example, it already applies to CHAPS and 'on us' payments and has additional provisions around prevention, detection and commitments to improving customer education. In the near future, we expect new protections to come into force for CHAPS and 'on us' payments (see Chapter 2). Additionally, we expect the new reimbursement requirement will incentivise further activity around prevention, detection and customer education

3.11 We expect the CRM Code requirements to stay in place until the new reimbursement requirement comes into force.

The FCA's Consumer Duty

3.12 The FCA's Consumer Duty will come into force on 31 July 2023 for new and existing products or services that are open for sale or renewal.[23] The Duty includes a new Consumer Principle that requires firms to act to deliver good outcomes for retail customers. This could include acting to prevent fraud. The new reimbursement requirement aligns with the Duty to support good customer outcomes.

3.13 The FCA expects the Duty to improve four outcomes, including consumer understanding (from account safety information, advice and warnings that can be easily and clearly actioned), consumer support when they need it, and appropriate victim aftercare. The Duty also introduces a cross-cutting rule that requires firms to avoid causing foreseeable harm. The FCA specifically highlights scams as an example of foreseeable harm – for example, when consumers become victims to scams relating to a firm's financial products due to a firm's inadequate systems to detect or prevent scams or inadequate processes to design, test, tailor and monitor the effectiveness of scam warning messages presented to customers.[24]

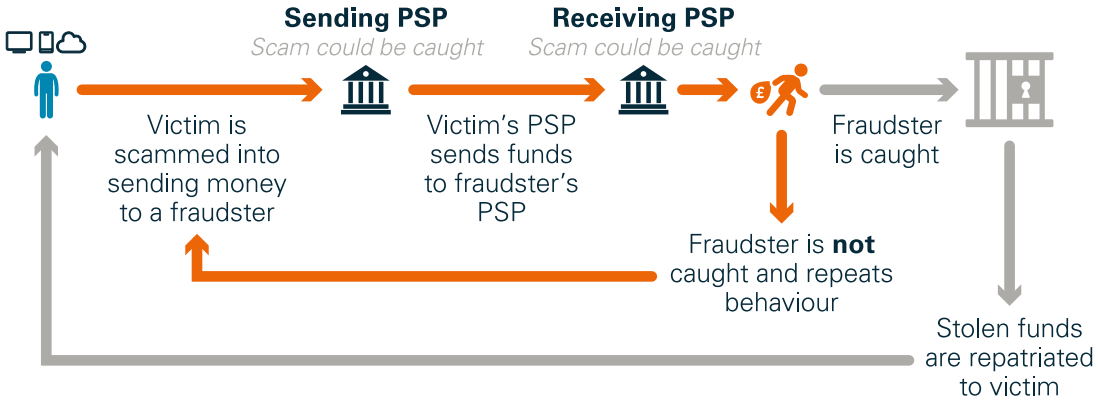
3.14 The Duty means a firm should strive to deliver good consumer outcomes and allow them to make informed decisions. For example, a firm could provide information about high-risk payments or inform consumers of account controls which could help keep them safer. Risk-based effective warnings to help prevent fraud could help a firm to deliver good outcomes.

22 PSR, *APP scams: Measure 1 – Collection and publication of performance data* (March 2023)

23 FCA, *PS22/9: A new Consumer Duty* (July 2022)

24 FCA, *PS22/9: A new Consumer Duty* (July 2022) See 5.23 in the guidance.

Figure 5: Priority actions across the wider fraud ecosystem supporting the new reimbursement requirement



Theme	Key actions from Home Office Fraud Strategy
1: Legislation	• Hold tech companies to account to reduce online fraud and issue significant fines for those who do not, by passing and implementing the Online Safety Bill, including the delivery of the Online Advertising Programme to ensure that UK-facing online advertising is safe from fraud and other harms. • Enable payment service providers to adopt a new risk-based approach to provide additional time for potentially fraudulent payments to be investigated. • Unlock information sharing by passing the Economic Crime and Corporate Transparency Bill. • Evaluate and determine the next steps on ensuring a consistent framework for repatriation of fraud funds to victims.
2: Data sharing	• Work with platforms to introduce seamless and consistent fraud reporting and implement existing Fraud Sector Charters by the end of 2023. • Agree further new charters with tech, insurance and other sectors by early 2024. • Improve the publication of APP fraud data (PSR's Measure 1). • Encourage intelligence and data sharing between PSPs (PSR's Measure 2). • Continue to work with all sectors and partners to maximise data sharing mechanisms, including through legislation.

Theme	Key actions from Home Office Fraud Strategy
3: Customer education and victim support	• Sharing best practice and expertise in developing awareness campaigns to educate individuals and businesses about the dangers of fraud and how to recognise and avoid scams. • Implement consistent support for victims across England and Wales by expanding the National Economic Crime Victim Care Unit and National Trading Standards' Multi-Agency Approach to Fraud by 2024.
4: Law enforcement	• Establish a National Fraud Squad with 400 new officers. • Replace Action Fraud with a state-of-the-art system for victims to report fraud.

4 Summary of feedback to our consultation

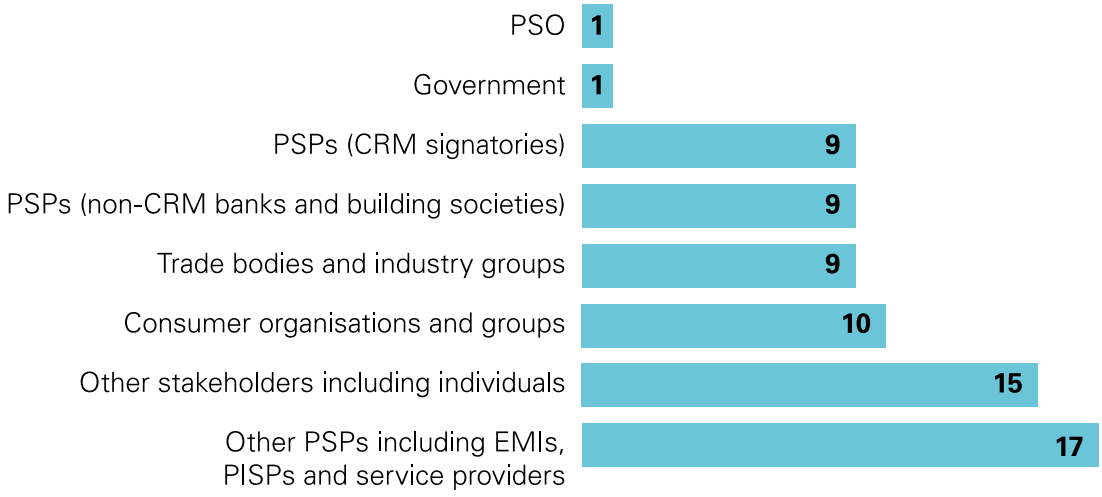
Respondents broadly supported our ambition to drive action to further prevent APP fraud. Consumer groups strongly supported the policy while industry expressed mixed views on its detail.

This chapter summarises stakeholders' views and responds to key themes identified through our September 2022 consultation. It includes a thematic analysis of the policy risks raised by respondents.

Respondents' views on the September 2022 consultation

4.1 We received 71 written responses to the consultation from a wide range of stakeholders across industry, trade bodies, consumer groups, individuals, and other stakeholders (see Figure 6).[25] We engaged extensively with stakeholders during the consultation, hosting or attending over 25 events including roundtables, discussions with trade bodies, appearances at conferences, and a lived experience workshop for consumers.

Figure 6: Respondents to the consultation divided into eight groups



4.2 In developing the policy framework for the new reimbursement requirement, we have listened to stakeholders and considered the diverse views they provided during our consultation from September to November 2022. This includes all formal submissions through the consultation process and informal submissions through industry events

25 We have provided a list of respondents and link to their published responses (where made available) as part of the separate Annex 3.

and wider engagement. We have evaluated the evidence provided (including alternative proposals for key policies) and adopted solutions judged to best achieve our strategic objectives. The separate Annex 3 provides a more detailed question-by-question response and a list of respondents.

'We believe these proposals could have a huge impact in reducing the financial and related emotional impact of APP fraud on victims if it leads to fairer decision-making by payment service providers and helps incentivise better reporting and prevention measures across industry.'

Which? Response to Consultation CP22-4, December 2023

4.3 **Consumer Groups and Organisations** (ten responses). Consumer groups and organisations were the strongest in acknowledging the benefits of the new reimbursement requirement. Some respondents questioned several of the detailed policies. Among their concerns were that the minimum threshold and claim excess could exclude those most at risk of harm, and that the 13-month time limit for victims to claim could exclude longer investment APP fraud cases. Some pressed us to expand the scope of the proposals to other payment systems including 'on us' payments.

4.4 **PSPs – CRM Code signatories** (nine responses representing eight of the ten Code signatories[26]). Code signatories had mixed views of the new reimbursement requirement. Most acknowledged the additional benefits for victims of APP fraud but disagreed with many of the detailed proposals. The 48-hour time limit to reimburse victims was seen as impractical. Several respondents said gross negligence was too high a bar for the customer standard of caution. Respondents were strong supporters of fighting APP fraud across the whole ecosystem and urged more upstream action, with additional legislation against this kind of fraud.

4.5 **PSPs – Banks and Building Societies (not CRM Code signatories)** (nine responses). Banks and building societies that have not signed up to the CRM Code had a wide range of views of the new reimbursement requirement, including strong support from industry innovators (TSB) to significant concerns from neo-banks. Building societies were keen for clarity on the scope of the policy. Neo-banks supported our objectives but disagreed with many of the detailed policies. They generally sought an iterative roll-out of the requirements and argued for more data-driven approaches including a risk-based approach to sharing the cost of reimbursement between PSPs. Some smaller business banks raised competition concerns, noting that the new policy may lead banks to reduce the services available to higher-risk businesses within its scope.

4.6 **PSPs – Other PSPs, including electronic money institutions (EMIs), payment initiation service providers (PISPs) and other financial service providers** (17 responses). EMIs and PISPs had split views. Some agreed that PIS-transactions should fall within the scope of the new policy (as long as the PISP was not liable to reimburse). Others, concerned that PSPs would place additional restrictions on PIS transactions, preferred to remain outside its scope. Indirect Access Providers (IAPs) and firms providing financial services to other PSPs pressed for the reimbursement obligations to be set directly on indirect participant PSPs.

26 HSBC responded alongside HSBC UK.

> ***'UK Finance and its members feel strongly that while a necessary step, a reimbursement model alone will not slow the UK's growing epidemic of scams, nor prevent the non-financial impacts on customers and industry'***
>
> *UK Finance. Response to Consultation CP22-4, December 2023*

4.7 **Trade bodies and industry groups** (nine responses). These reflected their members' diverse views on the policy. One of the largest, UK Finance, recognised reimbursement as a necessary step but argued wider action across the fraud ecosystem is needed. Most trade bodies and industry groups echoed this. A few respondents were less supportive of the proposals arguing that they would have disproportionate negative impacts on competition, customers and innovation. Most trade bodies and industry groups raised concerns that gross negligence was too high a bar for the customer standard of caution. They argued that PSPs needed more time to assess claims and reimburse victims, and they wanted a maximum limit on each claim.

4.8 **Payment system operator** (one response). Pay.UK, which operates Faster Payments, supported our ambition and said it was ready to play its role in implementing the policy. Pay.UK advocated for a PSR direction on PSPs to require them to reimburse and a further direction to require the implementation of Faster Payments rules to reflect that requirement.

> ***'We will work with the PSR and the payment firms to put effective reimbursement arrangements in place for FPS payments as soon as possible. It will be key for the industry to work together to ensure an effective regime is implemented to the timelines set out by HM Treasury and the PSR.'***
>
> *Pay.UK. Response to Consultation CP22-4, December 2023*

4.9 **Government Banking** (one response). Government Banking (HMRC) supported the proposals including many of the detailed policies. They acknowledged that it was a balanced approach. We are also continuing regular engagement with government via the Treasury, the Department for Culture, Media and Sport, and the Home Office to drive action across the wider fraud ecosystem (see Chapter 3).

4.10 **Other stakeholders** (15 responses). This group represented the widest range of stakeholders, including individuals, financial fraud solution providers and other interested parties. Many of the views presented were reflected in other stakeholders' submissions. We have also considered the specialist views put forward by these stakeholder's alongside other feedback.

Further views on our proposals

4.11 **Alternative proposals from industry**. In addition to the formal consultation responses, UK Finance provided an alternative proposal on the customer standard of caution, an industry-wide upper and lower threshold for claims, and an expanded timeline for reimbursement. UK Finance also encouraged the use of PSR directions instead of relying fully on Faster Payments rules. NatWest also proposed an alternative prevention model. In developing our final policy framework, we assessed these proposals alongside the consultation responses.

4.12 **Parliamentary engagement on our proposals**. We welcome the constructive and thorough engagement of the Treasury Sub-Committee on Financial Service Regulations. This included a hearing in December 2022 and subsequent correspondence, which focused on the proposed minimum threshold and the role of Pay.UK. We also considered and reviewed the findings of the 2022 House of Lords report, *Fighting Fraud: Breaking the Chain*.

Key themes from the consultation

4.13 We have identified key themes raised by stakeholders in response to our consultation proposals. In Table 3, we summarise their arguments, and our view on whether these would lead to more success for our objectives, including effective incentives to prevent fraud.

Table 3: Key themes raised by respondents

Key theme		Stakeholders' views	Our view
General themes			
1	**Reimbursement is a 'downstream' action and should be supported by 'upstream' action**	Many respondents said reimbursement should be supported with upstream action – for example, enacting the Online Safety Bill and providing additional customer education.	We agree reimbursement is only one part of a wider approach to effectively fight APP fraud, but the payment industry has a key role in stopping the use of the financial system to facilitate fraud. We outline our engagement and approach to the wider fraud ecosystem in Chapter 3.
2	**Additional legislative change must strengthen PSPs ability to prevent APP fraud**	Industry advocated for legislative changes to: • allow PSPs to intervene or slow payments (amendments to Payment Services Regulations 2017: 86 and 89) • unlock data sharing (passing the Economic Crime and Corporate Transparency Bill) • provide legislative protections for the repatriation of funds	In principle, we agree that further action would support a risk-based approach to payments. The Treasury is examining the best way to allow PSPs to achieve this. See Chapter 3 for our view on creating a wider statutory framework to support the new reimbursement requirement.

Key theme		Stakeholders' views	Our view
3	**The policy will be positive for victims of APP fraud**	Respondents broadly agreed that reimbursement will provide additional protections for customers and alleviate some of the hardship APP fraud causes.	We agree. Reimbursement will provide a step-change in protections for customers and prevent innocent victims from losing life-changing sums of money.
Policy-specific themes			
4	**Gross negligence is too high a bar for the customer standard of caution**	Industry generally argued that gross negligence was too high a bar for the customer standard of caution. Many industry respondents claimed it will: • increase moral hazard by removing customer responsibility when making payments • increase fraud as customers take less care, more criminals target the UK or more customers become complicit in fraud • significantly increase friction in the payment journey for legitimate transactions Consumer groups and organisations strongly disagreed with these arguments. They generally agreed gross negligence was the right level for the customer standard of care. They recognised that reimbursement would not be automatic, and that no customer would want to be a victim of APP fraud.	We have tested gross negligence against a range of alternative standards proposed in consultation responses. For the customer standard of caution, we see no credible alternative to gross negligence that would likely meet our objectives. Annex 3, Question 4 gives further details of our analysis. Table 4 acknowledges the moral hazard risk raised by industry.
5	**Further guidance on gross negligence would support effective implementation**	Respondents broadly agreed that additional guidance would help PSPs and customers to better understand the concept of gross negligence and what it means in practice.	We agree with the arguments and will develop additional guidance on the customer standard of caution (gross negligence) to be published in Q4 2023.

Key theme		Stakeholders' views	Our view
6	**In the long term, the policy should be set in legislation.**	Several respondents advocated for the policy to be set in legislation to drive consistency and mitigate the risk of fraud migrating to other payment systems.	Legislation has potential benefits, but we believe that Faster Payments rules and PSR directions, with their additional flexibility, are better suited to implementing and evolving the new reimbursement requirement.
7	**48 hours is not enough time for PSPs to reimburse customers**	A wide range of respondents, including some consumer groups and most PSPs, feared that the 48-hour time limit is not enough time for PSPs to gather evidence and reach the best outcome for victims. PSPs were especially concerned over whether the time limit would apply outside normal business hours.	We agree with the arguments presented and have increased the time limit to five business days with a 'stop the clock' provision. This will provide victims with reimbursement more quickly than the 15-day time limit under the CRM Code.
8	**There should be a maximum value of reimbursement for claims**	Industry advocated for a maximum level of reimbursement for individual claims in line with other customer protections in payment systems. Respondents highlighted the £85,000 cap under the Financial Services Compensation Scheme (FSCS) and the £375,000 cap (as of December 2022) for Financial Ombudsman Service claims.	We will bring the new reimbursement in line with other customer protections in the payment landscape and introduce a maximum level of reimbursement for APP fraud claims (by value). We will consult on the appropriate maximum level of reimbursement for individual claims in Q3 2023.

Key theme		Stakeholders' views	Our view
9	**It is unclear how the proposed minimum threshold for claims and claim excess will work together, and whether they are set at the appropriate level**	Opinion on the minimum threshold varied significantly. Several respondents warned that fraud could migrate below whatever level was set disadvantaging more financially vulnerable customers. Others argued that a minimum threshold was important to encourage customer caution. Respondents generally felt the proposed £35 excess would likely increase the administrative burden for PSPs while failing to encourage appropriate customer caution and making it unclear for victims what reimbursement they would be entitled to.	We have removed the separate minimum threshold for claims and will consult on the appropriate level for a claim excess. A maximum claim excess (set at the appropriate level) will be clearer to customers and so will encourage appropriate caution. It will also be easier for PSPs to administer. The claim excess will not apply to vulnerable customers (see Chapter 2).
10	**The obligation to reimburse should be placed directly on indirect participants and not via Indirect Access Providers (IAPs)**	Several respondents highlighted that placing any additional obligations on IAPs would impact their risk appetite and could reduce the services available to indirect Faster Payments participants.	We have refined our approach to implementation to place obligations directly on all PSPs within the scope of the policy (see Chapter 6).

Policy risks

4.14 Many respondents felt the proposals would achieve some of the intended outcomes but warned of potential risks. These broadly align with the policy risks we highlighted in our September consultation. Industry respondents generally saw the risks as more likely and/or problematic than we did but could provide no firm quantitative evidence. We have assessed respondents' limited evidence under five themes.

Table 4: Policy risks raised by respondents

Key theme	Stakeholders' views	PSR's view
The policy may have a negative impact on firms	The additional costs and liability for PSPs could lead to market exits, threaten innovation, and harm international investment in the UK market.	We have assessed the impact on firms in our updated cost benefit analysis (see the separate Annex 4). We are working with the FCA to manage potential negative effects to firms. We will set a reasonable implementation deadline so PSPs can prepare and invest in prevention ahead of day one of the new reimbursement requirement.
The policy may increase the likelihood of moral hazard	Industry raised significant concerns that the policy would increase the risk of moral hazard. Evidence was limited to some international comparisons, limited consumer research and one case study. Consumer organisations felt strongly that there was no evidence the policy would increase the risk of moral hazard. Instead, they highlighted the emotional impact and personal inconvenience of being scammed.	We have heard assertions but received no quantitative evidence as to whether the new reimbursement requirement will impact the likelihood of moral hazard. However, we recognise it is a valid risk that should be managed, and we believe customers and PSPs share the risk. PSPs should put effective protections in place and can take many actions to prevent APP fraud, such as introducing more effective warnings when customers are making payments. Recognising that many victims are socially engineered into being scammed, we have introduced policies to encourage customer caution, where appropriate, including: • **A customer standard of caution (gross negligence):** Gross negligence does not mean automatic reimbursement and provides an appropriate incentive for customers to take care. • **A claim excess (at a level subject to consultation):** We judge this is appropriate to manage the risk of moral hazard alongside the many actions PSPs can take to prevent APP fraud. Our research using a lived experience workshop suggested that consumers do not expect the policy to change how they currently spend money, make payments or review and approve requests for payment.

Key theme	Stakeholders' views	PSR's view
Implementing the policy may have a negative impact on the development of the NPA and expansion of open banking payments	Pay.UK does not have the means and capacity to manage implementation alongside the New Payments Architecture (NPA) and expansion of Confirmation of Payee (CoP).	Pay.UK's Board is supportive of implementation of reimbursement. We are continuing to engage with Pay.UK to agree the details of their role in implementing the new reimbursement requirement alongside wider priorities.
	The new reimbursement requirement could increase the costs of Faster Payments and make them uncompetitive in comparison to card payments.	Only limited evidence was provided on the potential increase in Faster Payments costs. We do not expect a significant increase in cost and will monitor this as part of implementation. We believe that greater customer protections will increase customer confidence in Faster Payments (see Chapter 2).
The policy may negatively impact service users	Payment friction and refusals will increase significantly and impact legitimate payments.	We recognise that 'good' friction can be a useful tool in preventing fraud. We do not support blanket friction where there is a high likelihood of disrupting legitimate payments. We see data as critical to driving more targeted, risk-based interventions to stop fraud (see Chapters 1 and 3). Previous claims that new policies, (such as the introduction of Strong Customer Authentication) would introduce too much friction have proven unfounded.
	There will be a reduction in services available to customers. Higher-risk customers could lose access to banking services (also known as 'de-banking').	Several PSPs dismissed the risk of the full removal of services or 'de-banking' users as they reported that there is no typical high-risk service user for APP fraud. We accept that there is a risk that some PSPs may conclude certain groups, which would not be classed as vulnerable, are higher risk and subsequently implementing greater friction with payments or the removal of some services. Based on the evidence provided through the consultation, we think this risk is manageable and we will consider this as part of our post-implementation review (see Chapter 8).

Key theme	Stakeholders' views	PSR's view
	Costs will increase for service users.	We expect the UK's thriving competitive payments market to mitigate any potential cost increases. we will consider this as part of our post-implementation review (see Chapter 8).
The policy will not reduce the level of fraud within the UK (and may increase fraud)	CRM Code signatories have been investing in fraud prevention since 2019 and the number of reported APP fraud cases increased.	Signatories represent only ten groups of the 1500+ PSPs in the market and the Code only applies consistent incentives to sending PSPs. The new reimbursement requirement sets sector-wide consistent minimum standards, and we have already begun to see receiving PSPs tighten up their controls in response to the new requirement. In the short to medium term, we expect reported APP fraud incidents to increase as victims become aware of the new reimbursement requirement and data is collected by more PSPs. Over time, we expect total APP fraud incidents to decrease (see Figure 1, Chapter 1).
	Setting the customer standard of care at gross negligence, alongside the 48-hour time limit to reimburse customers will increase first-party fraud.	We have not received any quantitative evidence that the new reimbursement requirement will lead to an increase in first-party fraud. We will monitor this as part of implementation (see Chapter 6).
	Fraud will migrate to other channels including CHAPS	We are working with the Bank of England to define a model for reimbursement which reflects the unique characteristics of CHAPS, is simple to operationalise and creates comparable protections for customers. We will also continue to consider risks across different payment systems and, where necessary, address them with future action (see Chapter 2).

5 Key policies in practice

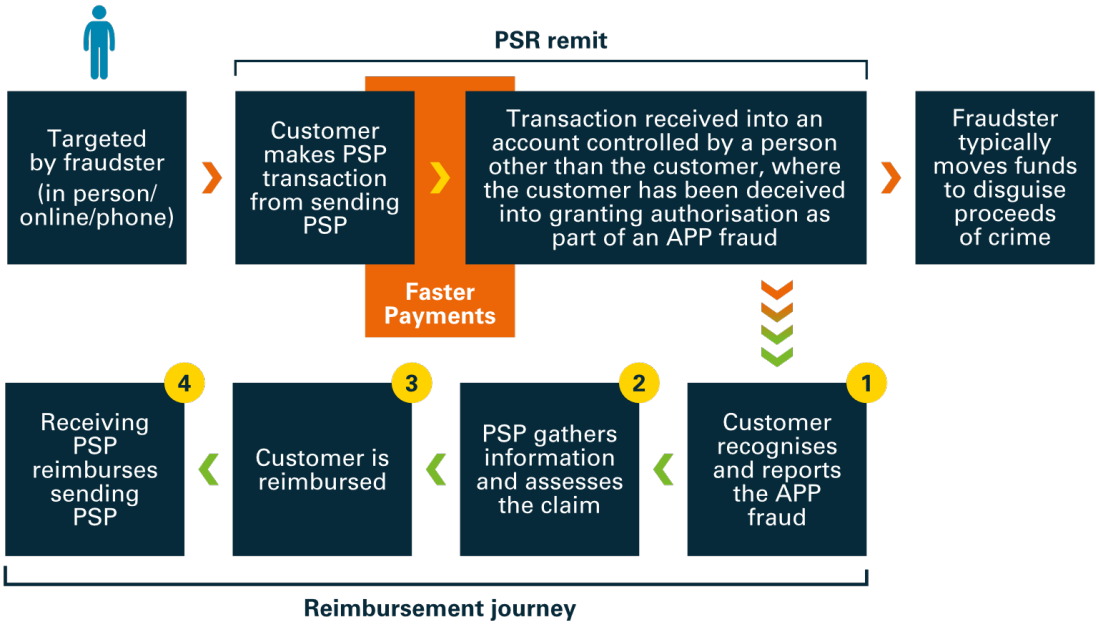
This chapter demonstrates how we expect the new reimbursement requirement to work in practice, placing the ten key policies in the context of a case illustrating the four stages of the reimbursement journey

Typical APP fraud reimbursement journey

5.1 Every fraud is different, but a typical APP fraud involves multiple steps. The fraudster may recruit the victim on social media or by phone, before inducing them to make the payment or a series of payments. Any investigation, recovery of proceeds, reimbursement and prosecution then follow.

5.2 We have structured this chapter around the four stages of the APP fraud reimbursement journey set as steps 1 to 4 in Figure 7. This chapter does not provide detailed step-by-step guidance and we do not intend to provide it. Industry is best placed to determine how to operationalise the policies, though we will provide further regulatory guidance to clarify, where necessary. We expect PSPs to evolve their approach over time as more data becomes available and lessons are learned.

Figure 7: A typical APP fraud payment and reimbursement journey



1 – Customer reports the fraud

We want customers to report fraud as quickly as possible, improve communication between sending and receiving PSPs to drive repatriation of stolen funds and minimise the harm caused to victims through uncertainty.

Table 5: Key policies relevant for stage 1

1. Reimbursement requirement for APP fraud within Faster Payments	Sending PSPs must reimburse all customers who fall victim to APP fraud (noting the exceptions and limits set out in policies 3 to 10). See Chapter 2 for the scope of the policy. The reimbursement requirement does not apply to: • civil disputes • payments which take place across other payment systems • international payments • payments made for unlawful purposes
6. Minimum threshold:	There is no separate minimum value threshold for APP fraud claims under the new reimbursement requirement.
7. Maximum level of reimbursement:	There is a maximum level of reimbursement for APP fraud claims (by value) under the new reimbursement requirement. *We will consult on the appropriate maximum value for APP fraud claims and publish this in PSR guidance in Q4 2023.*
8. Time limit to claim:	Sending PSPs have the option to deny APP fraud claims submitted more than 13 months after the final payment to the fraudster.
10. Approach to 'multi-step' fraud cases:	The new reimbursement requirement applies to the Faster 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 case (see Chapter 2).

How will the policies work in practice?

5.3 Once a customer has recognised that they have fallen victim to APP fraud, they should report it to their PSP (the sending PSP) as quickly as possible (and within a maximum of 13 months of the last payment).

5.4 The sending PSP must notify the receiving PSP as quickly as possible of an APP fraud claim (near real-time). Where a PSP, 'knows' or 'suspects' that a person is engaged in money laundering or dealing in criminal property, they must submit a Suspicious Activity Report, and follow their legal obligations.[27]

27 National Crime Agency, *Introduction to Suspicious Activity Reports (SARs)* (March, 2021)

5.5 Customers should provide all relevant information to the sending PSP as soon as possible. The sending PSP can reasonably request evidence sufficient for them to assess the background to the claim. In circumstances where reasonable evidence is not provided by the customer, the sending PSP can reject the claim. The standard for reasonable evidence must be considered on a case-by-case basis.

5.6 The sending PSP will need to engage with their customer as they will likely have the most meaningful evidence about the incident. The sending PSP should capture the chronology and what the customer was seeing, doing and thinking, and if they were coached through stages of the payment journey. Information should be gathered as soon as possible after an incident, with the first touchpoint with the customer often the most important. The sending PSP should strive to have open-ended reporting processes which give staff the flexibility to ask the questions they feel are important for capturing the right details. Digital reporting systems could provide free-text options rather than just prescriptive prompts.

5.7 Firms must be responsive to customers' needs and understand that fraud incidents will impact people in different ways which may affect how they engage with their PSP. Where possible, firms should use a 'tell us once' approach to avoid customers having to repeatedly go over their story with different staff.

5.8 When assessing the claim, our expectation is that the sending PSP will communicate with the receiving PSP and consider any information provided by the receiving PSP as part of their assessment. For example, where the receiving PSP has evidence that the claim is a civil dispute, the receiving PSP should provide any relevant information in a reasonable time period.

5.9 We want to encourage more victims to report APP fraud cases to the police. This will improve data on APP fraud, support law enforcement efforts and support our overall objective of preventing APP fraud. PSPs can encourage victims to contact the police and request a crime reference number. There may be cases where this is not possible, for example, if a customer has vulnerabilities which would make this difficult. In these cases, the sending PSP should support the customer in notifying the police. Failure to notify the police cannot be considered a reason for denying a reimbursement claim.

5.10 Once the customer has reported the fraud to the sending PSP, this will start the time limit of five business days to assess the customer's claim (see stage 2). The sending PSP is responsible for assessing the claim and reimbursing their customer.

5.11 To reduce the uncertainty and worry caused to victims, the sending PSP should provide an initial indication to their customer of whether their claim falls within the scope of the new reimbursement requirement. This should happen at the time of the claim, where possible.

No separate minimum threshold for claims

5.12 There is no separate minimum threshold for claims under the new reimbursement requirement (see Chapter 3).[28]

Maximum level of reimbursement for claims

5.13 There is a maximum level of reimbursement for claims under the new reimbursement requirement (by value). The maximum level of reimbursement does not prevent PSPs from voluntarily reimbursing customers above this limit. We will consult on the appropriate level in Q3 2023 and will publish this in PSR guidance in Q4 2023.

5.14 This aligns this policy with other customer protections in the payment market in having a maximum claim limit and establishes clear parameters for the scope of the new reimbursement requirement, allowing firms to understand their liability. Claims should include all relevant payments to a specific APP fraud case. Payments made prior to the start date for the new reimbursement requirement are not covered by it. See Chapter 2.

5.15 If a customer has been defrauded above the maximum level of reimbursement for claims, they are entitled to reimbursement up to this amount under the new reimbursement requirement.

Time limit to report the fraud

5.16 The sending PSP has the option to deny a claim which is reported more than 13 months after the final payment to the fraudster. This is the same as the time limit for claims for refunds of unauthorised payments under the Payment Services Regulations 2017.

5.17 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 a pursue a claim via the Financial Ombudsman Service (FOS) 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 FOS's scope or processes.

28 We will consult on the appropriate level for the claim excess and note that this could act as a de facto minimum threshold depending on how it is structured and implemented.

Key actions

Every fraud is different, but these are the actions we would typically expect to see. This table a is a summary of the actions set out above for stage 1.

Party	Action
Customer	• Once a customer has recognised that they have fallen victim to APP fraud, they should report it to their PSP as quickly as possible (and within a maximum of 13 months of the last payment). • The customer should report the APP fraud to the police, receive a crime reference number and provide this to the PSP if requested (failure to notify the police cannot be considered a reason for denying a reimbursement claim). • The customer should gather any evidence they have to support their claim and provide this to the sending PSP. Sending PSPs can reasonably request evidence sufficient for them to assess the background to the claim.
Sending PSP	• Communicate to customers on how to report APP fraud including what the process involves and any time limits. • Notify the receiving PSP as quickly as possible (period to be defined) of an APP fraud claim (see Chapter 6). • Provide an initial indication of whether the reported payment is likely to be in-scope of the reimbursement requirement.
Receiving PSP	• Act on the notification of an APP fraud claim from the sending PSP (in line with legal obligations). • Provide any relevant information to the sending PSP.

2 – PSP assesses the claim

We want PSPs to make effective and accurate decisions in a timely way.

Table 6: Key policies relevant for stage 2

1. Reimbursement requirement for APP fraud within Faster Payments	Sending PSPs must reimburse all customers who fall victim to APP fraud (noting the exceptions and limits set out in policies 3 to 10). See Chapter 2 for the scope of the policy. The reimbursement requirement does not apply to: • civil disputes • payments which take place across other payment systems • international payments • payments made for unlawful purposes
3. Exceptions for APP fraud claims	There are two exceptions to reimbursement (noting the other policies) under the new reimbursement requirement: • where the customer has acted fraudulently ('first-party fraud') • where the customer has acted with gross negligence. This is the customer standard of caution for APP fraud claims.
4. Time limit to reimburse	Sending PSPs must reimburse customers within five business days under the new reimbursement requirement. For specific actions, the sending PSP can 'stop the clock' (see Box 5, Chapter 5).
9. Treatment of vulnerable customers	The customer standard of caution and claim excess must not be applied to vulnerable customers.

How will the policies work in practice?

5.18 The sending PSP is best placed to assess the claim and decide on the evidence available. The sending PSP must assess a customer's APP fraud claim and reimburse their customer within five business days.

5.19 We expect sending PSPs to take a proportionate approach to validating claims based on the relative complexity and value of the fraud. We do not expect them to undertake complex or resource intensive investigations for simple APP fraud claims. The information for most cases should be gathered through the customers' initial claims.

5.20 In assessing the claim, we expect PSPs will, proportionally to the value and complexity of the claim:

- provide an initial indication of whether the claim is within the scope of the reimbursement requirement (see 5.11)
- assess whether there is any evidence of first-party fraud (see 5.23)
- assess customer vulnerability (see 5.26 to 5.28).
- assess whether there is any evidence of gross negligence (see 5.23)

5.21 For more complex claims, the sending PSP may need to gather additional information from the victim, receiving PSP or law enforcement.

5.22 The sending PSP is permitted to apply the 'stop the clock' provision for specific actions (see Box 5 for a list of what 'stop the clock' can be used for). The 'stop the clock' provision should be used in proportion to the value and complexity of the claim. PSPs will be monitored on the timeliness of reimbursement as part of the monitoring regime (see Chapter 6).

Exceptions to reimbursement for APP fraud claims

5.23 There are two exceptions to reimbursement for APP fraud claims under the new reimbursement requirement:

- **Where the customer has acted fraudulently ('first-party fraud'):** It is not the purpose of the new requirement to reimburse customers who have been complicit in fraud. This exception applies to all customers.
- **Where the customer has acted with gross negligence:** Gross negligence is already an exception to PSP liability for unauthorised frauds under section 77(3) of the Payment Services Regulations 2017 and is one of the exceptions to reimbursement in the CRM Code. We agree with the position in FCA guidance that gross negligence is a high standard: 'In line with the recitals to PSD2, we interpret 'gross negligence' to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness'. Where suspected, the burden of proof is on the PSP to prove gross negligence. This exception does not apply to vulnerable customers (see Chapter 2).

5.24 As set out in Chapter 2, the new reimbursement requirement does not apply to civil disputes, such as where a customer has paid a legitimate supplier for goods or services but has not received them, has found them defective in some way, or is otherwise dissatisfied with the supplier. Civil disputes do not meet our definition of an APP fraud payment as the customer has not been deceived. The law protects consumer rights when purchasing goods and services, including through the Consumer Rights Act.[29]

29 Gov.UK, *Consumer protection rights*

5.25 In response to the feedback, we received in our consultation, we will develop further guidance on the customer standard of caution (gross negligence), including an industry consultation in Q3 2023 (see Box 4).

Box 4: Customer standard of caution (gross negligence) guidance

- We have reflected on the feedback we received in our consultation and are preparing to publish guidance to support the new reimbursement requirement. This guidance will help drive consistent customer outcomes and we will consult on a draft of this guidance in Q3 2023.
- The PSR has formed a steering group with the FCA and FOS to help advise on the guidance. This will help ensure that the guidance aligns with existing rules and guidance for firms. We will also be engaging with key stakeholders such as firms, their representatives, consumer groups, and the government as we develop the guidance.
- The guidance will reinforce our expectation that PSPs must reimburse APP fraud victims in most cases.

Assessing vulnerability

5.26 The FCA has set out comprehensive guidance for firms on the fair treatment of vulnerable customers.[30] We agree with the FCA's position and want to see the fair treatment of vulnerable customers embedded as part of a healthy culture throughout firms. This includes firms' understanding the nature and scale of characteristics of vulnerability that exist in their target market and customer base, being able to spot signs of vulnerability, and setting up systems and processes in a way that will support and enable vulnerable consumers to disclose their needs.

5.27 As part of assessing an APP fraud case, the sending PSP should assess the customer's situation and any potential vulnerability in line with the FCA's guidance: 'Firms should consider consumers' vulnerability and capacity to make decisions when deciding how to treat consumers who have been victims of scams or fraud'.[31]

5.28 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 definition of vulnerability (see Chapter 2). This aligns with the FCA's guidance.

30 FCA, *FG21/1 Guidance for firms on the fair treatment of vulnerable customers* (February 2021)

31 FCA, *FG21/1 Guidance for firms on the fair treatment of vulnerable customers* (February 2021)

Rejected claims

5.29 If the sending PSP decides to refuse a claim and the customer does not agree with the outcome, the customer may have the opportunity to a pursue a claim via the FOS for 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.

Key actions

Every fraud is different, but these are the actions we would typically expect to see. This table a is a summary of the actions set out above for stage 2.

Party	Action
Customer	• The customer should provide all relevant information on the APP fraud to the sending PSP.
Sending PSP	• Assess whether there is any evidence of first-party fraud. • Assess customer vulnerability. • Assess whether there is any evidence of gross negligence. • Assess whether the claim qualifies.

Box 5: Explaining the 'stop the clock' provision

Sending PSPs must reimburse customers within five business days but can 'stop the clock' to:

- gather additional information from victims to assess the claim
- gather additional information from victims to assess vulnerability
- where relevant, verify that a claims management company is submitting a legitimate claim – for example, validating the authorisation from an individual to submit a claim
- in cases where first-party fraud is suspected, gather additional information from the receiving PSP and/or law enforcement or other relevant parties[32]
- in cases where multi-step fraud cases have occurred, gather additional information from the other PSPs involved

There is no limit to how many times a PSP can use the 'stop the clock' provision[33] but it should be used in proportion to the value and complexity of the claim.

32 Where a PSP, 'knows' or 'suspects' that a person is engaged in money laundering or dealing in criminal property, they must submit a Suspicious Activity Report, and follow their legal obligations.

33 Subject to other requirements in legislation including Payment Services Regulation 2017 Regulation 101 (7). Where it applies, it limits the resolution period to 35 days.

Example of 'stop the clock': Ms Smith rings her bank to report she has fallen victim to a £10,000 romance APP fraud which has taken place over the past six months. As part of assessing the claim, the bank asks for any further documents Ms Smith can provide including messages between her and the fraudster to verify the claim. Ms Smith notes that she is exhausted and will send photos of the messages the next day. The bank provides Ms Smith with additional information about victim support services and she ends the call.

The bank is entitled now to 'stop the clock' pending receipt of the relevant information from the customer (Ms Smith). Once the information has been provided by the customer, the 'clock' continues counting down to the five-business-day deadline.

Day and date	Action
Tuesday 21 March 2023	Ms Smith reports the APP fraud and the 'clock is stopped' pending additional information
Wednesday 22 March 2023	Ms Smith provides the additional information in the morning to their PSP
Thursday 23 March 2023	
Friday 24 March 2023	
Saturday 25 March 2023	Non-business day (not counted towards the five-day limit)
Sunday 26 March 2023	Non-business day (not counted towards the five-day limit)
Monday 27 March 2023	
Tuesday 28 March 2023	Deadline to reimburse Ms Smith

3: Customer is reimbursed

We want customers to clearly understand what they are entitled to receive.

Table 7: Key policies relevant for stage 3

1. Reimbursement requirement for APP fraud within Faster Payments:	Sending PSPs must reimburse all customers who fall victim to APP fraud (noting the exceptions and limits set out in policies 3 to 10). See Chapter 2 for the scope of the policy. The reimbursement requirement does not apply to: • civil disputes • payments which take place across other payment systems • international payments • payments made for unlawful purposes
5. Claim excess:	Sending PSPs have the option to apply a claim excess under the new reimbursement requirement. *We will consult on the appropriate level for this and publish the maximum excess in PSR guidance in Q4 2023.*
6. Minimum threshold:	There is no separate minimum value threshold for APP fraud claims under the new reimbursement requirement.

7. Maximum level of reimbursement:	There is a maximum level of reimbursement for APP fraud claims (by value) under the new reimbursement requirement. *We will consult on the appropriate maximum value for APP fraud claims and publish this in PSR guidance in Q4 2023.*

How will the policies work in practice?

5.30 Once the sending PSP has completed its assessment of the claim, it should notify the customer of the outcome and the reimbursement they will receive. PSPs should reimburse customers back to the account which made the payment and avoid introducing any unnecessary friction.

Claim excess

5.31 The sending PSP has the option to apply a claim excess. The claim excess is an effective way to manage the potential risk of increasing the likelihood of moral hazard alongside the many actions PSPs can take to prevent APP fraud. We will set out the level of the claim excess after consultation in Q3 2023. It will work like a claim excess in insurance. The claim excess must not be applied to vulnerable customers (see Chapter 2).

Key actions

Every fraud is different, but these are the actions we would typically expect to see. This table is a summary of the actions set out above for stage 3.

Party	Action
Sending PSP	• Reimburse the customer within the five business-day deadline after deducting any optional excess.

4 – Receiving PSP reimburses sending PSP

We want to improve communication between PSPs, and for receiving PSPs to send their share of the reimbursement to sending PSPs in an effective, timely way.

Table 8: Key policies relevant for stage 4

2. Sharing the cost of reimbursement:	Receiving PSPs must pay sending PSPs 50% of the reimbursement that the sending PSP paid to the customer. A time period will be set by Pay.UK with an ultimate backstop to ensure receiving PSPs reimburse sending PSPs.

How will the policies work in practice?

5.32 Neither sending nor receiving PSPs can, at present, reliably detect 100% of APP fraud, but both can take steps to detect potential frauds. If they suspect fraud, they can refuse payment orders or block accounts. Receiving PSPs need adequate financial incentives to do more to detect fraud and prevent fraud losses, because they provide the accounts that fraudsters control and use for APP fraud.

5.33 The sending PSP is responsible for assessing the claim and determining whether a claim is valid and in scope (and therefore determining whether receiving PSP is liable for 50% of the claim). Having reimbursed the customer, the sending PSP can require 50% of the amount paid to the customer from the receiving PSP. The receiving PSP must pay this subject to 5.34.

5.34 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. In practice, this could include:

- If the sending PSP chose not to apply the maximum claim excess, the sending PSP can only require 50% of the amount less the maximum excess from the receiving PSP. The receiving PSP is only liable for 50% of an in-scope claim less the maximum claim excess.
- The sending PSP can only require up to 50% of the maximum level of reimbursement under the new reimbursement requirement in the event they decide to voluntarily reimburse the customer additional funds (above the maximum level of reimbursement).
- If the sending PSP chose to voluntarily reimburse a claim submitted after the 13-month time limit to claim, the sending PSP cannot require any of the reimbursement back from the receiving PSP.
- If the sending PSP chose to voluntarily reimburse a claim which was assessed to be first-party fraud, or the customer had acted with gross negligence (excluding where a customer is vulnerable) the sending PSP cannot require any of the reimbursement back from the receiving PSP.

5.35 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.

Refining the 50:50 cost of reimbursement in future

5.36 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.

5.37 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.

5.38 This is part of Pay.UK's role to evolve the rules over time in line with refinements to the policy, for example as data and technology improve (see Chapter 6). This will support the principle that the firms which invest and are better at preventing APP fraud should be recognised.

Disputes

5.39 If disputes arise, 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.

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

Allocation of repatriated funds

5.41 Repatriation of APP fraud losses occurs where the receiving PSP is able to detect, freeze and return funds stolen as part of APP fraud.

5.42 Where a receiving PSP recovers and is able to repatriate funds, and when the customer has already been reimbursed by the sending PSP, repatriated funds should be shared between the sending and receiving PSPs to cover what they paid out as reimbursement, reflecting the split adopted by PSPs at the time of reimbursement.

5.43 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.

5.44 Rarely, a sending PSP will have reimbursed a customer and received 50% of the claim from the receiving PSP only to discover the customer's claim was not covered by the reimbursement requirement – for example a case of first-party fraud. In such a case, the sending PSP should follow its usual processes to repatriate funds and must refund the 50% to the receiving PSP.

Key actions

Every fraud is different, but these are the actions we would typically expect to see. This table a is a summary of the actions set out above for stage 4.

Party	Action
Sending PSP	• In the event costs are fully defrayed through repatriated funds, send any additional funds to the victim.
Receiving PSP	• Reimburse the sending PSP in line with the guidance provided by Pay.UK. • Where successful in repatriating funds, send 50% of the repatriated funds to the Sending PSP.

6 Putting reimbursement in place

We want to establish an agile set of rules for APP fraud that can evolve over time to address the ever-changing fraud threat. All PSPs using Faster Payments will be required to comply with those rules. Pay.UK as the payment system operator will manage and maintain those rules.

Our approach to implementing the requirements

6.1 Our vision is for Pay.UK to run Faster Payments in a way that adequately protects customers, and prevents fraud from entering the system, as set out in Chapter 1. If account-to-account payments are to continue to evolve and provide a wider choice of payment types, as part of securing our aim for greater competition between payment systems, customers will need to have sufficient confidence in the safety of Faster Payments. Customer protection is central to this aim.

6.2 As the independent payment system operator (PSO), our view is that Pay.UK is the appropriate body to make, maintain, refine, monitor and enforce compliance with comprehensive scheme rules to ensure that PSPs have appropriate incentives to prevent fraud and protect customers. The alternative would be for the PSR to give directions to PSPs and limit Pay.UK's role in making rules that implement those directions. But our view is that Pay.UK is the body with the operational oversight, expertise on system rules and ability to coordinate across participants needed to monitor participants' responses to the rules and respond flexibly through enforcement or changes to rules where necessary.

6.3 Scheme rules can be managed and refined more efficiently and quickly than regulatory instruments. As with other PSOs and system operators in other sectors, who manage their system rules and the consequences for breaking them, our view is that Pay.UK's rulebook is the most practical tool for addressing the harms from fraud across the payment system.

6.4 Looking forward, we expect Pay.UK will need to establish, maintain and enforce cross-market, operational arrangements in a number of areas, including as part of its role in assessing and enabling use cases for the NPA, such as account-to-account retail transactions. Our requirements on APP fraud provide an opportunity for Pay.UK to start moving towards this longer term role and develop greater expertise in this territory before the NPA is implemented. As far as possible, we want Pay.UK to take on this role from the outset of NPA implementation.

6.5 We will require Pay.UK to include the main requirements in the Faster Payments rules and it will be their role to evolve those rules over time, for example as data and technology improve.

6.6 However, Pay.UK is not currently able to take on this role fully. 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.

6.7 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 the PSR a role in enforcement to support Pay.UK. We will retain responsibility for some of the key requirements. We will look to hand over responsibility for some of these to Pay.UK in the future as it develops the capabilities required to achieve our long-term vision. Before doing so, we would review and consult on any subsequent changes to Pay.UK's role and implement these changes through appropriate legal instruments.

6.8 Responsibility for the requirements will fall into three categories:

Regulatory requirements set by the PSR

6.9 There are regulatory requirements that will remain within our control for the foreseeable future. These are:

- the reimbursement requirement
- the scope of reimbursement requirement

Requirements retained by the PSR initially, with the potential to become Faster Payments rules in the future

6.10 There are certain rules that we will retain control of initially but that we intend to hand over to Pay.UK when we deem it has sufficient capability to manage and enforce them (see 6.7). These are:

- maximum claim excess and the maximum level of reimbursement
- customer standard of caution (gross negligence) guidance

Requirements Pay.UK will be responsible for from day one

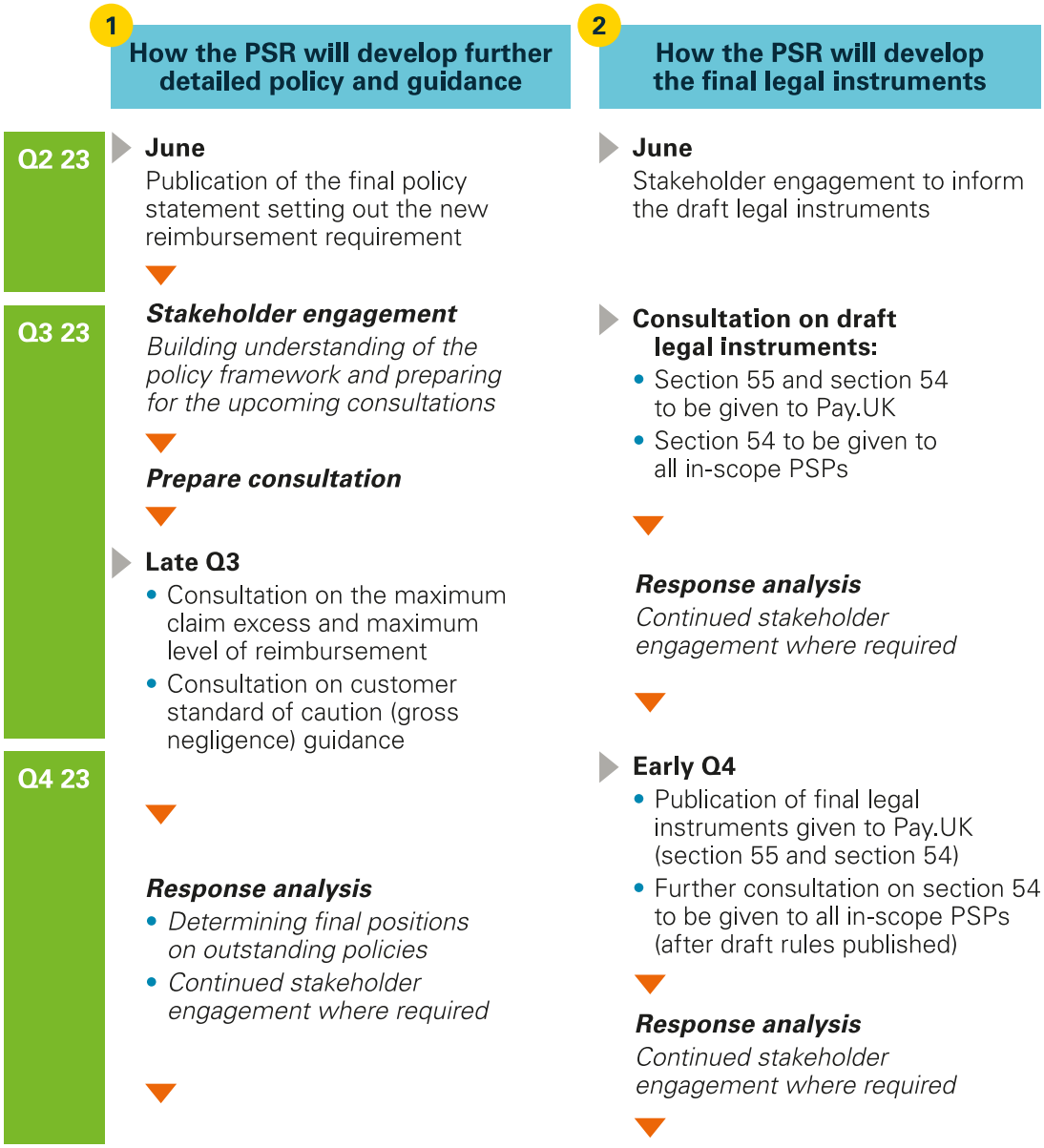
6.11 We want Pay.UK to take responsibility for ensuring all remaining rules function effectively from day one. These are:

- 50:50 cost allocation of reimbursement between sending and receiving PSPs
- an option for PSPs to refuse claims submitted after 13 months
- the five-business-day deadline for reimbursing customers
- the 'stop the clock' provision

6.12 To ensure that the rules deliver the intended policies, we will require Pay.UK to notify us of any proposed changes to the relevant reimbursement rules. Where proposed changes could have a material impact on the policy outcomes the reimbursement requirements are designed to achieve, we would expect to be closely involved in the assessment of those changes. In some cases, we may need to consider varying our section 55 requirement to enable changes to the rules.

6.13 Figure 8 sets out how we will engage stakeholders in implementing the new reimbursement requirement, including developing further detailed policy and PSR guidance.

Figure 8: Engagement roadmap on the new reimbursement requirement through 2023



Meeting our statutory obligation

6.14 The Financial Services and Markets Bill (FSMB) includes a duty for us to 'prepare and publish a draft of a relevant requirement for reimbursement' within six months of the FSMB becoming law.[34] We will use our statutory powers under section 54 and section 55 of the Financial Services (Banking Reform) Act 2013 (FSBRA) to implement the new reimbursement requirement via a combination of PSR directions and Faster Payments rules. This will drive effective implementation, ensure that all PSPs sending and receiving qualifying Faster Payments comply with the requirement or be held to account, and fulfil our statutory obligation set out in the bill.

6.15 Figure 9 provides a high-level summary of how the new reimbursement requirements will be set. This is outlined in more detail in paragraphs 6.16-6.21.

Faster Payments rules (rule change requirement under FSBRA section 55)

6.16 We will embed the reimbursement policies into the Faster Payments rules via a rule change requirement under section 55 of FSBRA. We will provide additional guidance and detail for some policies. The rule change requirement will specify a date by which the rules must be in place. Specifically, the Faster Payments rules will include:

- **Reimbursement requirement:** Sending PSPs must reimburse their customers who suffer APP fraud, except where the **customer standard of caution** is not met. We will set this standard and publish it in Q4 2023 in guidance on what constitutes the standard. This exception does not apply when the customer is vulnerable.
- **Claim excess:** The sending PSP can subtract an amount up to the maximum level of the claim excess from the amount reimbursed to the victim. We will publish the level of the claim excess in Q4 2023. The claim excess does not apply when the customer is vulnerable.
- **Maximum level of reimbursement:** The sending PSP is not obligated to reimburse above the maximum value level of a single APP fraud case. We will set the level and publish it in Q4 2023.
- **Time limit to claim:** The sending PSP is not obligated to reimburse any APP fraud where the customer submitted the claim more than 13 months after making the last payment in the case. Pay.UK is to keep the 13-month period under review.
- **Notifying the receiving PSP:** The sending PSP must notify the receiving PSP of any payment it has validated as being an APP fraud within a specified period from receipt of the claim from the customer (period to be determined). Pay.UK is to keep the period under review.
- **Sharing the cost of reimbursement:** A receiving PSP must send 50% of the cost of a reimbursement to the sending PSP within a deadline to be set by Pay.UK. Pay.UK is to lead work to consider how a more refined reimbursement cost allocation model could be developed.

34 UK Parliament, *Financial Services and Markets Bill* (March 2023), Clause 68.

- **Time limit to reimburse:** The sending PSP must reimburse a customer who falls victim to APP fraud within five business days, except when they 'stop the clock'. Pay.UK is to keep the five-day deadline under review. Sending PSPs can 'stop the clock' to:
  - gather additional information from victims to assess the claim
  - gather additional information from victims to assess vulnerability
  - where a claims management company is submitting a claim, verify that it is legitimate (for example, by validating that an individual authorised the company to submit a claim)
  - where first-party fraud is suspected, gather additional information from the receiving PSP and/or law enforcement or other relevant parties
  - where multi-step fraud has occurred, gather additional information from the other PSPs involved
- **Repatriation:** 50% of any funds that are stolen in an APP fraud but then recovered must be repatriated to the sending PSP.

Directions under section 54 of FSBRA

6.17 We will give a general direction to direct all in-scope PSPs (including indirect participants) to comply with the relevant Faster Payments rules and report data to Pay.UK. The general direction will place a regulatory obligation on both direct and indirect participants to reimburse customers and define the scope of which payments and customers are covered, while maintaining responsibility for the rules with Pay.UK. We intend to remove the requirement to comply with scheme rules and report data once we are satisfied this is no longer necessary to support Pay.UK's implementation and oversight of the reimbursement requirement.

6.18 We will also give a specific direction requiring Pay.UK to create and implement effective monitoring of PSPs in line with the rule change requirement and general direction we give.

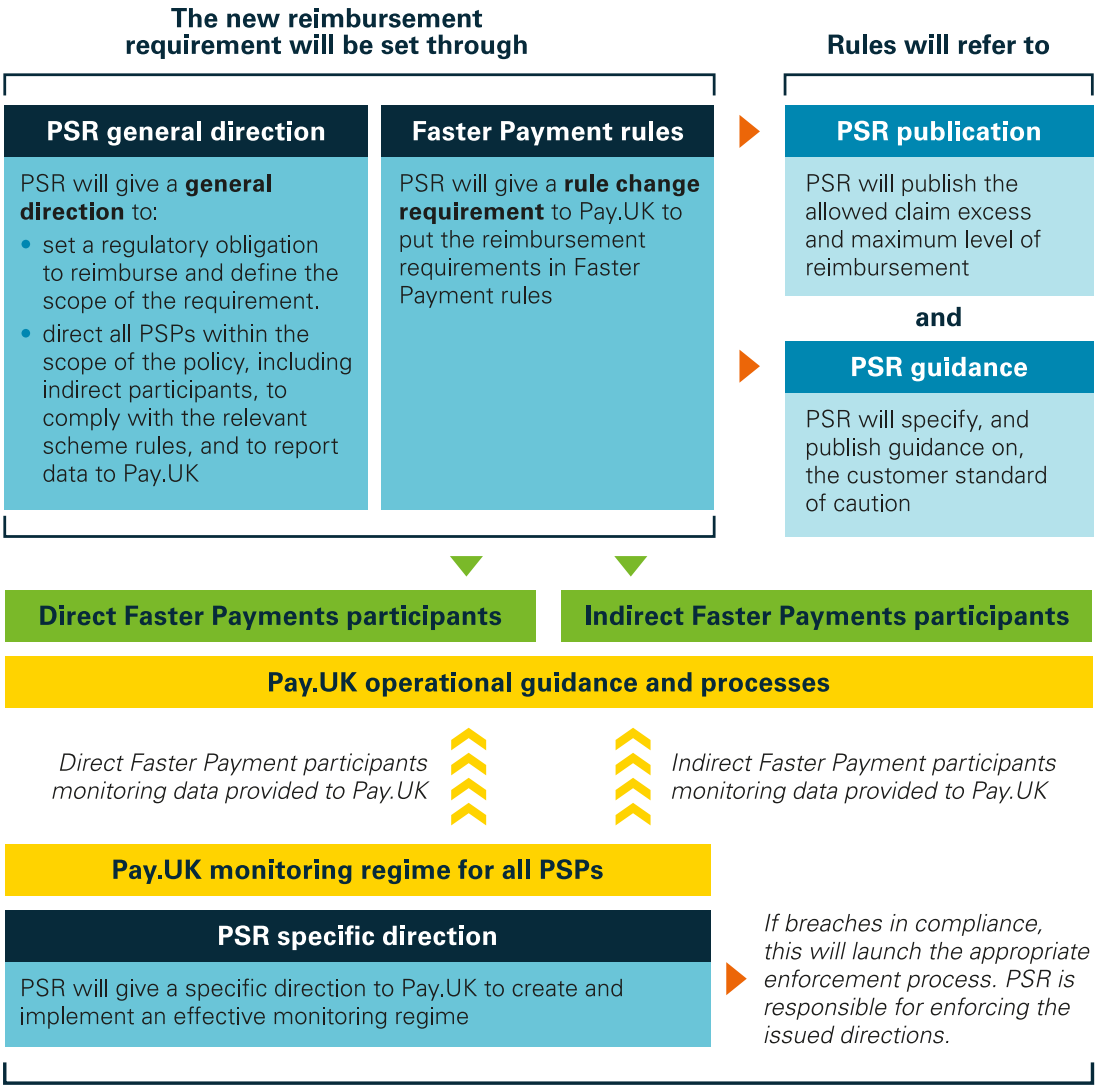
PSR guidance and publications

6.19 We will provide regulatory guidance on the customer standard of caution (gross negligence) and publish the maximum level of the claim excess. At this stage, it is more appropriate for us to control these customer incentives so that we can take account of all competing interests and objectives.

6.20 The scheme rules will allow PSPs to apply a customer standard of caution and a claim excess to APP fraud claims. But we will specify the customer standard of caution (gross negligence) in a PSR guidance document and the maximum value of the claim excess through a separate PSR publication (such as an online notice on the PSR website).

6.21 We will also take initial responsibility for defining the maximum level of reimbursement under the new reimbursement requirement. In the future, when Pay.UK has built sufficient capability and capacity, we will explore transferring these roles to Pay.UK.

Figure 9: Implementing the new reimbursement requirement



Role of Pay.UK

6.22 To prepare for the new reimbursement requirement, we have engaged extensively with Pay.UK. In advance of the requirements coming into force, we require Pay.UK to:

- draft and implement Faster Payments rules to comply with the section 55 rule change requirement by the date specified in the requirement (see 6.16)
- create and implement a compliance monitoring regime for all requirements across all in-scope PSPs (including indirect participants) (see 6.28 to 6.32)

6.23 We also expect Pay.UK to:

- lead engagement with industry to complete the actions needed for successful implementation, including providing operational guidance for firms to comply with the new rules (see Chapter 7)
- ensure the enforcement procedure for the reimbursement rules is clear to direct Faster Payments participants (see 6.34)

6.24 We expect Pay.UK to continue working towards the stronger role we set out in our five-year Strategy. We will continue to monitor and work with Pay.UK as it develops the NPA and makes related adjustments to its rulebook. As part of ensuring that the reimbursement provisions and requirements are carried forward into the NPA. We want Pay.UK to:

- consider how the reach of its rules may need to change to adapt to existing and emerging risks (including APP fraud)
- develop its enforcement regime with more tools and powers to enforce compliance with its rules
- evolve and refine the relevant rules as evidence is gathered, including leading industry work to consider how a more refined reimbursement cost allocation model could be developed[35]

Monitoring Pay.UK's implementation

6.25 We will create a compliance monitoring regime to assess whether Pay.UK is fulfilling its role set out in the specific direction and the section 55 rule change requirement.

6.26 We will gather appropriate data to inform our planned post-implementation review of the new reimbursement requirement. We expect to gather and analyse data on Pay.UK's performance on all areas set out in paragraphs 6.22 to 6.24, including:

- **Implementing the new reimbursement requirement:** We will monitor and evaluate Pay.UK's performance in effectively implementing the new reimbursement requirement, including achieving key milestones.
- **Creating a compliance monitoring regime:** We will monitor and evaluate how effectively Pay.UK performs in monitoring all in-scope PSPs (including indirect participants).
- **Enforcing the new reimbursement requirement:** We will monitor and evaluate how effectively Pay.UK performs in enforcing the new reimbursement requirement.

6.27 We will require Pay.UK to notify us of any proposed changes to the relevant reimbursement rules. This will allow us to raise any concerns and to intervene, if necessary (including by using our powers under section 55), if we do not consider the changes will support our policy objectives. We will keep the need for this safeguard under review.

35 To ensure that the rules deliver the intended key policies, we will require Pay.UK to notify us of any proposed changes to the relevant reimbursement rules.

Monitoring PSPs' implementation of the new reimbursement requirement

6.28 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.

6.29 An effective monitoring regime is one that will measure whether PSPs are consistently complying with the scheme rules on reimbursement requirements. To achieve this, Pay.UK and industry will need to complete several key actions including agreeing new systems and governance processes (see Chapter 7).

6.30 We will require Pay.UK to provide us with a summary of PSP performance and compliance with the new reimbursement requirement. The information gathered will inform our monitoring of the general direction we give to PSPs.

6.31 The high-level areas we expect Pay.UK to gather data and analyse data on are:

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

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

Enforcing the new reimbursement requirement

6.33 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' performances in complying with the requirements.

6.34 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.

6.35 For any cases referred to the PSR, we use our enforcement powers as we judge appropriate, taking account of our administrative priority framework.[36]

6.36 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. Once we have been notified of a potential breach, we will use enforcement powers as we judge appropriate, taking account of our administrative priority framework.

Putting reimbursement in place in other payment systems

6.37 As Chapters 1 and 2 set out, we are increasing protections for Faster Payments because this is the system across which the majority of APP fraud currently takes place. Fraud can operate and migrate across payment systems, and work is underway to consider whether the new reimbursement requirement should be applied to other payment systems. The Bank of England, as the operator of the CHAPS system, is committed to achieving comparable outcomes of consumer protection regardless of the payment system the consumer uses (see Chapter 2).

36 PSR, *Administrative Priority Framework* (March 2015).

7 Achieving successful implementation

Cross-sector collaboration is essential to successfully implementing the new reimbursement requirement so that all eligible customers will be entitled to reimbursement from day one.

The industry must complete a series of key actions to comply with the new Faster Payments rules and with our directions. Pay.UK will act as coordinator with industry where necessary, while we will focus on unblocking regulatory barriers to success and supporting cross-sector consistency. We will decide the start date of the new requirement based on a balance between urgency to act and practicality.

Acting now to implement the new reimbursement requirement

7.1 We want customers to understand the new reimbursement requirement by day one. We expect the payment industry to take the lead in making their customers aware of their responsibilities, what they are entitled to if they fall victim to APP fraud, how to claim and what will happen if they claim.

7.2 To comply with the new requirements, industry will need to meet a number of minimum conditions (see paragraph 7.4) by day one. It is up to firms, individually and collectively, how they meet these conditions. We want to give Pay.UK and the industry space to innovate and choose how to best deliver the new reimbursement requirement. But we believe industry must now begin allocating appropriate resources to understanding how they can meet these conditions and collaborate where necessary.

7.3 We will support implementation by unblocking regulatory barriers and supporting cross-sector consistency (see paragraph 7.7). This will include tracking key actions across the wider ecosystem to ensure the appropriate measures are in place from day one.

Industry action

7.4 To comply with the new Faster Payments rules and our directions industry will need to complete several actions, from implementing new systems to sharing data and improving communication between PSPs. It is up to industry to decide how to complete these actions (to the extent they are not in place already). The key capability requirements include that:

- PSPs can effectively communicate, share information on APP fraud claims and compensate each other for the cost of reimbursement in line with our requirements

- APP fraud cases can be tracked to enable reimbursement and repatriation across PSPs
- PSPs can initiate and engage with reimbursement requests from a sending PSP to a receiving PSP for 50% of a claim after it has reimbursed the customer
- APP fraud claims can be assessed, and the outcome communicated to the victim, within five business days (subject to the 'stop the clock' provision)

7.5 Many firms are likely to want to undertake additional actions beyond the minimum required for compliance to mitigate how the new requirements impact their business.

Pay.UK action

7.6 We will look to Pay.UK to play a leading role in coordinating and enabling implementation. Pay.UK will need to:

- draft rule changes in line with our section 55 requirement
- engage with participants to understand what they require from Pay.UK, including for example operational guidance and centralised communication capability
- provide any operational guidance necessary to help firms comply with scheme rules
- set out the form, frequency and process of PSP reporting requirements
- put in place effective monitoring with reporting requirements and clear enforcement processes in the event of non-compliance

The PSR and wider ecosystem action

7.7 We will unblock regulatory barriers and support cross-sector consistency, collaborating closely with the FCA, other regulators and government, and coordinating action across the sector where appropriate. Specifically, we will:

- consult on the claim excess and maximum level of reimbursement in Q3 2023
- consult on the customer standard of caution (gross negligence) guidance in Q3 2023
- engage with industry on implementation requirements to raise understanding of the new policy framework and how we expect the new reimbursement requirement to operate
- identify and address any regulatory barriers to effective communication between sending and receiving PSPs, in collaboration with the Information Commissioners Office (ICO)

Setting an appropriate start date

7.8 The new reimbursement requirement will come into force in 2024. We will consult on a specific start date in Q3 2023 and publish a final date alongside the final legal instruments in Q4 2023. We expect industry to start work now to implement the new reimbursement requirement.

7.9 We want to implement the new reimbursement requirement as soon as practically possible. Every day, more people fall victim to APP fraud, which can have a devastating impact on their lives or businesses. But changing the payment industry's approach to APP fraud will not take place overnight. As this chapter has described, some firms will find it challenging to implement changes required to meet the new reimbursement requirement in the short term.

7.10 A reasonable start date for the new reimbursement requirement will bring protections in as soon as practically possible. It will also give PSPs sufficient time to invest in prevention and prepare for the new reimbursement requirement. To set a reasonable start date, we will engage stakeholders ahead of our consultation on the draft legal instruments in Q3 2023. We will consider various factors in setting a reasonable start date:

- **Time required to achieve the minimum viable system-wide changes,** including PSPs being able to communicate, share information on APP fraud claims and effectively compensate each other for the cost of reimbursement in line with our requirements. We will push industry to consider a range of options including where tactical solutions can be deployed in the short term to accelerate implementation.
- **Time for PSPs to invest in prevention and prepare for the new reimbursement requirement,** recognising changes will be required across many business areas. In our September consultation, one PSP listed more than ten business areas which would be impacted by the policy. We also want to ensure that smaller PSPs are not disproportionately impacted by the start date, acknowledging that they may have fewer available resources.
- **The impact on the end users of Faster Payments,** recognising that there are new victims of APP fraud every day. We will provide industry with reasonable time to prepare but will balance this with the need to protect end users as soon as practically possible.

8 Evaluating policy effectiveness

The UK is the first country in the world to implement consistent minimum standards to reimburse victims of APP fraud. We will monitor the effectiveness of our policy from day one and publish a post-implementation review within two years.

Monitoring the effectiveness of the new reimbursement requirement

8.1 We will monitor the effectiveness of the new reimbursement requirement by using information that Pay.UK gathers as well as data we gather on how Pay.UK itself is monitoring compliance. We will collect data regularly on outcomes set out in Chapter 1, including:

- the level of APP fraud, including total value and the number of reported cases (see Figure 1 on how and why we expect this number to rise initially but decrease over time)
- the level of APP fraud reimbursement under the new requirement, including number of claims and their value
- treatment of vulnerable customers, including levels of reimbursement to them
- the value of repatriated APP fraud funds
- transaction volume through Faster Payments
- the speed of reimbursement, including the average length of all investigations

8.2 We will also gather data regularly to assess the potential policy risks set out in Chapter 4. This will include:

- data on market health, including how many PSPs have ceased trading and how many have reduced their service offering (in collaboration with the FCA)
- data on moral hazard
- the cost of Faster Payments transactions
- the number of legitimate payments stopped ('false positives')
- the level of first-party fraud
- any evidence of 'de-banking' of certain groups
- any evidence of fraud migrating to other payment methods and systems

8.3 We will report on the effectiveness of the new reimbursement requirement through our annual performance report and publish a review within two years (see 8.8).

Aligning with the balanced scorecard of APP fraud data

8.4 In March 2023, we directed 14 PSP groups to collect and report data on their management of APP fraud using three metrics of performance:

- **Metric A:** The proportion of APP fraud victims left out of pocket.
- **Metric B:** APP fraud rates for each sending PSP.
- **Metric C:** APP fraud rates for each receiving PSP (not including any money that has been returned to the victims).

8.5 We will publish this balanced scorecard of APP fraud data on a six-monthly basis. Over time, the data reporting method is likely to change. Once the new reimbursement requirement is implemented, the Metric C validation process may be replaced by a fuller process for checking information between sending and receiving PSPs to support the liability split between them. We will review how well the balanced scorecard supports our ongoing evaluation of the new reimbursement requirement, recognising overlaps between some data points. We will also consider whether there are opportunities to streamline our reporting requirements.

Post-implementation review

8.6 We will publish a comprehensive review of the new reimbursement requirement within two years of day one, including evaluation of:

- overall effectiveness of the requirement, including an assessment of the potential policy risks, using the data gathered through our ongoing monitoring
- our approach to implementation and the legal instruments we give
- Pay.UK and the payment industry's implementation of appropriate systems and governance to meet the requirement
- PSP compliance with the requirement, using data gathered through Pay.UK's ongoing monitoring
- the level and accuracy of PSP interventions and stopped payments (in collaboration with the FCA)
- the effectiveness of the monitoring regimes and enforcement processes
- any identified equality impacts or issues

8.7 We will also continue to work with Pay.UK to understand how we can achieve the PSR's ambition for Pay.UK to make, maintain, refine, monitor and enforce compliance with comprehensive scheme rules that address fraud risks in the system. Where necessary, we will consult on any changes to Pay.UK's role and implement these changes through appropriate legal instruments.

8.8 We will review the progress of wider action to fight fraud. This will include our own efforts through publishing a balanced scorecard of APP fraud data, increasing intelligence sharing and expanding Confirmation of Payee. It will also include an overview of the wider fraud ecosystem and the progress of others in taking the priority actions we set out in Chapter 3.

Annex 1
Equality impact assessment

In line with our Public Sector Equality Duty (PSED) under the Equality Act 2010, we have assessed the likely equality impacts for the new reimbursement requirement. We have consulted on this policy and considered any responses we received in respect to potential impacts on specific groups.

Approach to assessment

1.1 Section 149 of the Equality Act 2010 requires us to consider the likely equality impacts of our policy on the public, including on people with the following relevant protected characteristics: age, disability, gender reassignment, pregnancy and maternity, race, religion or belief, sex, sexual orientation, and marital status. We have looked at a broad range of evidence to support our assessment, including the responses to our September consultation and data from the Victims Commissioner.[37]

All customers

1.2 As a result of the new reimbursement requirement we expect PSPs to prevent more APP fraud, leading to fewer APP fraud cases. This would be a positive impact for people across all demographics, including those with protected characteristics.

Interaction with vulnerable customers

1.3 We recognise that there is likely to be a significant overlap between vulnerable customers and those with certain protected characteristics. There is evidence, for example, that shows that older customers are more likely to be victims of APP fraud.[38]

1.4 We have taken the interests of vulnerable customers into account. According to the FCA's definition, a 'vulnerable customer' is 'someone who, due to their personal circumstances, is especially susceptible to harm – particularly when a firm is not acting with appropriate levels of care'. As further set out in the FCA guidance, 'consumers with some characteristics of vulnerability may be more likely to fall victim to scams'.[39] Some types of vulnerability can negatively affect decision-making, leading to people being at greater risk from social engineering and less able to exercise caution to protect themselves from APP fraud.

37 Victims Commissioner, *Who suffers fraud? Understanding the fraud victim landscape* (October 2021); FCA, *Financial Lives 2022 Survey* (2022).

38 Victims Commissioner, *Who suffers fraud? Understanding the fraud victim landscape* (October 2021).

39 FCA, *FG21/1 Guidance for firms on the fair treatment of vulnerable customers* (February 2021).

The Equality Objectives

Remove or minimise disadvantages suffered by people due to their protected characteristics

1.5 We accept that some PSPs may see certain groups with protected characteristics as being at higher risk of APP fraud. This could result in PSPs implementing greater friction in payment journeys or removing some banking services. In our consultation, several PSPs reported that there is no typical high-risk service user for APP fraud. We think this is a manageable risk, and we will consider it as part of our post-implementation review (see Chapter 8).

Take steps to meet the needs of people from protected groups where these are different from the needs of other people

1.6 We recognise that there is likely to be a significant overlap between vulnerable customers and those with certain protected characteristics. We require PSPs to exempt vulnerable customers from the customer standard of caution exception and the claim excess. This is a proactive step to meet the needs of vulnerable people with protected characteristics who may be more susceptible to APP fraud.

Encourage people from protected groups to participate in public life or in other activities where their participation is disproportionately low

1.7 There is limited evidence of how our policy will impact this area. However, a decrease in successful APP fraud and clearer consumer protection will inspire greater confidence for customers in the Faster Payments system.

Equality risks and mitigations

Groups being disproportionately impacted by the claim excess

1.8 We accept that some groups may be disproportionately impacted by the claim excess, particularly those groups from low-income households. Those customers with low financial resilience may qualify as vulnerable and therefore will be exempt from the claim excess under the new reimbursement requirement. We will monitor this and consider it as part of our post-implementation review (see Chapter 8).

Groups being disproportionately impacted by the customer standard of caution (gross negligence)

1.9 We accept that some groups may be disproportionately impacted by the customer standard of caution (gross negligence), particularly those with low mental capacity or cognitive disability, low knowledge or confidence in managing finances, poor literacy or numeracy skills, poor English-language skills, poor or non-existent digital skills, or learning difficulties. These groups may not be able to take the same level of care.

1.10 We have taken proactive steps to support those with characteristics of vulnerability linked to a specific APP fraud case. PSPs should assess, as part of the claim, whether these characteristics prevented the individual from taking appropriate steps to protect themselves, and hence whether they should be considered vulnerable. Vulnerable customers are exempt from the customer standard of caution.

Increased customer reluctance to use payment services

1.11 There is a risk that increased warnings and other fraud prevention measures introduced by PSPs could cause vulnerable people to experience heightened fear of APP fraud and therefore reduce or stop their use of Faster Payments. We expect that this risk will be mitigated as customers will also be more aware of their rights to reimbursement if they do fall victim to APP fraud. We also consider that the new reimbursement requirement will lead to fewer APP fraud cases, which should increase confidence in the payment system. We therefore do not consider that we should need to take any further mitigating action.

Claim excess driving excessive caution

1.12 There is a risk that any claim excess may cause some customers to become overly cautious with Faster Payments transactions for fear of losing the excess amount, even when the payment is legitimate. While this may occur, without our policy the risk for many customers would be a total loss of funds if they fell victim to APP fraud. The excess is voluntary for PSPs to introduce. We want to make sure that the excess is set at a reasonable level to encourage sufficient customer caution and so we will consult on the excess level in Q3 2023.

Increased friction

1.13 Under our proposals, PSPs will be incentivised to reduce the incidence of APP fraud by introducing stronger fraud controls. This could mean that more genuine payments are also stopped because they trigger PSPs' detection processes or are considered higher risk. This could affect people with certain protected characteristics more than other customers, as they may be perceived as more likely to become victims of APP fraud.

1.14 Our view is that some additional friction for a small proportion of payments is an acceptable price for preventing APP fraud and achieving increased customer protection, including additional protection for those most vulnerable to becoming victims. We also note that current industry initiatives to improve data sharing between PSPs and increased incentives to improve fraud detection and prevention should help to minimise the number of payments stopped unnecessarily (see Chapter 3).

FCA Consumer Duty

1.15 We consider the Consumer Duty to be a significant mitigation against the equality risks that we have identified (see Chapter 3 and above). We will work closely with Pay.UK and the FCA to help ensure that customers are treated fairly and equally.

Monitoring and evaluation

1.16 As part of our post-implementation review, we will assess whether there are any equality impacts or issues, and consider what changes and mitigations are necessary. The monitoring regime will help to ensure that any negative outcomes for specific groups are identified and mitigated as soon as possible.

Annex 2
Payment initiation service transactions

2.1 Payment initiation service (PIS) transactions are in scope of the new reimbursement requirement.

2.2 We apply the new reimbursement requirement to PIS transactions in the same way as with other types of Faster Payments. The obligations on sending and receiving PSPs are unchanged, including that sending and receiving PSPs must share the cost of the new reimbursement requirement through a 50:50 split. Our analysis identifies two main models of how PIS transactions work, which we refer to as:

- 'Model A': PIS-provider (PISP) has no access to funds during the payment journey
- 'Model B': PISP operates as the receiving PSP, and has access and holds funds during the payment journey

2.3 A PISP that operates as the sending or receiving PSP for a fraudulent transaction is subject to the new reimbursement requirement. These are Model B PISPs.

2.4 Figure 10 provides examples of Model A and Model B PIS transactions. Figure 11 shows how reimbursement will work.

2.5 All organisations in the examples below are entirely fictional and are not based on real companies. They are provided for illustrative purposes only.

Explaining a 'Model A' fraudulent PIS transaction: PISP is not liable for the cost of reimbursement

2.6 In Model A, the PISP acts as the payer's agent sending a payment from their account to the recipient's. The PISP has no access to funds during the payment journey. The payer may be directed to the PISP's website by the end recipient (as a payment option); they may alternatively receive a link by email or QR code; or the recipient may be selected through another method.

2.7 In our Model A example, 'BIG CARS', a fraudster posing as a fictional car dealership, deceives a victim into sending funds for a non-existent car in response to a post the customer has seen on social media. The fraudster chooses to use PISPAY (a fictional company), which acts only as a PISP:

- 'BIG CARS' (the fraudster posing as a car dealership) sends the payer a unique reference and link to PISPAY.

- PISPAY gets the customer to select their bank (UKBANK) and connects to it using Open Banking.
- UKBANK authenticates that the victim is its customer. PISPAY provides the payment information to UKBANK and requests the payment to be made.
- UKBANK sends the payment directly to the bank of 'BIG CARS' (the fraudster) via Faster Payments and confirms to PISPAY that the payment has been initiated. PISPAY confirms to the payer that the payment has been accepted.
- The bank of 'BIG CARS' (the fraudster) has now received the payment.

2.8 PISPAY is not responsible for 50% of the cost of reimbursement if the transaction is fraudulent, nor for reimbursing its customer. The customer would be reimbursed by their PSP (UKBANK), and the bank of 'BIG CARS' (the fraudster) would be responsible for 50% of the cost of reimbursement.

Explaining a 'Model B' fraudulent PIS transaction: PISP is liable for the cost of reimbursement as it is acting as the receiving PSP

2.9 In Model B, the PISP is also the receiving PSP – it performs both roles – and it offers a payment account to its recipient customer(s) or else collects the funds into its own accounts, and generally nets a number of payments together before sending this on to the final recipient.

2.10 In our Model B example, 'BIG CARS', a fraudster posing as a fictional car dealership, deceives a victim into sending funds for a non-existent car in response to a post the customer has seen on social media. The fraudster chooses to use INTPAY, which acts as a PISP and also provides a receiving account for its customers (in this case, the fraudster):

- 'BIG CARS' (the fraudster posing as a car dealership) sends the payer a unique reference and link to INTPAY.
- INTPAY gets the customer to select their bank (UKBANK) and connects to it using Open Banking.
- UKBANK authenticates that the victim is its customer. INTPAY provides the payment information to UKBANK and initiates the transaction.
- INTPAY sees the incoming payment and allocates it to the payment account of 'BIG CARS' (the fraudster). It informs 'BIG CARS' (the fraudster) that they have been paid.
- Later that day INTPAY makes a payment for the total value of the five payments the PISP has received for 'BIG CARS' (less any fees) to the bank of 'BIG CARS' (the fraudster).

2.11 INTPAY chooses to operate as a receiving PSP and hold the funds for a period of time. Therefore, INTPAY is responsible for 50% of the cost of reimbursement if the transaction is fraudulent. The customer would be reimbursed by their PSP (UKBANK).

Figure 10: Examples of different PIS transaction models

All organisations in the examples below are entirely fictional and are not based on real companies. They are provided for illustrative purposes only.

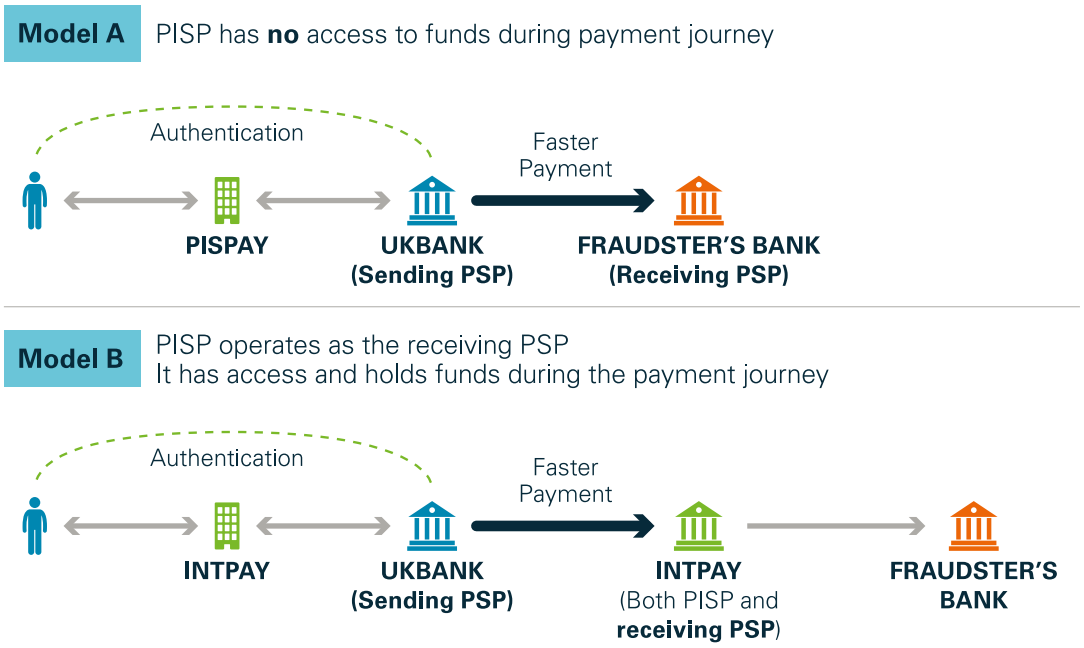
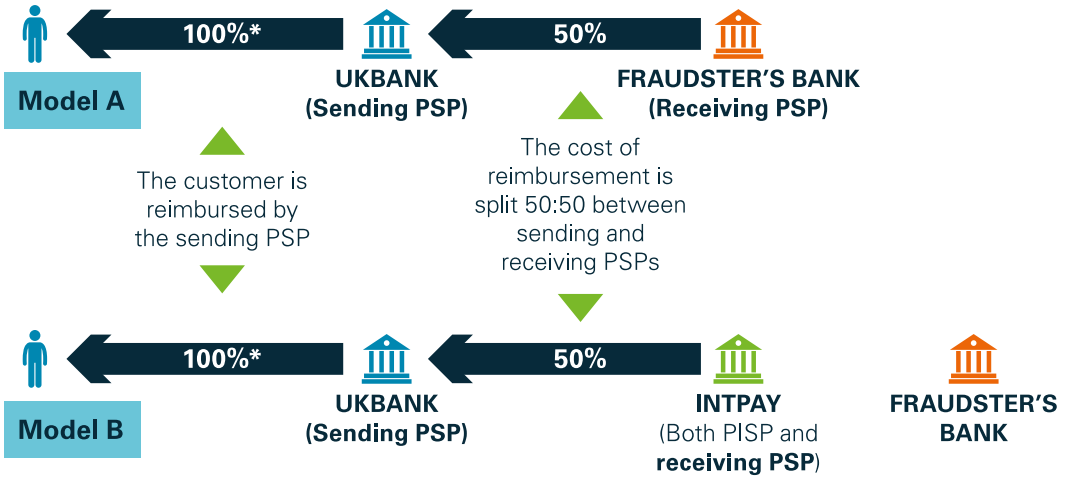


Figure 11: Examples of different PIS transaction models

All organisations in the examples below are entirely fictional and are not based on real companies. They are provided for illustrative purposes only.



Model A and B are PSR terms covering many business models

* Minus any claim excess

Glossary

Concept	Definition
Authorised push payment (APP) fraud payment	A payment made as part of an APP fraud. The new reimbursement requirement applies to payments executed by the sending PSP, in accordance with an authorisation given by its customer, to an account controlled by a person other than the customer, where the customer has been deceived into granting that authorisation as part of an APP fraud case. This includes where: • the payer intends to transfer the funds to a person other than the recipient, but is deceived into transferring the funds to the recipient • the payer intends to transfer the funds to the recipient but is deceived as to the purposes for which they are transferring the funds
Bacs	A UK payment system used to make electronic payments between bank accounts, used for Direct Debit payments and Direct Credit payments. Typically, payments are initiated by corporates for collection of regular bills and payment of salaries and invoices.
Charities	Charities are defined under the relevant legislation in the UK and registered as such. Charities in scope have an annual income of less than £1 million.
CHAPS	The UK's real-time, high-value payment system operated by the Bank of England.
Consumer	A consumer is an individual who, under contracts for payment services to which the Payment Services Regulations 2017 apply, is acting for purposes other than a trade, business or profession.
Contingent Reimbursement Model (CRM) Code	A voluntary industry code administered and overseen by the Lending Standards Board that sets out the standards expected of PSPs in reimbursing victims and sharing liability when an APP fraud case occurs. As of publication, there are ten signatories to the CRM Code.
Direct PSP	A PSP that is a direct participant in a specified payment system. A PSP is considered to have direct access to a payment system when it is contractually signed up to the rules and standards of the system and is able to send and receive payments directly through the payment system infrastructure.
Faster Payment	A payment across the Faster Payments system.

Concept	Definition
Faster Payments system	The UK electronic payment system that provides near real-time payments as well as standing orders and forward-dated payments, operated by Pay.UK.
Gross negligence	The FCA has said in guidance: "In line with the recitals to PSD2, we interpret 'gross negligence' to be a higher standard than the standard of negligence under common law. The customer needs to have shown a very significant degree of carelessness".[40] We will publish further guidance on the customer standard of caution (gross negligence) in Q4 2023.
Indirect PSP	An organisation is considered to have indirect access to a payment system if it has a contractual arrangement with an indirect access provider that is an organisation that already has direct access to that payment system. An indirect PSP may be classified as either an agency or non-agency PSP.
Micro-enterprises	A micro-enterprise is an enterprise that employs fewer than ten persons and whose annual turnover and/or annual balance sheet total does not exceed €2 million.
Payment initiation service provider (PISP)	A firm that provides a third-party service to customers who initiate a payment order via an account held at another PSP (often referred to as an Account Servicing PSP).
Payment service provider (PSP)	A provider of payment services to customers typically through the provision of accounts. A PSP may be a bank, an E-Money Institution or a Payment Institution. In the UK a PSP must be authorised and regulated by the FCA. PSPs may be direct PSPs or indirect PSPs depending on whether they are able to initiate payments directly in a payment system or only via an Indirect Access Provider.
Receiving PSP	The Payment Service Provider that operates the ultimate account into which a payment is received.
Sending PSP	The Payment Service Provider that operates the account from which a payment is sent.

40 FCA, *Payment Services and Electronic Money – Our Approach: The FCA's role under the Payment Services Regulations 2017 and the Electronic Money Regulations 2011* (November 2021).

PUB REF: PS23/3

12 Endeavour Square
London E20 1JN
Telephone: 0300 456 3677
Website: www.psr.org.uk