frontier economics

INDEPENDENT EVALUATION OF APP SCAM POLICIES: TECHNICAL REPORT

01 JULY 2026

WWW.FRONTIER-ECONOMICS.COM

Contents

Glossary

APP scam / APP fraud: A scam where a consumer is manipulated, deceived or persuaded into authorising a payment to an account outside their control, where the recipient is not who the consumer intended to pay, or the payment is not for the purpose the consumer intended.

Bacs: The UK payment system used mainly for Direct Debits and Direct Credits, including salary, pension and supplier payments.

Civil dispute: A dispute about the quality, delivery or terms of goods or services, rather than an APP scam. Civil disputes are outside the reimbursement requirement.

CHAPS: The UK high-value same-day sterling payment system, typically used for large or time-critical payments.

Confirmation of Payee: A name-checking service that allows a payer to check whether the account name they have entered matches the name on the recipient account before making a payment.

Consumer: For the purposes of the reimbursement requirement, individuals, microenterprises and eligible charities that use payment services.

Consumer Standard of Caution (CSOC): The standard consumers are expected to meet under the reimbursement requirement, including having regard to relevant warnings, promptly reporting suspected scams, responding to information requests, and consenting to police reporting where required.

Contingent Reimbursement Model (CRM) code: The voluntary code that preceded the mandatory reimbursement requirement and set standards for how participating firms should reimburse victims of APP scams.

Direct FPS participant: A payment service provider that connects directly to the Faster Payments System and settles payments through its own settlement arrangements.

Faster Payments System (FPS): The UK payment system that enables near real-time electronic payments between participating payment service providers.

Financial Conduct Authority (FCA): The UK regulator responsible for conduct regulation of financial services firms and financial markets.

Financial Ombudsman Service (FOS): The independent body that resolves complaints between consumers and financial services firms.

First-party fraud: A case where a customer falsely claims to have been the victim of fraud, for example to obtain reimbursement.

Indirect FPS participant: A payment service provider that accesses the Faster Payments System through another PSP, usually a direct participant, rather than connecting directly itself.

In-scope APP scam policies: The APP fraud reimbursement requirements for Faster Payments and CHAPS, and the PSR's APP fraud performance data.

In-scope claim: A claim that is recorded as needing assessment under the reimbursement requirement, before any decision is made on whether it is reimbursable.

Intrabank payments: Payments made between accounts held at the same payment service provider, rather than between different firms through an interbank payment system. Sometimes called 'on us' payments.

Measure 1: The PSR's APP fraud performance data policy, under which major PSP groups report comparable data on reimbursement and APP scam rates by sending and receiving PSP.

Mule: A person or account used to receive, move or transfer funds obtained through fraud or other criminal activity, often on behalf of another person.

Pay.UK: The operator of the UK's main retail interbank payment systems, including Faster Payments, Bacs and the Image Clearing System. Pay.UK also has roles in implementing and operating elements of the APP scam reimbursement framework.

Payment Service Provider (PSP): In relation to a payment system, means any person who provides services to persons who are not participants in the system for the purposes of enabling the transfer of funds using the payment system.

Payment Systems Regulator (PSR): The UK regulator responsible for regulating payment systems, including Faster Payments, and for introducing the APP scam reimbursement requirement.

Performance data: APP fraud data published by the PSR, mainly for the fourteen largest UK banking groups, covering firms' management of APP fraud, with some additional receiving-side data for smaller firms.

Receiving PSP: A PSP providing a payment account into which APP scam payments are received.

Reimbursable claim: A claim that a PSP has assessed as meeting the criteria for reimbursement under the reimbursement requirement.

Reimbursement requirement: The requirements introduced by the PSR for Faster Payments, and by the Bank of England for CHAPS, which set minimum standards for PSPs to reimburse eligible victims of APP fraud up to a maximum value of £85,000 per claim.

Relevant account: An account held in the UK that can send or receive Faster Payments or CHAPS payments and is within the scope of the reimbursement requirement.

Reporting Standard A: The compliance reporting standard under which sending PSPs report core data on in-scope APP scam cases, including claim volumes, values and reimbursement outcomes.

Second-generation mule: A mule account that receives funds from another mule account rather than directly from the victim, helping criminals layer and move stolen funds through the payment system.

Sending PSP: a PSP that provides a relevant account for a consumer, from which one or more FPS APP scam payments were made.

Statement of Requirements: The PSR document setting out the scope, objectives, requirements and expected outputs for the independent review of the APP fraud policies.

Stop the clock: The process by which the reimbursement timeline can be paused while a PSP obtains additional information needed to assess a claim.

UK Finance: The trade association representing the UK banking and financial services industry.

1 Introduction

Frontier Economics has been commissioned by the Payment Systems Regulator (PSR) to conduct an independent evaluation of its two key policies on Authorised Push Payment (APP) scams: the reimbursement requirement and the publication of APP fraud performance data.[1]

This document is the Technical Report for the Independent evaluation of APP scam policies. It is intended to be used as a supporting document for the Summary Report. The Technical Report provides detailed information on the regulatory landscape and the policy interventions, the evaluation theory of change and the methodology. It also provides the full evidence base upon which we have drawn our assessment of the policies.

This document does not provide our assessment of the PSR's policies. **The summary of our findings and our overall assessment of the impact of the policies and their effectiveness at achieving its target outcomes is covered in the Summary Report.**

The evaluation was conducted between September 2025 and June 2026.

- The first stage of this work was to develop the evaluation approach, including the theory of change, evidence collection strategy and the methodology for assessing the impacts from the policies. The details of the evaluation report were shared with stakeholders in the Evaluation Framework Report in December 2025.[2]
- The Technical Report and the Summary Report summarise our analysis and provide our conclusions about the impact of the policies on the market. This Technical Report and the Summary Report were shared with key stakeholders for comment in advance of publication.[3]

The evaluation has been designed in line with the best practice principles for theory-based evaluation, as set out in HM Treasury's Magenta Book. It draws on both quantitative and qualitative evidence, reflecting the need to assess measurable changes in outcomes as well as wider behavioural and market effects. Further detail on the evaluation methodology, including evidence sources, stakeholder engagement and the approach to attribution, is set out in Section 5.

The structure of this report is as follows:

- Section 3 provides an overview of the relevant APP scam policies;

[1] Following the PSR's terminology, we use "APP scam(s)" and "APP fraud" interchangeably throughout this evaluation report. We note that only "APP scam" has a formal technical definition in the PSR's legal instruments as set out, for example, in Specific Direction 18 (PSR, 2023), Specific Direction 20 (PSR, 2024), Specific Direction 21 (PSR, 2024).

[2] This report is not publicly available

[3] See section 5.3 for details of our Working Group and Advisory Group.

- Section 4 sets out the theory of change underpinning the evaluation, including the expected mechanisms through which the policies may affect consumer outcomes, PSP behaviour and wider market outcomes;
- Section 5 describes the evaluation approach;
- Section 6 presents our findings for Theme 1 – the impacts on PSP actions to tackle APP scams;
- Section 7 presents our findings for Theme 2 – the impact on fraud;
- Section 8 presents our findings for Theme 3 – the impacts on consumer welfare; and
- Section 9 presents the findings for Theme 4 – the impacts on PSPs and other markets.

2 Overview of the regulatory landscape and relevant policy interventions

This section summarises the in-scope APP scam policies considered in this evaluation, and the wider regulatory landscape for APP fraud.

As defined by the PSR:

> *"Authorised Push Payment (APP) scam means where a person uses a fraudulent or dishonest act or course of conduct to manipulate, deceive or persuade a consumer into transferring funds from the consumer's relevant account to a relevant account not controlled by the consumer, where:*
>
> - *The recipient is not who the consumer intended to pay, or*
> - *The payment is not for the purpose the consumer intended."*[4]

APP fraud has been a significant issue in the UK for the past 10 years.[5] Prior to the introduction of the reimbursement requirement, APP scams cost UK consumers £485 million in 2022[6] and £460 million in 2023.[7, 8]

[4] PSR (2024). APP Scams Amended Specific Direction July 2024. Throughout this evaluation, we generally use "consumer" in line with its meaning under Specific Direction 20 (PSR, 2024) to mean service users of PSPs that are individuals, microenterprises (an enterprise that employs fewer than ten persons and that has either an annual turnover or annual balance sheet total that does not exceed €2 million) or charities (a body whose annual income is less than £1 million per year and is a charity as defined by the Charities Act 2011, Charities and Trustee Investment (Scotland) Act 2005 or the Charities Act (Northern Ireland) 2008). As defined in the PSR's (2024) Specific Direction 20 and Specific Direction 21, we use "relevant account" to mean an account held in the UK that can send or receive either Faster Payments or Clearing House Automated Payment System (CHAPS), respectively. Specific Direction 20 and 21 exclude accounts provided by credit unions, municipal banks and national savings banks; Specific Direction further excludes CHAPS payments made to Financial Market Infrastructures (FMIs).

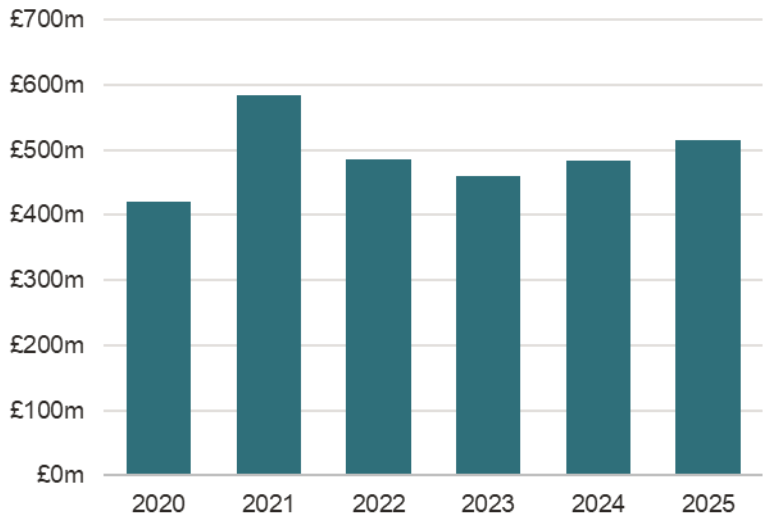
[5] Which? raised a super-complaint about protecting consumers from harm caused by APP scams in September 2016.

[6] UK Finance (2023). Annual Fraud Report 2023.

[7] UK Finance (2024). Annual Fraud Report 2024.

[8] The largest 14 banking groups reported APP fraud of £389 million in 2022 and £340.7 million in 2023. PSR (2024) Authorised push payment (APP) scams performance report.

Figure 1 APP fraud consumer losses over time



Source: Frontier analysis of UK Finance's Annual Fraud Report 2026

2.1 The voluntary CRM code

In May 2019, the CRM Code was developed via the APP Scams Steering Group, convened by the PSR with representatives from industry and consumer groups. The aim of the code was to develop a voluntary framework under which PSPs would commit to reimbursing victims of APP scams.[9]

CRM signatories committed to taking reasonable steps to protect their customers from APP scams by detecting, preventing and responding to APP scams. It set standards for sending firms, including scam detection, effective warnings, customer education and protection for vulnerable customers, and for receiving firms, including steps to prevent accounts being used to receive and move the proceeds of APP scams. It also set expectations for customers, including that they should pay attention to warnings and take reasonable steps to avoid scams. Where a customer was the victim of an APP scam, CRM signatories committed to reimbursing their losses unless an exception applied, including where the customer had not taken sufficient account of warnings.[10] The Lending Standards Board oversaw the scheme and FOS provided dispute resolution between banks and customers.

Many major banks signed up to the Code and by 2022 it covered around 90% of relevant transactions.[11] In 2023, CRM members reimbursed 68% of the money their consumers lost to APP scams, compared to non-CRM banks, who reimbursed 17% of APP scam losses.

[9] PSR (2018). Authorised push payment scams: Outcome of consultation on the development of a contingent reimbursement model.

[10] Lending Standards Board (2019). Contingent Reimbursement Model Code for Authorised Push Payment Scams.

[11] HMT (2022). Government approach to authorised push payment scam reimbursement.

Average APP scam losses were almost four times lower for transactions covered by the Code than for those outside it. [12,13]

Nevertheless, while the CRM Code marked meaningful progress, it did not provide consistent redress for all victims. Because it was voluntary, customers of non-signatory firms were not protected, and even among signatories implementation varied considerably.[14]

2.2 Overview of in-scope and related APP fraud policies

Over the last few years, the PSR and the FCA have introduced a programme of policies aimed at reducing the incidence of APP fraud and better protecting victims (see Figure 2 below). The following policies are in scope of this evaluation:

- **The reimbursement requirement**, which was enabled by government legislation[15] requiring the PSR to introduce a mandatory reimbursement requirement for APP fraud over the FPS, came into force on 7 October 2024. The requirement sets minimum standards for PSPs to reimburse victims of APP fraud over FPS. The Bank of England introduced similar requirements for CHAPS.
- **APP fraud performance data**, first published in October 2023, which the PSR publishes primarily in relation to the fourteen largest UK banking groups regarding their management of APP fraud, alongside some receiving-side data for smaller firms with high APP fraud receipt levels.

Alongside these in-scope policies, the PSR, government and the FCA have each taken action aimed at preventing APP fraud, although their roles differ across the relevant policies and initiatives:

- **The PSR's Confirmation of Payee (CoP)** is a name-checking service that helps ensure payments are sent to the correct account holder. It was initially rolled out in 2019 to the largest PSPs. The list of PSPs in scope was expanded in 2023 and 2024, extending CoP coverage to nearly all retail CHAPS transactions and around 99% of Faster Payments transactions. The rationale for introducing CoP was to reduce both accidentally misdirected payments and certain APP fraud ("malicious redirection" scams) by achieving near-ubiquitous CoP coverage.[16]

- **The government's Delayed Payments Legislation** came into force on 30 October 2024, extending the time PSPs can hold outbound payments where fraud or dishonesty is

[12] PSR (2024). Authorised push payment (APP) scams performance report. This figure excludes TSB, which offered a fraud refund guarantee. Including TSB, the reimbursement rate for non-signatories to the CRM was 48%.

[13] UK Finance (2024). Annual Fraud Report 2024. LSB (2025) Mind the Gap: The Legacy & Impact of the Lending Standards Board.

[14] PSR (2023) PS23/3 (p12). PSR (2023). Authorised push payment (APP) fraud performance report (p5).

[15] Financial Services and Markets Act 2023, s.72.

[16] PSR (2022). PS22/3.

suspected.[17] The government's objective was to improve APP fraud prevention and customer protection by giving PSPs sufficient time to investigate suspected APP fraud, particularly complex cases, while minimising disruption to legitimate payments.[18] The FCA issued guidance on how PSPs are expected to apply these legislative changes.[19]

- **The PSR's Fraud enabler report**: published in December 2024, using data from the 14 largest UK banking groups to identify where APP fraud tends to originate (such as social media and tech platforms) and what types of fraud (for example, romance fraud, purchase scams, investment scams) are prevalent.[20] The PSR's aim with this report was to increase transparency of the root causes of fraud in order to drive cross-sector action to address it. [21]

- **The FCA's wider work on fighting financial crime.** The FCA's work on APP fraud forms part of its broader approach to tackling fraud and financial crime, which is a priority in its 2025-2030 Strategy.[22] This includes work to improve firms' fraud systems and controls, explore greater data sharing, issue scam warnings, encourage online platforms to tackle illegal financial promotions, conduct multi-firm reviews, and take action where firms have inadequate fraud prevention arrangements. The FCA has a range of enforcement and supervisory tools to support these objectives. For example, its supervisory work on anti-fraud controls and money mule detection included multi-firm reviews on anti-fraud controls and complaint handling in firms, with a focus on APP fraud, and on detecting and preventing money mule activity,[23] These activities may affect APP fraud prevention by influencing firms' onboarding, account monitoring and suspicious activity controls.

These policies are not directly in scope of the evaluation as per the PSR's terms of reference but provide important context to the questions covered by this work. In the following sections, we provide further details of the in-scope policies.

[17] The Payment Services (Amendment) Regulations 2024, SI 2024/1013.

[18] The Payment Services (Amendment) Regulations 2024. Implementation Assessment.

[19] FCA (2024). FG24/6.

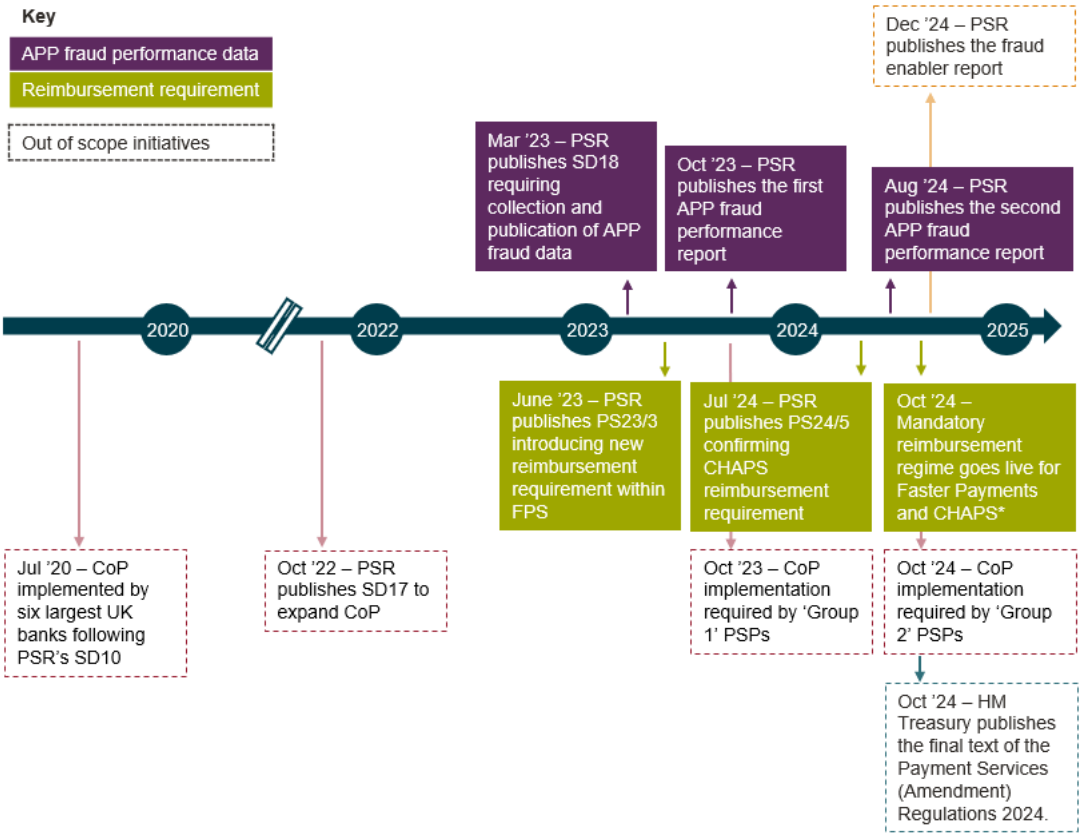
[20] PSR (2024). Unmasking how fraudsters target UK consumers in the digital age.

[21] *Ibidem.*

[22] FCA (2025). Strategy 25-30.

[23] FCA (2023). Multi-firm review: Anti-fraud controls and complaint handling in firms (with a focus on APP Fraud).

Figure 2 Timeline of APP fraud policies



Source: Frontier Economics

The reimbursement requirement

The APP scam reimbursement requirement came into force on 7 October 2024. It requires PSPs participating in FPS and providing relevant accounts to reimburse eligible victims of APP scams up to a maximum value of £85,000 per claim.

The Bank of England, as the operator of CHAPS, subsequently introduced comparable protections for consumers using CHAPS through the CHAPS Reimbursement Rules. These protections came into force in October 2024, alongside the protections for FPS users.

The PSR's objective was to strengthen fraud prevention and improve consumer protection by introducing consistent reimbursement obligations across PSPs. The policy, through mandatory reimbursement and shared liability, increases incentives for both sending and receiving PSPs to prevent APP fraud.[24] Key features of this policy are as follows:

[24] PSR (2023). PS23/4.

- **Liability sharing:** the liability for this reimbursement is shared equally between the sending and receiving PSPs involved in the transaction.
- **Time limit for reimbursement**: subject to some exceptions, the sending PSP must reimburse consumers within five business days. Where the PSP needs further information to assess the claim, it may "stop the clock", pausing the five-business-day period. However, the claim must still be closed by the end of the 35th business day following the consumer's report
- **Consumer standard of caution:** reimbursement is not required where the consumer has, because of gross negligence, failed to meet at least one of the following standards:
  - **Consider warnings**: consumers must consider any clear warnings or interventions that indicate the payment is likely a scam.
  - **Report to PSP promptly**: consumers must report the suspected scam to the PSP as soon as they are aware of it, and within 13 months of the last fraudulent payment.
  - **Respond to PSP requests**: consumers must respond to reasonable requests for information from their PSP to support the assessment of their claim.
  - **Report to police if required**: after making a claim, consumers must consent to their bank reporting the details to the police on their behalf or report it themselves if asked.[25]
- **Optional claims excess:** sending PSPs have the option to apply a claims excess of up to £100.
- **Maximum reimbursement limit:** the PSR has set the reimbursement limit at £85,000 per claim.
- **Vulnerable consumers:** the consumer standard of caution and claim excess cannot be applied to vulnerable consumers, where this vulnerability had a material impact on their ability to protect themselves from the scam.[26,27]
- **Scope**: the requirement applies to APP fraud payments executed by individuals, microenterprises and charities.[28] The requirement applies to all PSPs participating in FPS and CHAPS that provide relevant accounts, including both direct participants and indirect participants that access Faster Payments and/or CHAPS through a sponsor. The requirement also applies to multi-step frauds.[29] However, the requirement does not apply to civil disputes, payments which take place across systems other than FPS and CHAPS,

[25] These standards are set out fully here: PSR (2025) PS25/5.

[26] PSR (2023) Specific Requirement 1: Faster Payments APP Scam Reimbursement Rules. The Consumer Standard of Caution Exception; PSR (2024) Information on consumer communications for payment service providers (PSPs); PSR (2026) Policy clarifications.

[27] As set out in PSR (2025), PS25/5, A vulnerable consumer 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."*

[28] PSR (2025). Consolidated policy statement APP scams reimbursement requirement.

[29] As set out in PSR (2023) CP22/4 Fighting authorised push payment fraud, "*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… This document refers to them as multi-step fraud cases.*"

international payments or payments made for unlawful purposes. Payments made to crypto exchanges and "me to me" payments are also out of scope for the requirement.[30]

These protections build on and supersede the previous voluntary CRM Code. The reimbursement requirement strengthens the previous framework by making reimbursement mandatory for eligible APP scams, applying consistent rules across in-scope PSPs, and extending liability beyond firms that had voluntarily signed up to the CRM Code.

The reimbursement requirement also changed the allocation of liability for APP scam losses. Under the CRM Code, reimbursement obligations generally applied to the sending PSP where that PSP was a signatory to the Code. Receiving PSPs were generally not liable for reimbursing customers for inbound fraud. Under the reimbursement requirement, liability for reimbursable APP scam losses is shared equally between the sending and receiving PSPs. This means that receiving PSPs became financially liable for a share of reimbursable APP scam losses.

The table below summarises the main differences between the CRM Code and the reimbursement requirement.

Table 1 Key differences between the CRM Code and the reimbursement requirement

Feature	CRM code	Reimbursement requirement
Nature of scheme	Voluntary industry code	Mandatory regulatory requirement
Firms covered	Firms that had signed up to the CRM Code	All in-scope PSPs participating in FPS and CHAPS that provide relevant accounts
Sending PSP liability	Liability generally sat with the sending PSP where it was a CRM signatory	Sending PSPs are liable for 50% of reimbursable APP scam losses
Receiving PSP liability	Receiving PSPs were generally not liable for reimbursing customers for inbound fraud	Receiving PSPs are liable for 50% of reimbursable APP scam losses
Consumer standard	Reimbursement could be refused where the consumer had not met the expectations under the Code	Reimbursement is not required where the consumer has, as a result of gross negligence, failed to meet the consumer standard of caution
Claim excess and reimbursement limit	N/A	Sending PSPs may apply a claims excess of up to £100, and the maximum reimbursement limit is £85,000 per claim

Source: Frontier Economics

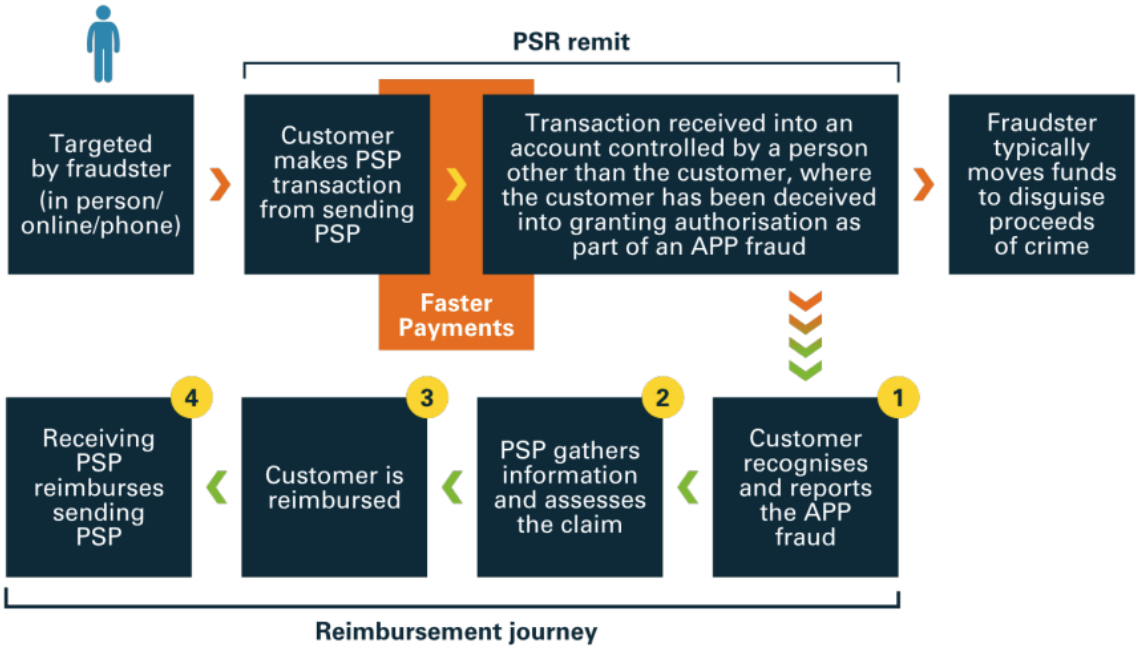
[30] Me to me payments are in scope if the evidence shows that the consumer was not in control of the beneficiary account.

Typical APP fraud payment and reimbursement journey

The core process for receiving and assessing claims under the new APP fraud reimbursement requirement operates as outlined in Figure 3 and as follows.

- **Reporting the scam:** the consumer reports a suspected APP scam to their PSP.
- **Notification of receiving PSP:** upon receiving the claim, the sending PSP must notify any receiving PSPs identified in the claim within two hours.
- **Assessment:** the sending PSP gathers and assesses the available information to determine the consumer's eligibility for reimbursement.
- **Reimbursement to consumer:** eligible claims are reimbursed to the consumer, while ineligible claims are rejected. Sending PSPs must reimburse consumers within five business days. Under certain circumstances, the sending PSP may "stop the clock" – pausing the reimbursement timeline while additional information is obtained.
- **Reimbursement to sending PSP:** all receiving PSPs contribute their share to the cost of reimbursement (reimbursable contribution amount).

Figure 3 A typical APP fraud payment and reimbursement journey



Source: PSR (2025) PS25/5 APP scams reimbursement requirement

Additional obligations

PSPs have several ongoing obligations under the new reimbursement requirement:

- **Reporting:** all sending directed PSPs must submit data on core metrics to Pay.UK covering all in-scope APP scam cases closed in the reporting period.[31] These metrics include total volumes and values of in-scope APP scam claims and number of claims reimbursed. This is used for compliance monitoring, is reported by senders only and does not identify performance by the receiving PSP. These metrics are known as Reporting Standard A.[32]

- **Record-keeping:** PSPs must retain relevant claim information for at least five years to support oversight and compliance monitoring.[33]

APP fraud performance data

In March 2023, the PSR required the 14 largest UK banking groups to collect and report APP fraud management data for subsequent publication.[34] The policy, known as Measure 1, required firms to submit standardised data on APP scam rates and reimbursement outcomes, enabling the PSR to publish comparable information on firms' APP fraud performance. This was intended to strengthen incentives on PSPs in two ways: by enabling consumers to consider APP fraud performance when choosing or switching provider, and by increasing reputational pressure on PSPs to reduce APP fraud and improve reimbursement outcomes.

The policy requires firms to report three key performance metrics:

- the proportion of APP scam victims who are reimbursed;
- the rate of APP scams for each sending PSP; and
- the rate of APP scams for each receiving PSP.

Unlike Standard A, which is described above, Measure 1 provides a breakdown of APP fraud data by receiving PSP, rather than only sending PSPs. PSPs report on the amount of APP fraud activity associated with each receiving firm, normalised by value (per £1 million of transactions) and by volume (per million transactions). Critically, this view spans scams sent from the 14 largest banks to any UK firm, so it can include smaller, non-directed receivers where relevant. The PSR has committed to publishing the results for these 14 PSP groups on its website annually.[35]

[31] For clarity, "directed PSPs" are PSPs that are formally addressed by the PSR's Specific Directions for the reimbursement requirement (FPS: Specific Direction 20 (PSR, 2024); CHAPS: Specific Direction 21 (PSR, 2024)). "Non-directed PSPs" are PSPs not addressed by those Directions.

[32] PSR (2024). Faster Payments APP scams: Compliance Data Reporting Standard. PSR (2024). Specific Direction 20.

[33] PSR (2024). Specific Direction 20.

[34] As per PSR (2024): Publishing APP scams data A guide for PSPs, the 14 largest PSP groups are comprised of the 12 largest banking groups in Great Britain by the number of payments they send across Faster Payments, plus the two largest independent banks in Northern Ireland by the same measure; together they account for over 95% of consumer Faster Payments by volume and value.

[35] PSR (2023). Cycle 2 Additional Changes to timelines and reporting periods.

3 Theory of change

As set out in HM Treasury's *Magenta Book*, a theory of change is a core building block for an impact evaluation.[36] It provides a structured way to identify how a policy is expected to lead to change, the outcomes and impacts that may result, and the groups that may be affected.

The theory of change is used to translate the in-scope policies into a testable evaluation framework. It maps the impacts that the in-scope policies are expected to have and the mechanisms through which those impacts are expected to occur, and the assumptions that need to hold for those impacts to materialise. This provides the basis for identifying the key evaluation questions, relevant indicators and evidence needed to assess whether the policies are working as intended.

In line with the *Magenta Book*, the theory of change was informed by engagement with industry, regulatory and consumer stakeholders.[37] This engagement helped to gather practical insights on how the policies may operate in practice, the changes they may bring about, and the groups that may be affected. The process was led independently by Frontier, building on and expanding the theory of change in the PSR's original cost-benefit analysis of the policies and using the stakeholder input to inform and refine the theory of change.

This section first explains the key changes in incentives created by the policies, as these are central to the expected causal pathways. It then presents the logic models, which summarise the theory of change in a structured format, and sets out the expected impacts, grouped under the four evaluation themes. Finally, it identifies wider contextual factors that need to be considered when interpreting the evaluation findings.

3.1 Key changes in incentives due to the policies

3.1.1 Reimbursement requirement

A central mechanism in the theory of change is how the reimbursement requirement changes incentives for PSPs. As shown in Figure 4, the reimbursement requirement changes the financial consequences of APP scam fraud for PSPs. The change in financial consequences differs depending on whether the PSP is sending or receiving funds, and whether the firm was previously signed up to the CRM Code.[38]

[36] HM Treasury (2025) Magenta Book: Central Government guidance on evaluation

[37] HM Treasury (2025) Magenta Book: Central Government guidance on evaluation

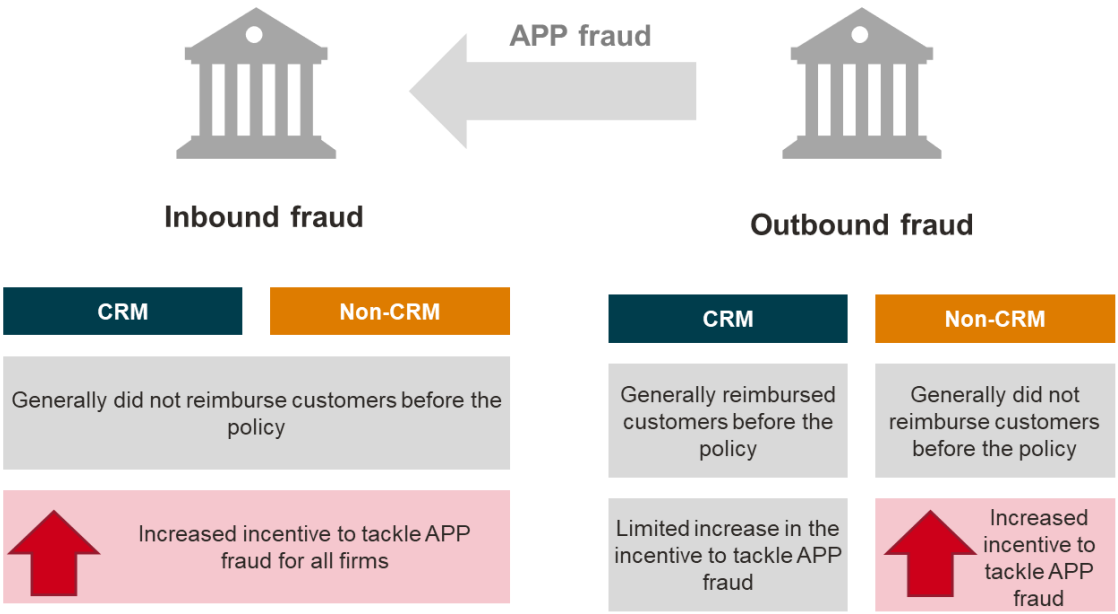
[38] Prior to the reimbursement requirement, TSB offered a fraud refund guarantee and their reimbursement rate in the PSR's 2024 APP Fraud Performance report was estimated at 80%, the second highest in the market. TSB is therefore treated as a CRM firm throughout this analysis despite not being a signatory to the code. The change in incentives for TSB is aligned to those of CRM firms.

Before the policy, both CRM and non-CRM firms generally did not reimburse customers for inbound fraud. Under the reimbursement requirement, firms became liable for 50% of their inbound fraud and this increased the incentive to tackle inbound fraud.

Pre-policy approaches to outbound fraud varied more significantly:

- Non-CRM firms did not generally reimburse customers for outbound fraud before the policy. For these firms, the reimbursement requirement increased the financial incentives to tackle outbound fraud, as they became liable for 50% of the value of outbound fraud.
- CRM firms tended to reimburse customers for outbound fraud, with reimbursement rates by value between 49% and 85%.[39] For these firms, the reimbursement requirement did not create the same step-change in financial incentives to detect and prevent outbound fraud.

Figure 4 Change in incentives from the reimbursement requirement



Source: Frontier Economics

These incentive effects are fundamental to the evaluation framework. Throughout the evaluation, we therefore analyse impacts on inbound and outbound fraud separately and explore differences between CRM and non-CRM firms.

3.1.2 Performance data

The performance data intervention is expected to operate primarily through increased transparency. By publishing comparable information on fraud incidence and reimbursement

[39] PSR (2026). 2024 APP scam performance data – before the reimbursement requirement was implemented.

rates, it is intended to increase awareness of PSP performance among PSPs, consumers, fraudsters, regulators and wider stakeholders. This, in turn, is expected to create reputational and regulatory incentives for PSPs to improve fraud prevention and reimbursement practices, while also informing consumer choice, regulatory oversight and wider stakeholder action.

3.2 Logic models and expected impacts

The logic model presents the theory of change in a structured format, showing the links between the policies, the changes in behaviour they may create, and the short-, medium- and longer-term outcomes that may follow. In doing so, it translates the theory of change into a framework that can be used to structure the evaluation questions, evidence collection and analysis.

The logic models for the expected impacts from the reimbursement requirement and performance data publication are provided in Figure 5 and Figure 6.[40]

There are implicit assumptions underlying the logic model that are needed for the policy to feed through into the expected short- and longer-term outcomes. These assumptions include, for example, that the PSPs comply with the policies and that consumers are aware of them. The evaluation needs to explicitly test these assumptions or test them implicitly by testing links in the logical chain. Evaluation questions were formulated to explore key outcomes of interest and test underlying assumptions. The evaluation questions are discussed in more detail in Section 4.

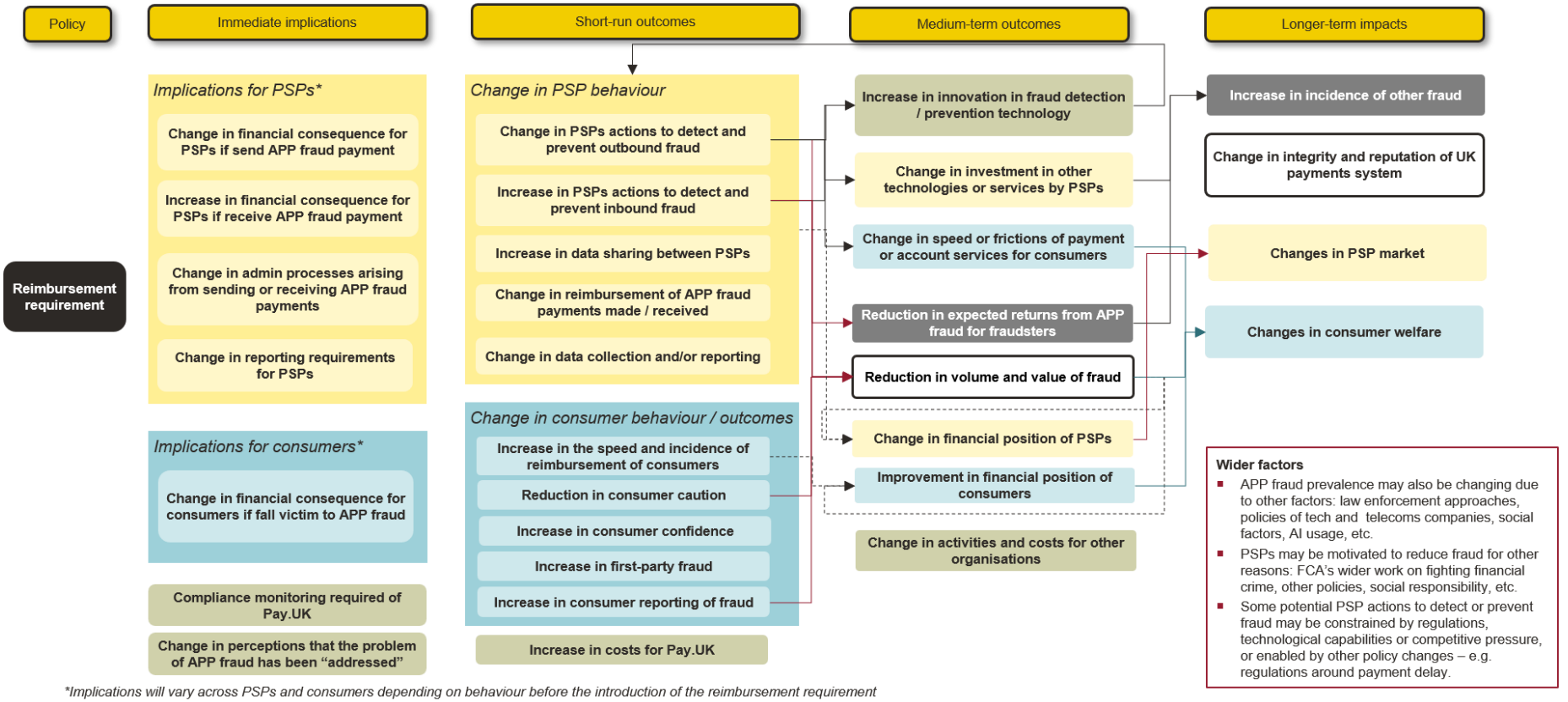
The expected impacts of the policies can be grouped into four evaluation themes. These themes reflect the main pathways through which the policies are expected to have an impact: PSP actions to tackle APP scams, fraud, consumer welfare, and PSPs and other markets. These themes provide the structure for the findings presented later in this report.

The sections below summarise the expected impacts shown in the logic models under each evaluation theme.

The themes are not intended to be mutually exclusive. They reflect different points in the causal chain, and all relate to one another, so some overlap is expected. For example, changes in APP fraud (Theme 2) are driven by both PSP actions (Theme 1) and consumer behaviour (Theme 2). Consumer behaviour has an impact on both APP fraud levels (Theme 2) and on outcomes for the PSP market (Theme 4).

[40] These logic models build on the cost benefit analysis carried out by the PSR in PS23/1 and PS23/3.

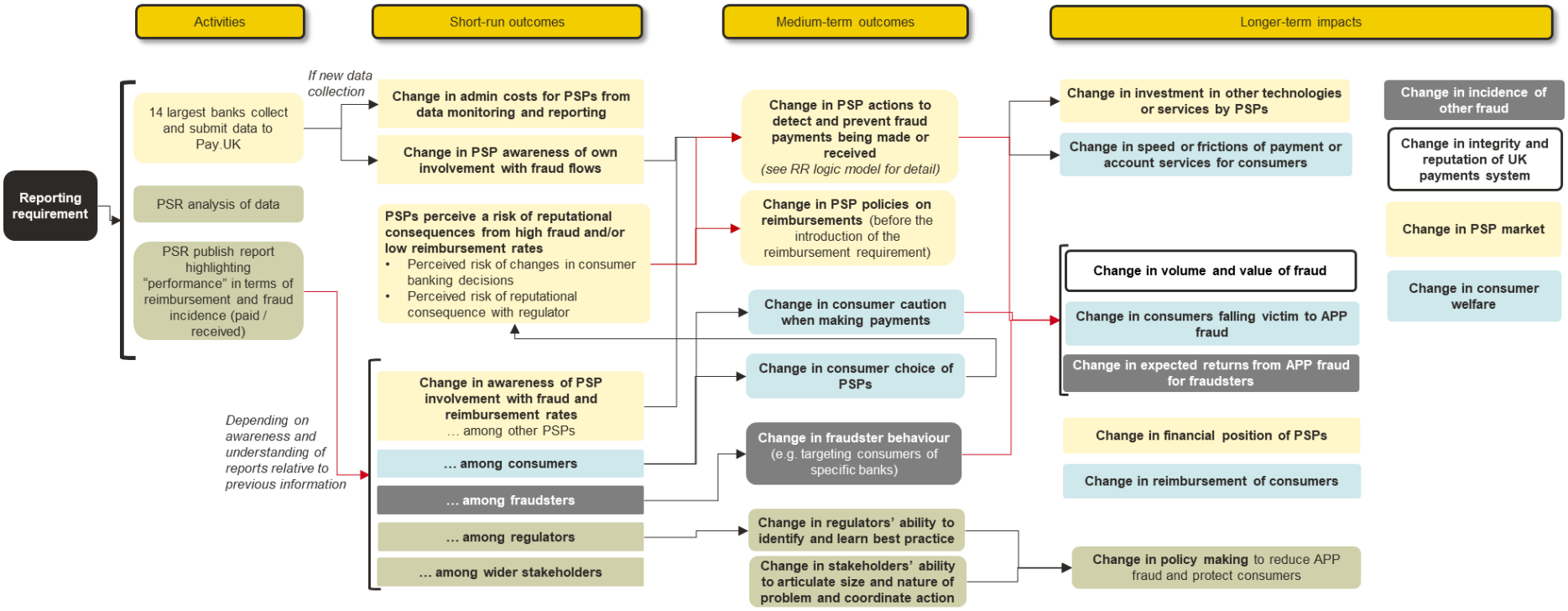
Figure 5 Theory of change: Introduction of the reimbursement requirement



Implications will vary across PSPs and consumers depending on behaviour before the introduction of the reimbursement requirement

Source: Frontier Economics

Figure 6 Theory of change: Publication of APP fraud performance data



Source: Frontier Economics

3.2.1 Theme 1: PSP actions to tackle APP scams

The policies are expected to affect PSP actions by changing the financial, operational and reputational incentives firms face in relation to APP scams. The reimbursement requirement changes the financial consequences of APP fraud for both sending and receiving PSPs, while the publication of APP fraud performance data increases transparency around firms' fraud and reimbursement outcomes.

The reimbursement requirement is expected to affect PSPs differently depending on their role in the payment chain, pre-policy fraud rates and their pre-policy reimbursement practices. For inbound fraud, the policy creates a stronger financial incentive for all PSPs to identify and prevent mule activity, as receiving PSPs become liable for a share of reimbursable APP scam losses. For outbound fraud, the expected change in incentives is greater for firms that did not previously reimburse customers, as these firms face a larger change in financial exposure. For firms that were already reimbursing customers, the policy may reinforce existing incentives or even reduce reimbursement exposure and therefore reduce incentives.

As a result, PSPs may change their approach to tackling APP fraud across different points in the fraud chain. This may include actions to detect and prevent outbound fraud, such as stronger transaction monitoring, more targeted warnings, customer interventions and payment controls. It may also include actions to detect and prevent inbound fraud, such as enhanced mule detection, stronger onboarding controls and tighter monitoring of accounts receiving suspicious funds. PSPs may also take steps to prevent the onward movement of suspected fraudulent funds, including holding or freezing funds, tracing linked accounts and improving recovery processes. Shared liability and operational requirements may encourage greater inter-PSP coordination, information sharing, claims reconciliation and fund recovery.

The policies may also create operational incentives for PSPs to improve how they manage APP fraud. For example, the reimbursement requirement was expected to increase PSPs' costs of compliance, including through additional claims handling, investigation, monitoring, reporting and customer communication requirements.[41] This creates a further incentive for PSPs to target fraud more effectively, both to reduce reimbursable losses and to limit the operational costs associated with processing APP fraud claims. The policies are also expected to affect how PSPs coordinate with each other, as shared liability and the need to investigate, reimburse and recover funds create stronger incentives for information sharing, claims reconciliation and inter-PSP cooperation.

The publication of APP fraud performance data is expected to operate through a different, and more indirect, mechanism. By making fraud and reimbursement performance more visible, it is expected to support benchmarking, senior-level scrutiny and reputational or regulatory incentives for PSPs to improve fraud prevention and reimbursement outcomes. PSPs may have an incentive to improve where the published data highlights relatively poor performance,

[41] PSR (2023). PS23/3, Annex 4: Cost benefit analysis.

exposes them to regulatory scrutiny, or creates reputational or commercial pressure from customers, competitors or wider stakeholders. However, the extent to which this affects PSP actions is expected to depend on whether PSPs, consumers, regulators and wider stakeholders use the published data in ways that create pressure for change.

Under the Theory of Change, firms are expected to consider actions to tackle APP fraud in response to these incentives. The scale and nature of those actions are expected to vary across PSPs. This reflects differences in their exposure to APP fraud, pre-policy reimbursement practices, size, operational capability and attitude to risk.

3.2.2 Theme 2: Impact on fraud

The policies are expected to affect fraud outcomes through changes in PSP behaviour, consumer behaviour and fraudster responses. If PSPs strengthen prevention, detection and recovery capabilities, this may reduce the volume and value of successful APP fraud, increase recovery rates and reduce APP fraud losses.

The expected impact on fraud is likely to vary across PSPs. For inbound fraud, PSPs with higher pre-policy levels of inbound APP fraud may face the greatest incentive, and have the greatest scope, to reduce fraud after the reimbursement requirement is introduced. For outbound fraud, CRM firms may already have had stronger incentives to prevent APP fraud due to their pre-existing reimbursement commitments and may therefore have had lower levels of outbound APP fraud before the policy. The reimbursement requirement may therefore create a greater change in incentives for non-CRM firms, particularly those with higher pre-policy outbound APP fraud rates, as they face a larger increase in financial exposure.

When interpreting changes in recorded APP fraud, the evaluation also needs to consider whether observed trends reflect changes in underlying fraud or changes in reporting, claiming or classification behaviour. This includes changes in consumer willingness to seek reimbursement, the treatment on the boundary between APP fraud and civil disputes, and potential changes in first-party fraud.

The policies may also have unintended impacts on fraud outcomes. These could include changes in consumer or business caution when making payments, fraudsters using performance data to target specific PSPs, or displacement into other types of fraud. PSP investment in APP fraud controls may also affect wider fraud outcomes, either through positive spillovers to broader fraud and financial crime capabilities or by diverting resources away from other fraud risks.

3.2.3 Theme 3: Expected impacts on consumer welfare

The policies are expected to affect consumer welfare through changes in APP scam reimbursement outcomes, fraud prevalence, consumer confidence and payment journeys. The reimbursement requirement is expected to reduce financial losses for eligible victims by increasing the likelihood, speed and consistency of reimbursement. If the policies also reduce

APP fraud over time, consumers may benefit from lower financial and non-financial harms associated with APP scams.

The overall impact on consumer welfare will also depend on how consistently consumers are treated across PSPs. Differences in how firms interpret and apply the reimbursement rules, including the consumer standard of caution, civil dispute exclusions, vulnerability assessments, the optional claim excess and the reimbursement cap, may lead to variation in consumer outcomes.

Reimbursement does not remove all consumer harms from APP scams. Victims may still experience non-financial harms, including stress, anxiety, shame, loss of confidence and reduced trust in others. As a result, reductions in APP fraud may improve consumer welfare by reducing the number of consumers exposed to these wider harms.

However, stronger fraud controls may also create costs for consumers and businesses. These may include additional payment journey frictions, payment delays, account freezes, false positives or restrictions on higher-risk payments. Some consumers may find it harder to open or maintain payment accounts, or to use certain payment services, if PSPs adopt more cautious onboarding, tighter account monitoring or restrictions on higher-risk activity. These effects may be particularly relevant for vulnerable consumers, consumers with limited financial history and business users whose payments are more time sensitive.

The policies may also affect wider trust and use of payment services. Additional friction could affect consumer or business willingness to use Faster Payments or Open Banking.

3.2.4 Theme 4: Expected impacts on PSPs and other markets

The policies are expected to affect PSPs' costs, operations, financial position and wider market outcomes. PSPs may face changes in reimbursement costs, fraud prevention investment, administrative and claims-handling costs, dispute management, reporting costs and compliance requirements. This reflects the cost categories identified in the PSR's cost benefit analysis, including reimbursement costs, implementation costs and ongoing operational costs associated with the reimbursement requirement.[42] These costs may arise both from the direct reimbursement obligation and from the operational changes needed to assess claims, coordinate with other PSPs, manage disputes and meet reporting obligations.

The scale and nature of these impacts are expected to vary across PSPs. Differences may reflect firms' size, business model, exposure to APP fraud, pre-policy reimbursement practices and ability to automate reporting and claims processes. For some PSPs, particularly smaller or growing firms, reimbursement liabilities and operational costs may represent a larger share of revenues and capital. This could affect profitability and their ability to attract capital. In more

[42] PSR (2023). PS23/3, Annex 4: Cost benefit analysis.

severe cases, where liabilities are material relative to a PSP's financial resources, the policies could increase financial resilience risks, including the risk of firm exit or insolvency.

Increased financial exposure from APP fraud may strengthen the commercial case for investment in fraud detection and prevention technology, including transaction monitoring, analytics, external data sources, consortium data, AI tools and customer risk profiling. Investment in APP fraud prevention may also generate positive spillovers, where improvements in data, systems, controls or analytical capability help PSPs to detect and prevent other types of fraud or financial crime. This may increase demand for anti-fraud technology and support innovation in the fraud technology market. At the same time, investment in APP fraud prevention and compliance may reduce the resources available for other priorities, including product development, service improvements, payments innovation or controls for other types of financial crime.

The policies may also affect other organisations involved in APP fraud claims, oversight or enforcement. Pay.UK, industry organisations, regulators, law enforcement, the FOS and Trading Standards may face changes in costs, infrastructure requirements, monitoring activity, caseloads or resource allocation.

Over the longer term, the policies may affect wider market outcomes. Higher liability exposure could affect market entry, market participation, competition and the attractiveness of the UK payments sector to investors. PSPs may also adjust service offerings, onboarding practices or provision to higher-risk customer segments or payment types to manage fraud and liability risks.

3.3 Wider contextual factors

The impacts of the reimbursement requirement and the publication of APP fraud performance data will occur alongside broader factors that shape APP fraud outcomes. These include changes in scam tactics, law enforcement activity, telecoms and online platform interventions, macroeconomic conditions, payment technology and the use of AI by both fraudsters and PSPs.

These factors are not directly within the scope of the policies, but they are important context for interpreting the evaluation findings. The evaluation therefore focuses on outcomes for which there is a clear pathway of influence from the policies in scope of the evaluation, while taking wider developments into account when interpreting the evidence.

4 Evaluation approach

In this impact evaluation, we assess what difference the PSR's APP scam policies have made to market outcomes. To do this, we compare current market outcomes with a counterfactual – the hypothetical world in which the in-scope policies were not introduced. This allows us to assess what changes have occurred, the scale of those changes, and the extent to which they can be attributed to the APP scam policies.

The counterfactual is not observable and there is no clear evidence to indicate what would have happened to APP fraud in the absence of the PSR's APP scam policies. On one hand, APP fraud may have risen during this period due to increased use of technology for payments and the sophistication of tools available to fraudsters such as AI. On the other hand, PSPs may have invested in bringing down APP fraud in the absence of the policies for example, due to the strain on resources from managing consumer claims. Many other factors influence APP fraud levels too, such as law enforcement approaches, policies of tech and telecoms companies, social factors and the wider economic environment, for example the cost-of-living pressures.

The evaluation questions were designed to test each stage of the causal chain set out in the theory of change and logic model. They assess the expected progression from policy inputs and activities through to outputs, outcomes and impacts. In practice, this involves examining whether PSPs have changed their actions to tackle APP scams, whether those actions have affected levels of APP and other fraud, how any resulting changes have affected consumers, and whether there have been wider impacts on PSPs and other markets.

We used the theory of change to inform the evaluation questions and structure the assessment. The questions were designed to test the expected progression from policy inputs and activities, through to outputs, outcomes and impacts. In practice, this means assessing whether PSPs have changed their actions to tackle APP scams, whether these actions have affected levels of APP and other fraud, how these changes have affected consumers, and whether there have been wider impacts on PSPs and other markets.

We approached the evaluation as follows.

- **Developed evaluation questions based on the theory of change.** We used the theory of change and logic model to translate the expected causal chain into evaluation questions. The questions were designed to test each stage of this chain, covering inputs and activities, outputs and outcomes, and impacts. This included questions on PSP actions to tackle APP scams, changes in APP fraud and other fraud, consumer welfare, and wider impacts on PSPs and other markets.

- **Validated the evaluation questions and approach with key stakeholders**. We reviewed the evaluation questions and proposed approach with key stakeholders in stakeholder interviews and workshops to test whether they reflected the policy objectives

and expected market changes at time of implementation, key evidence sources and potential unintended consequences. We used this feedback to refine the evaluation questions and confirm the scope of evidence collection.

- **Evidenced each pathway:** We gathered and assessed quantitative and qualitative evidence against each evaluation question. This allowed us to test whether the expected changes in the theory of change had occurred and whether there was evidence of unintended consequences.

- **Assessed effectiveness:** We assessed the effectiveness of the in-scope APP fraud policies by considering the evidence against each evaluation question, the scale of observed changes, and the extent to which those changes could be attributed to the policies rather than to other factors.

The rest of this section sets out the evaluation questions, methodology and evidence sources in more detail. Section 4.1 presents the evaluation questions, grouped under the four evaluation themes. Section 4.2 explains the theory-based contribution analysis approach used to assess impact. Section 4.3 describes the data and evidence sources used in the evaluation.

4.1 Evaluation questions

The impact evaluation is structured around four themes, with each theme comprising several evaluation questions. Together these evaluation questions capture the most important expected outcomes and impacts of the APP scam policies as set out in the theory of change. These questions capture both the intended outcomes of the policy and the unintended consequences of the policy.

These questions are set out below.

Theme 1. Impacts on PSP actions to tackle fraud

1. Have PSPs taken action to tackle APP fraud?
2. To what extent are PSPs' actions attributable to the APP scam policies as opposed to driven by other factors?

Theme 2: Impacts on fraud

1. How has the level of APP fraud changed?
2. What impact have the in-scope APP scam policies had on APP fraud?
3. How have levels of other fraud changed?
4. To what extent are the changes in other fraud attributable to the APP scam policies as opposed to driven by other factors?

Theme 3: Impacts on consumer welfare

1. What has been the impact of the policies on victims of APP fraud?
2. How consistently have consumers been treated by different PSPs?
3. How has the change in the level of APP fraud impacted consumers?

4. Have the policies led to increased payment friction for consumers and businesses?
5. Have there been any adverse effects on consumer or business usage of FPS and/or Open Banking?

Theme 4: Impacts on PSP and other markets

1. How have the policies affected the costs faced by PSPs?
2. What has been the impact on PSPs' financial position?
3. What has been the impact on the market for anti-fraud technology?
4. How have the policies affected the costs faced by other organisations involved in managing fraud?
5. What might be the potential longer-term effects on service quality, innovation, and economic growth?

We updated the evaluation questions during the analysis phase to align with the structure of our findings. The mapping between the original evaluation questions set out in the Evaluation framework report and the final evaluation questions is provided in Annex A.

4.2 Impact evaluation methodology

We use theory-based contribution analysis as the overarching approach for the impact evaluation. Theory-based methods investigate impacts by testing the causal chains through which an intervention is expected to affect outcomes. As noted in the *Magenta Book,* these methods are particularly well suited for the evaluation of complex interventions and complex environments.[43] This method is appropriate here because, as Section 3 shows, the in-scope policies are expected to affect outcomes through multiple, interrelated pathways. Contribution analysis allows the evaluation to test whether these pathways are supported by the evidence and to consider alternative explanations for observed changes

A contribution analysis approach is appropriate for this evaluation because a robust counterfactual econometric design is not feasible. The in-scope APP fraud policies affected firms across the market at broadly the same time, meaning there is no untreated group of firms that can be used as a control group. APP fraud and PSPs' efforts to tackle it are also highly context-specific, so other markets or geographies would not provide a sufficiently comparable benchmark. In addition, firm-level APP fraud outcomes are driven by factors that are difficult to observe and measure consistently, including fraudster targeting, PSP control environments, customer bases, reporting behaviour and claims handling practices. This means that we cannot use firm and market variables to construct a robust synthetic control group.

Under a contribution analysis framework, a reasonable claim of causality can be made if three conditions are met:

[43] HM Treasury (2025). Magenta Book: Central Government guidance on evaluation.

- There is a clearly specified theory of change that has been discussed and agreed with key stakeholders.
- The main pathways to impact are supported by evidence on activities and outputs delivered, outcomes of interest and the key assumptions.
- Other factors that could plausibly have influenced outcomes have been identified and considered.

Within the contribution analysis framework, we use a mixed-methods approach to triangulate evidence on the expected causal pathways from multiple sources. This provides a robust basis for assessing what changes can be attributed to the policies. The methods and analytical approaches brought together include:

- **Realist evaluation.** This has a particular focus on "what works, for whom and in what circumstances", recognising that context is important for determining whether, and how, hypothesised causal mechanisms operate.
- **Process tracing.** This is a method for developing and assessing theories for how a particular outcome arose. Hypothesised causal mechanisms are identified using a theory of change, and then evidence is collected on outcomes that would be observed if a theory were true and outcomes that would be observed if the theory were false.
- **Time series and timing of events analysis**. This tracks changes in key outcomes of interest over time and can be used, under some circumstances, to associate changes in outcomes with drivers of those outcomes based on the timing of events.
- **Qualitative evidence.** This includes stakeholder interviews to gather detailed insights on whether and how the policies have had an impact, why impacts may or may not have occurred, and the role that other factors may have played.
- **Descriptive analysis**. This provides key contextual information or descriptions of metrics that are measured as snapshots rather than repeatedly over time.

Together these methods allow us to balance breadth and depth. The quantitative analyses provide coverage across a wide range of providers but offer limited insight into the underlying mechanisms, while the stakeholder interviews allow us to explore those mechanisms in depth but cannot represent the whole market. Combining these approaches helps address the limitations of each and strengthens the overall contribution narrative.

4.3 Data and evidence sources

The impact evaluation draws on a range of quantitative and qualitative evidence sources. These sources include data collected directly for the evaluation, existing industry and regulatory datasets, stakeholder interviews, case studies, survey evidence, and input from the Working Group and Advisory Group.

4.3.1 Definition of APP fraud

APP fraud can be defined in different ways. For the purposes of the analysis in this report, where we use the term "APP fraud" or "APP scams", we mean an FPS or CHAPS APP scam payment aligned with Specific Direction 20 and 21 (SD20 and SD21): an Authorised Push Payment, authorised by a victim as part of an APP scam, that has all the following features.[44]

- It is executed through the Faster Payments Scheme or CHAPS.
- It is authorised by a PSP's consumer.
- It is executed by that PSP in the UK.
- The payment is received in a relevant account in the UK that is not controlled by the consumer.
- The payment is not to the recipient the consumer intended or is not for the purpose the consumer intended.

4.3.2 Industry evaluation data

To support the evaluation, a mandatory data request was issued to 23 PSPs using the PSR's section 81 information-gathering powers.[45] This data request allowed us to collect data on a range of metrics on a consistent basis over time:

- Monthly data on APP scam payments sent and received;
- Consumer claims activity, reimbursement outcomes and repatriation;
- Consumer caution indicators; and
- Actions PSPs have taken to detect or prevent fraud.

The sample of PSPs was selected to be representative of the UK payments landscape and capture both high-volume participants and those with elevated exposure to APP fraud. We selected firms based on three criteria:

- **Market coverage:** PSPs that collectively account for around 95% of Faster Payments transaction volumes (May 2025 – July 2025) provided they had at least one APP scam claim in between October 2024 and January 2025; [46]
- **Absolute APP fraud exposure**: Firms in the top quartile (25%) of APP scam claims volumes; [47] and

[44] PSR (2024). Specific Direction 20. PSR (2024). Specific Direction 21.

[45] Financial Services (Banking Reform) Act 2013, s.81.

[46] Pay.UK data (2025).

[47] Based on FPS Standard A data (Oct 2024 – Jan 2025).

- **Relative APP fraud exposure**: PSPs ranked in the top 20 for APP scam value or volume per million transactions in the 2023 fraud performance dataset.[48]

The sample covers 95% of the UK payments market by FPS payment volume and value. We scale up our results from the sample by a factor of 1/0.95 to estimate market-level impacts on APP fraud. This assumes that the APP scams outside our sample have changed at the same rate as APP scams among firms in our sample, which is a plausible assumption.

The sample included 11 firms that were part of the CRM scheme or had reimbursement rates very closely aligned to CRM firms, and 12 firms that were not part of the CRM scheme.[49] We have further segmented firms by size to derive the following four PSP categories used in the analysis.[50,]

- **Large CRM PSPs (6 firms):** CRM signatories that have FPS volumes of more than 5% of the total market FPS volume.
- **Medium to small CRM PSPs (5 firms):** CRM signatories with FPS volumes of less than 5% of the market.
- **Medium to large non-CRM PSPs (5 firms):** non-CRM signatories with FPS volumes or values above 0.5% of the market.
- **Small non-CRM PSPs (7 firms):** non-CRM signatories with FPS volumes and values below 0.5% of the market.

The analysis was tested by distinguishing between banks and non-banks for all the impacts. There were no consistent trends in the results within these groups, so these results are not reported.

The data covers the period from April 2023 to September 2025. This includes 18 months before the reimbursement requirement came into effect and one year after implementation. Data for a long period prior to implementation is important to capture anticipation effects. The impacts of the reimbursement requirement are expected to be felt earlier than implementation, as firms are likely to take action to reduce their exposure to fraud as soon as they are clear the policy will be implemented, rather than waiting until the reimbursement requirement comes into force. The starting date of April 2023 for the data collection was chosen to balance the burden of the data request on PSPs with the desire to document metrics of interest for a period before the policies were introduced.

[48] PSR (2024). Authorised push payment (APP) scams performance report. See *Metric C: Value and Volume of APP scams received per £ million of transactions (p17-p23).*

[49] Prior to the reimbursement requirement, TSB offered a fraud refund guarantee and their reimbursement rate in the PSR's 2024 APP Fraud Performance report was estimated at 80%, the second highest in the market. TSB is therefore treated as a CRM firm throughout this analysis despite not being a signatory to the code.

[50] We use total FPS payment volume and value data from Pay.UK for the period May 2025 – July 2025 combined with firm submissions on the volume and value of indirect access transactions they provide as a sponsor bank for this segmentation.

The data was collected between December 2025 and February 2026.

There are some differences in the data provided on APP scams between different PSPs. Most PSPs provided data on all APP scams meeting the definition set out in Section 4.3.1, but for some PSPs APP scams that are not in scope of the reimbursement requirement, such as crypto payments and payments between two accounts held by the same individual were excluded. These differences have implications for how we interpret reimbursement rates between different PSPs and are further discussed in Section 7.2.

For claims where a proportion of the payments meets the definition of an APP scam and a proportion of payments does not (such as due to not being sent over FPS or CHAPS), some PSPs were unable to separate the value of losses that does not meet the APP scam definition, and this is included in the dataset we use. This only affects a small proportion of claims and PSPs and is not expected to have a significant impact on our analysis.

Several PSPs were only able to report a part of the data that we requested. For example, firms that only participate in FPS as sponsor banks for indirect access providers and do not have any direct FPS transactions were unable to provide data on FPS transactions. Some of the data fields that we requested (for example, data on consumer APP fraud claims before the reimbursement requirement) were not recorded by several PSPs and therefore not provided in the industry evaluation data request. We are confident that these exclusions do not affect our findings as there were enough firms across all PSP types with available data in the sample. Further, the data coverage for firms that constitute most of the payment market was high.

We have adopted a pragmatic approach and used the data from all of the firms that it was available for in each part of the analysis. The number of individual PSP results reported in different sections of the report varies for this reason.

4.3.3 Voluntary evaluation PSP survey

We issued a voluntary survey by email through industry organisations to all PSPs to collect predominantly qualitative insights.[51] The survey was also shared with other industry participants, industry groups and claims management companies, as an opportunity to feed in further insights.

The survey collected evidence on:

- Actions PSPs have taken to detect or prevent fraud;
- Perception of APP scam prevalence;
- Indicators of payment frictions and consumer experience;
- Costs associated with in-scope APP scam policies;
- Perceptions of longer-term implications of in-scope APP scam policies; and

[51] The industry organisations that distributed the survey are UK Finance, The Payments Association and Innovate Finance.

- Perceptions of the effectiveness of in-scope APP scam policies.

The data was collected between December 2025 and February 2026. Each industry body shared the survey with all their member PSPs. We received 15 responses that are incorporated into our analysis.

4.3.4 Stakeholder interviews

We conducted 25 semi-structured interviews with a range of stakeholders between January and February 2026. The interviews were designed to capture a depth of perspective on whether, and how, the in-scope APP fraud policies have affected key outcomes of interest, and the extent to which observed changes may also be explained by wider factors.

Interviewees were selected to provide a broad range of perspectives across the APP fraud ecosystem. This included PSPs of different sizes, business models and market segments, including firms with different approaches to reimbursement before the reimbursement requirement. We also invited industry and trade bodies, fraud technology providers, consumer groups and other stakeholders involved in fraud prevention, enforcement or claims management. Not all stakeholders invited to participate were willing to take part.

We interviewed:

- Eleven PSPs, covering different business models and market segments;
- Four industry and trade bodies;
- Four consumer groups;
- Three fraud technology providers; and
- Three other stakeholders involved in fraud enforcement and claims management.

The stakeholder interviews followed topic guides aligned to the evaluation questions. This allowed us to explore common themes consistently across stakeholders, while also giving interviewees flexibility to raise issues specific to their role or experience. Where permission was granted, interviews were transcribed. Stakeholder interview evidence was then synthesised against the evaluation questions and used alongside quantitative evidence and other qualitative inputs to inform the contribution analysis.

4.3.5 Existing data sources

We also drew on a range of existing data sources.

- **Standard A (Compliance Data Reporting Standards**) is data collected from sending PSPs. It is reported to Pay.UK for FPS payments and to the Bank of England for CHAPS payments. It includes data on customer claims and reimbursements and has been collected monthly since October 2024.[52]

[52] Provided by the PSR.

- **PSR APP Fraud Consumer Survey.** This is a survey of 1,509 members of the public commissioned by the PSR. It captures consumer awareness of the ability to claim, behavioural responses, and the financial and non-financial harms associated with falling victim to fraud. It was carried out in January 2025.[53]
- **UK Finance Fraud Reporting data.** Aggregated industry-level data on APP scam and other fraud claims, allowing comparison across time and between different types of fraud.[54]
- **FCA-PSR Joint Survey.** The FCA and PSR issued a voluntary survey to a selection of PSPs in July 2025. The survey included a range of both qualitative and quantitative questions relating to APP scams such as industry costs, APP scams not in scope of the reimbursement requirement and suspected first-party fraud.[55]
- **APP fraud performance data (Measure 1).** Data is collected by the PSR from 14 major PSP groups covering over 95% of consumer Faster Payments. Summary data is published by the PSR.[56] The data covers APP scam rates by PSP and proportion of victims reimbursed before the reimbursement requirement.
- **Other data sources**: data from the FCA on Regulatory Sandbox uses and metrics on firm financial performance, the Extended Industry Sort Code Directory (EISCD) provided by Pay.UK, FOS complaints data and customer switching data from CASS.[57]

4.3.6 Other qualitative inputs

The evaluation was supported by a Working Group and an Advisory Group. These groups were used to test hypotheses, methodology and emerging findings and to provide independent challenge and contextual input at key milestones of the evaluation.

- The Working Group consisted of representatives from the PSR, the FCA, HM Treasury, the Bank of England as the operator of CHAPS, and the Home Office.
- The Advisory Group consisted of UK Finance, The Payments Association, Innovate Finance and Which? in addition to the Working Group members.

[53] PSR (2025). APP Fraud Survey 2025.

[54] UK Finance (2025). Half Year Fraud Report 2025. UK Finance (2026). Annual Fraud Report 2026.

[55] Provided by the FCA.

[56] PSR (2025). APP fraud performance data.

[57] https://www.wearepay.uk/what-we-do/switching-services/current-account-switch-service/current-account-switch-service-statistics/

5 Theme 1 Findings: Impacts on PSP actions to tackle fraud

In this theme we first examine whether PSPs have acted since April 2023 to enhance their detection and prevention of APP fraud and how this varies across PSPs. We then explore the question of whether any of this action can be attributed to the PSR's APP scam policies or whether it would have happened regardless. We examine actions since April 2023 to reflect that some firms may have started taking actions in response to the reimbursement requirement policy being developed and announced, rather than waiting to act until the reimbursement requirement came into force.

5.1 Have PSPs taken action to tackle APP fraud?

5.1.1 Firms have taken a wide range of actions to tackle APP fraud

Firms have taken a wide range of actions to tackle APP fraud since April 2023. Some of these actions reflect incremental improvements to existing fraud controls and continued investment in established programmes of work. However, many firms also reported significant new activity, including new controls, enhanced analytics, greater use of external providers and more targeted interventions across different stages of the fraud chain.

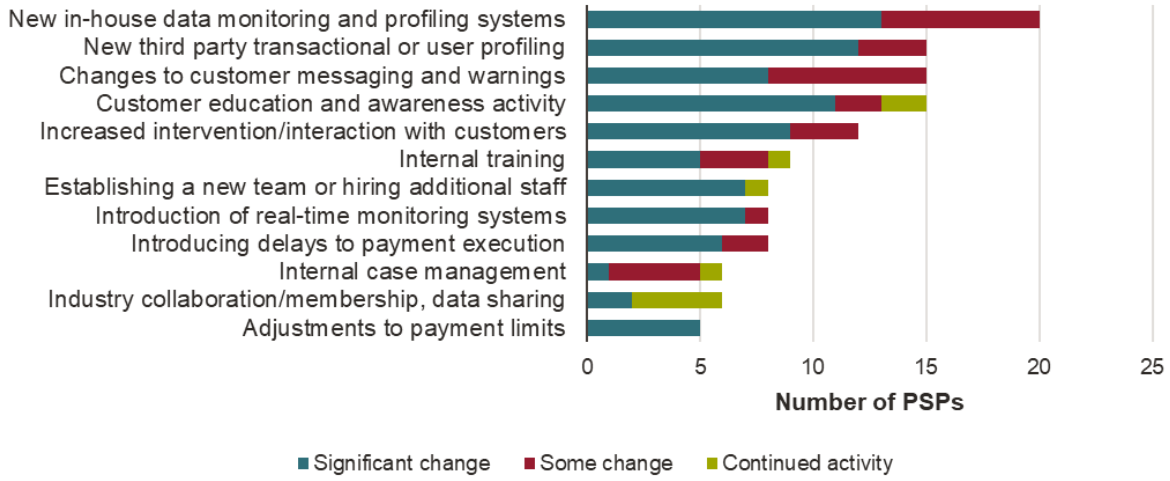
We obtained detailed information on PSPs' actions to tackle APP fraud through qualitative questions in the industry evaluation data request and the voluntary evaluation PSP survey, as well as through the stakeholder interviews with PSPs.

To provide an indication of the breadth and strength of different actions across PSPs we conducted a classification exercise on the qualitative data provided by PSPs. For these PSPs we categorised whether they mentioned actions of various types. We then categorised whether those actions were most likely to be a continuation of existing activity, some increase in existing activity, or a significant increase in activity (including completely new activity). This categorisation should be viewed as illustrative, as it is our subjective classification of qualitative information provided by PSPs. Nevertheless, it gives a helpful sense of the breadth and intensity of actions taken by PSPs.

Actions taken to prevent outbound APP fraud

The results of this classification exercise for PSP actions to tackle outbound fraud are shown in Figure 7. Overall, the figure suggests that PSPs have focused most heavily on strengthening fraud detection and customer-facing interventions. The most commonly reported areas of increased activity were new in-house data monitoring and profiling systems, changes to customer messaging and warnings, customer education and awareness, new third-party transactional or user profiling, and increased intervention or interaction with customers.

Figure 7 Outbound fraud prevention activity undertaken by firms since 2023



Source: *Frontier analysis of industry evaluation data and the voluntary evaluation PSP survey.*

Note: *PSP free-text submissions on the types of activity undertaken since 2023 have been classified into types of activities and the scale of activity by Frontier. These subjective classifications should be viewed as illustrative.*

Drawing on the classification exercise and evidence from stakeholder interviews, we identified several main areas of PSP activity since April 2023.

- **New in-house data monitoring and profiling systems.** As shown in Figure 7, this was the most reported area of activity, with 20 PSPs reporting increased activity. In stakeholder interviews and the voluntary evaluation PSP survey, most firms reported increases in the scale or sophistication of their in-house monitoring and profiling systems to combat outbound fraud. Various PSPs told us that they had enhanced their use of machine-learning capabilities to detect fraud risk.

- **Changes to customer messaging, warnings, education and awareness.** Customer-facing activity was also a major area of focus. Around 15 PSPs reported changes to customer messaging and warnings, and a similar number reported increased customer education or awareness activity. In stakeholder interviews, firms highlighted increased use of customer-facing warnings and questions to interrupt potentially fraudulent outbound payments. Many moved beyond simple value-based transaction thresholds towards more targeted, analytics-driven interventions. Some PSPs described continually refining these interventions, testing different warning designs by scam type and transaction value to improve effectiveness. Some described refining these interventions over time, including testing different warning designs by scam type and transaction value.

- **Increased use of third-party providers.** Many PSPs reported greater use of external providers to support outbound fraud detection and prevention. Interviewees told us that these included providers offering external data, advanced analytics, destination-risk information, and device-level behavioural or biometric profiling to help identify social-engineering and other APP fraud risks.

- **Increased intervention and interaction with customers.** Around 12 PSPs reported increased intervention or interaction with customers. In stakeholder interviews, some PSPs created or expanded specialist teams to handle complex or high-risk cases in real time. Interviewees told us that these teams often involved labour-intensive direct customer engagement aimed at interrupting the scam and helping customers reassess the transaction, or "breaking the spell".

- **Stronger payment controls.** Eight PSPs reported introducing payment holds or pauses for transactions flagged as high risk, pending investigation. Interviewees described strengthening the behavioural effectiveness of existing controls, such as Confirmation of Payee, and moving beyond minimum compliance to deliver clearer fraud warnings.

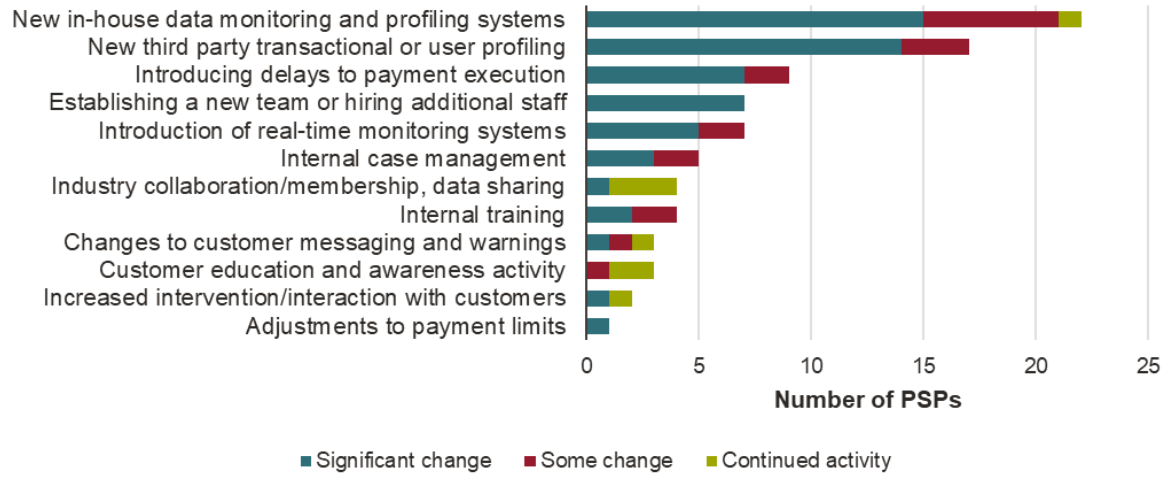
- **More targeted outbound controls for specific risks.** In stakeholder interviews, some PSPs described blocking or restricting crypto payments or focusing protection efforts on vulnerable customers, rather than applying blanket friction across all users.

- **Internal capability building, including training, staffing and case management.** PSPs also reported internal operational changes to support stronger fraud prevention. Around nine PSPs reported increased internal training, around eight reported establishing a new team or hiring additional staff, and around six reported changes to internal case management.

Actions taken to prevent inbound APP fraud

PSPs also reported measures aimed at identifying and preventing accounts from being used to receive fraudulent funds (inbound fraud). The results of the classification exercise for these actions reported by PSPs are shown in Figure 8. Compared with outbound fraud, PSP activity was more concentrated in a smaller number of areas. The most commonly reported actions related to new in-house data monitoring and profiling systems and new third-party transactional or user profiling. A smaller number of PSPs also reported increased activity relating to real-time monitoring, payment delays, internal case management, additional staff or specialist teams, and industry collaboration or data sharing.

Figure 8 Inbound fraud prevention activity undertaken by firms since 2023



Source: *Frontier analysis of industry evaluation data and the voluntary evaluation PSP survey.*

Note: *PSP free-text submissions on the types of activity undertaken since 2023 have been classified into types of activities and the scale of activity by Frontier. These subjective classifications should be viewed as illustrative.*

Drawing on the classification exercise and stakeholder interview evidence, PSP activity can be grouped into several broad areas:

- **New or enhanced mule detection capabilities**. In interviews, PSPs reported strengthening inbound transaction monitoring to better identify mule activity and evolving fraud risks. This enabled faster action on suspected mule accounts. This included faster freezing or restricting suspicious accounts or funds once risky activity was detected.

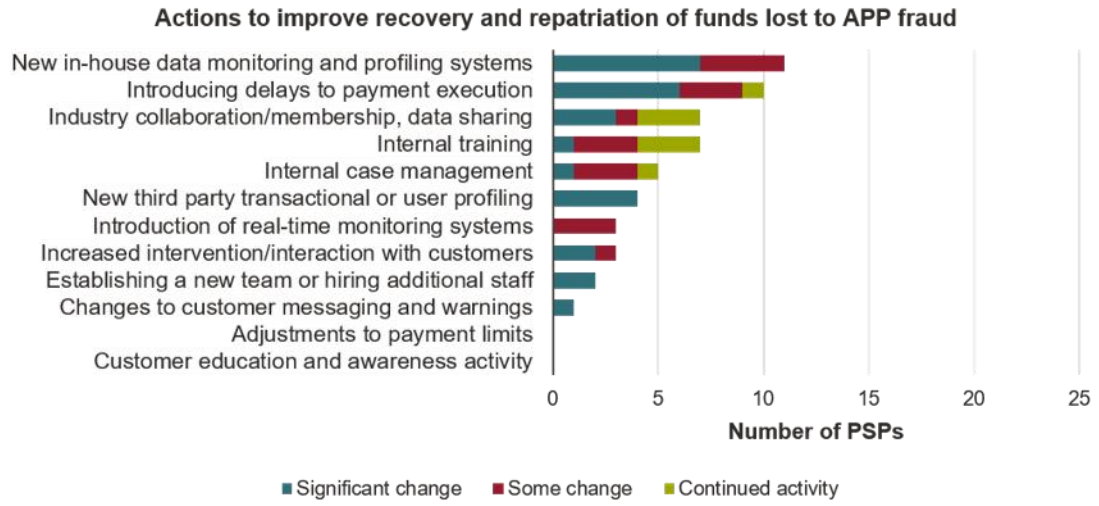
- **Increased use of third-party providers**. In interviews, several PSPs reported increased use of third-party providers to help identify mule networks and assess account risk, including the use of scam-baiting intelligence. For example, one PSP told us, "*We're trialling a few fintechs… that work on the consumer end or in social media to try to find dodgy mule accounts… a whole bunch of innovation in that space.*"

- **Stronger controls earlier in the customer lifecycle.** Several PSPs reported strengthening onboarding controls to prevent fraudulent or mule accounts from being opened. Measures described included introducing new machine-learning models during onboarding, identifying patterns of activity associated with known or suspected scammers, and making more explicit risk-based decisions to deny account opening where applicants fell outside their fraud risk appetite.

Actions taken to prevent onward transfers of fraudulent funds

Many firms described introducing measures aimed at preventing the onward movement of suspected fraudulent funds or recovering funds lost to scams, though Figure 9 shows such measures were less commonly reported than actions to prevent inbound or outbound fraud.

Figure 9 Activity to prevent onward transfer of fraud undertaken by firms since 2023



Source: *Frontier analysis of industry evaluation data and the voluntary evaluation PSP survey.*

Note: *PSP free-text submissions on the types of activity undertaken since 2023 have been classified into types of activities and the scale of activity by Frontier. These subjective classifications should be viewed as illustrative.*

Interviewees provided further insight into actions taken to prevent onward transfer of fraudulent funds, including:

- **Holding or freezing inbound funds where fraud risk was identified**. Many PSPs described taking steps to hold or freeze incoming payments where fraud risk is identified, preventing onward transfers while checks are undertaken.
- **Greater focus on second-generation mule activity**. Several firms highlighted an increased focus on mule detection, including identifying second-generation mules and tracing links between accounts, and in some cases freezing entire receiving accounts, including where recipients were thought to be unwitting mules.

Repatriation of funds from receiving PSPs to sending PSPs

While the qualitative evidence shows that PSPs have taken steps to detect and freeze fraudulent funds, industry evaluation data combined with Standard A data provides a quantitative indication of how often those efforts result in funds being repatriated by receiving PSPs. This data relates to claims made after the introduction of the reimbursement requirement. It therefore shows the extent to which, under the new regime, sending PSPs reported that receiving PSPs had repatriated funds in FPS APP scam claims. This is captured through repatriation rates, measured both by claim value and by claim volume.

Overall, sending PSPs reported that receiving PSPs repatriated funds equivalent to 16% of the total value of claims. Larger PSPs reported a higher proportion of outbound fraud claim

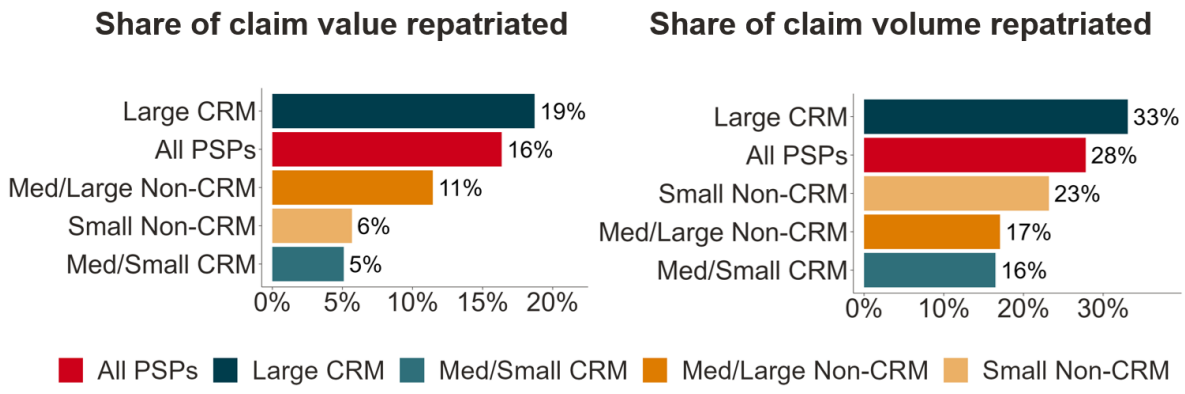
value being repatriated by receiving PSPs. Large CRM firms reported that receiving PSPs repatriated funds equivalent to 19% of the fraud value they sent, while medium and large non-CRM firms reported 11% of claim value being repatriated. This compares with 5% to 6% for small CRM and small non-CRM firms.

Looking at claim volumes, sending PSPs reported that receiving PSPs repatriated some or all funds in more than a quarter of cases, at 28% overall. Large CRM firms reported repatriation by receiving PSPs in a third of cases. This was higher than the rate reported by medium and large non-CRM firms, at 17%, small CRM firms, at 16%, and small non-CRM firms, at 23%.

These results should be interpreted as differences in reported repatriation outcomes for claims where the firm was the sending PSP, rather than direct evidence of receiving PSP behaviour in isolation. While receiving PSPs may freeze and return funds, successful repatriation also depends on how quickly and effectively sending PSPs identify suspected fraud, notify receiving PSPs, and pursue repatriation.

A potential explanation for the higher recovery rates among larger firms is that they may have more established fraud detection, case management and inter-PSP coordination processes, enabling them to identify fraud and seek repatriation more quickly. This may also apply to firms that were previously members of the CRM Code, to the extent that they had already developed processes to manage reimbursement and recovery.

Figure 10 Repatriation of funds from receiving PSPs



Source: *Frontier analysis of Industry evaluation data and Standard A data.*

Note: *Data from 19 PSPs. We show repatriated/recovered value from the Industry evaluation data as a percentage of reimbursable claims from Standard A.*

This data is only available for the period after the reimbursement requirement was introduced. We are therefore not able to comment on whether the policy has led to an increase in repatriation and recovery of funds lost to APP scams.

5.1.2 Coordination between PSPs has improved in some areas, but constraints remain

In addition to influencing firms' individual actions to tackle APP fraud, the introduction of the reimbursement requirement was expected to improve intra-PSP coordination and lead to more effective real-time data sharing.

The evidence on changes in such coordination over the past two years is mixed. Some stakeholders reported greater collaboration between PSPs on fraud prevention. This appeared to take several forms:

- **More structured and timely case-by-case coordination.** Respondents suggested that the reimbursement requirement had contributed to more structured coordination between sending and receiving PSPs, building on pre-existing arrangements for flagging suspected fraud. One industry group spokesperson reflected that process and timing changes associated with the reimbursement requirement, including the two-hour notification window, had supported earlier engagement and helped *"a little bit"* to prompt faster action to identify and disrupt potential mule activity.
- **Wider engagement from smaller PSPs.** Some respondents also reflected that smaller PSPs have become more engaged in wider fraud prevention efforts, with one noting that "*PSPs that weren't involved in the fraud space… are definitely more vocal, they're engaging more."*
- **Best-practice sharing and informal support.** Stakeholders also described examples of best-practice sharing and informal support that had been driven by the reimbursement requirement. For example, a larger PSP told us that it had offered guidance to smaller receiving PSPs to help interpret policy requirements. Some respondents also pointed to cross-industry implementation meetings as a forum for discussing practical issues and sharing emerging approaches.

Collaboration is however not always consistent. Some stakeholders suggested that larger PSPs may be less willing to engage on investigating lower-value cases that smaller receiving PSPs would prefer to investigate further before reimbursing**.**

Stakeholders also consistently highlighted continuing challenges in real-time data sharing across PSPs, which limited the effectiveness of coordination to tackle APP fraud. One consumer group noted that cross-PSP data sharing *"is not operating as anyone would want it to".* A smaller PSP illustrated the practical challenges created by limited cross-PSP data sharing. It explained that, while it can block suspected fraudsters within its own systems, gaps in information sharing mean linked accounts or mules may continue to emerge at other institutions:

> *"We block them in our systems … but [they can] open another account and come from another account and another account...It's endless."*

PSPs highlighted several constraints as to why cross PSP data sharing remained limited.

- **Network effects:** The value of data sharing only materialises once participation becomes widespread.
- **Cost asymmetries:** One smaller PSP noted they may face higher implementation costs relative to expected benefits. While improved data sharing was widely seen as beneficial, some respondents questioned the marginal benefit for smaller firms.
- **Coordination challenges:** Efforts to mandate data sharing have stalled, leaving no clear coordination mechanism.

5.2 To what extent are PSPs' actions attributable to the APP scam policies as opposed to driven by other factors?

In the previous section we showed how most PSPs have taken significant action to increase their detection and prevention of inbound and outbound APP fraud since April 2023. The key question the evaluation must then address is whether any of this action can be attributed to the PSR's APP scam policies or whether it would have happened regardless. We examined this in two ways:

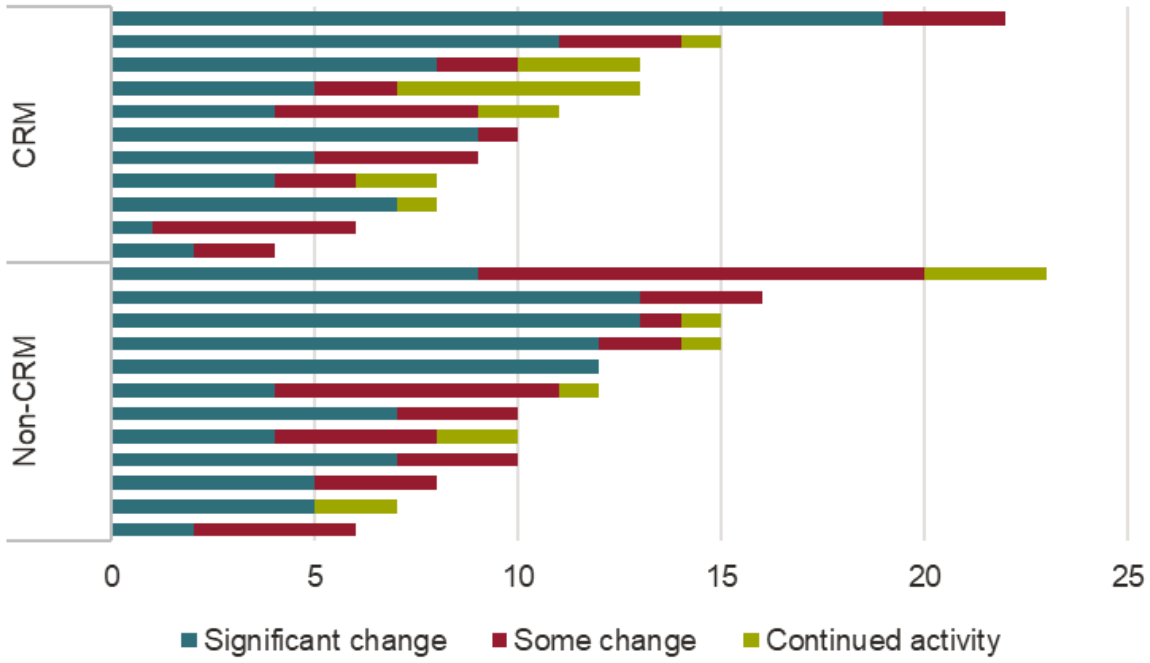
- Exploring differences in actions taken by CRM and non-CRM firms, since the change in incentives created by the reimbursement requirement differs between these groups.
- Discussing motivations for activities directly with PSPs through the in-depth stakeholder interviews.

Non-CRM firms were more likely to report taking significant new action

The scale and nature of action taken to tackle APP fraud since 2023 has varied across firms. Within that variation there are some systematic differences according to firms' pre-policy reimbursement arrangements. Firms that were already reimbursing victims before the policy more often described refinements to existing activity. By contrast, non-CRM firms more often described significant new investment, the development of new capabilities or more substantial changes to internal processes.

We have quantified the number of actions taken by each PSP to tackle APP fraud as part of our classification exercise of PSPs' qualitative responses to the industry evaluation data request and voluntary evaluation PSP survey. This should be viewed as indicative, as it is our subjective classification of qualitative information provided by PSPs. The results for each PSP that provided responses are shown in Figure 11. Both CRM and non-CRM firms reported a significant number of actions, but non-CRM firms typically report more significant increases in activity than CRM firms (an average of approximately 8 per PSP across the 12 non-CRM firms compared to approximately 7 per PSP among the 11 CRM firms).

Figure 11 Number of actions taken to tackle APP fraud, by PSP

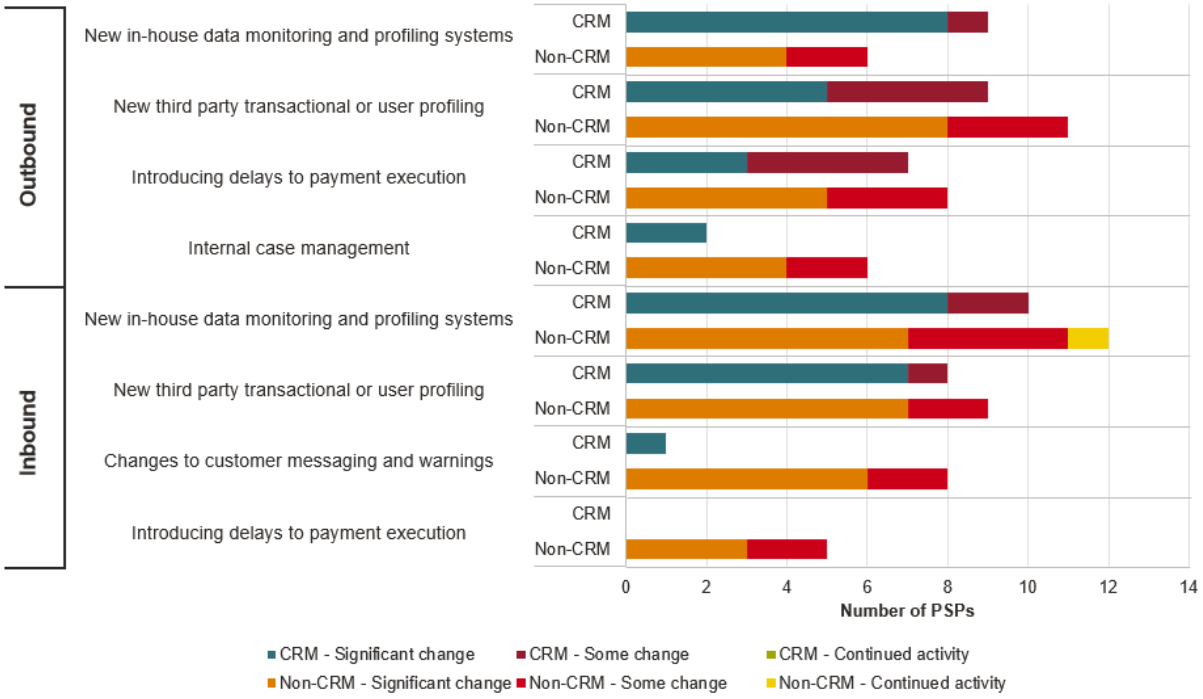


Source: *Frontier analysis of Industry evaluation data and the voluntary evaluation PSP survey*

Note: *PSP free-text submissions on the types of activity undertaken since 2023 have been grouped into types of activities and the scale of activity by Frontier*

A comparison of the type of activities reported by PSPs, also reveals some differences between CRM and non-CRM firms (shown in Figure 12). Non-CRM firms are much more likely to have reported introducing or changing delays to payment execution than CRM firms (reported by 6 out of 12 non-CRM firms compared to 2 CRM firms), and more likely to report having changed internal case management (5 out of 12 non-CRM firms compared to no CRM firms).

Figure 12 Types of actions to tackle APP fraud, by CRM and non-CRM firms



Source: *Frontier analysis of Industry evaluation data and the voluntary evaluation PSP survey*

Note: *PSP free-text submissions on the types of activity undertaken since 2023 have been grouped into types of activities and the scale of activity by Frontier*

While this quantification should be viewed as indicative, similar differences in emphasis came through the qualitative engagement with PSPs.

Firms already reimbursing victims before the policy more often described incremental improvements to relatively mature systems, rather than wholly new capabilities. This reflected their stronger starting position, as these firms already had established outbound monitoring and intervention processes in place before the policy. Many reported refinements to existing processes and targeted human intervention. One CRM firm described a complex, multi-disciplinary approach:

> *"we currently have 33 AI driven models in the fraud arena that do all sorts of different profiling to help to understand what's going on", which are "ingest[ed] together to actually create a… combined view", with "those systems sit[ting] very much in the flow of transactions… picking out the right ones for the operations teams to review with the customers".*

Some also reported mature inbound controls linked to AML and KYC requirements. One larger PSP noted that it had already had inbound detection "in place for many years". Nevertheless, inbound monitoring became a greater focus for many firms, including some CRM firms. One large CRM PSP reported that it had "*introduced a new detection system for our inbound transaction monitoring*".

Larger non-CRM firms also reported increasing the sophistication of existing processes. This included more frequent improvements to outbound fraud monitoring systems, such as updating models more regularly than in the past. One large non-CRM firm noted that these updates had previously occurred only *"twice a year".*

These firms also reported developments in inbound detection and prevention, including new models for onboarding, mule detection, and inbound transaction monitoring. One large non-CRM firm noted that, while it had had inbound transaction monitoring *"since 2021"*, there had been *"a lot of work in the last two years".*

Smaller and specialist non-CRMs also reported development of completely new capabilities or significantly updating internal processes. Examples included:

- investment in real-time fraud monitoring, with one smaller PSP describing "*significant programmes channelled towards fraud monitoring measures in real time*."
- new payment control functionality, including one smaller PSP moving to "*a hold and release functionality for outputs of our fraud controls*."
- greater focus on inbound monitoring, with one smaller PSP describing this as "*probably quite big for us*."
- reviews of internal controls and customer due diligence processes, with one smaller PSP reporting that it had "*really reviewed all of our KYC policies, procedures, systems*."

Overall, the evidence suggests that both CRM and non-CRM firms acted since April 2023, but the nature of that action differed. Non-CRM firms more often reported significant new investment or capability-building, while CRM firms more often described refinements, acceleration or extension of more mature pre-existing systems.

5.2.2 The reimbursement requirement incentivised a step-change in fraud tackling activity for non-CRM firms

There are plausible explanations other than the reimbursement requirement for why non-CRM firms reported more significant changes. Some non-CRM firms may have had less mature fraud-control capabilities before the policy, meaning observed changes partly reflect catch-up investment rather than the reimbursement requirement alone. Wider regulatory scrutiny and financial-crime expectations may also have contributed to some actions, particularly around onboarding and mule controls.

Interview evidence, however, suggests that the reimbursement requirement contributed materially to the step-change in activity among non-CRM firms. Non-CRM firms were more likely to describe explicit commercial decisions based on projected reimbursement exposure, revised risk appetite and the potential effect of APP fraud losses on profitability or growth. For example, non-CRM signatory said:

> *"The entire industry is probably more responsive… because we have to pay people out".*

"The key element that it comes back to is the financial loss that could sit there."

This is further illustrated by PSP account 1, which shows how mandatory reimbursement created the commercial case for new fraud controls at one non-CRM firm.

PSP account 1: Mandatory reimbursement created a commercial case for new fraud controls at a non-CRM firm

One non-CRM firm told us that the reimbursement requirement created a material new financial exposure. The firm said it had not previously been part of the CRM and that, before the policy, fraud losses were mainly linked to complaints or cases where the firm had failed in a significant way. Mandatory reimbursement therefore represented a significant change in its expected liability and said its expected losses could have risen from a relatively small amount to *"15, 20 million"* a year.

The firm explained that this led to a senior-sponsored review of its APP fraud controls:

"We had a strategic project… led by the CEO. That project looked at the full process and all components associated to APP fraud, looking at current controls, how we would then change those in relation to changes that would happen with mandatory reimbursement and what we would need to then implement to reduce our financial risk exposure."
"And that, to be brutally honest, was the main driver behind the investment."

The programme led to changes across the fraud journey, including new machine-learning models and rules, hold-and-release functionality for payments flagged by fraud controls, enhanced inbound monitoring, clearer Confirmation of Payee messaging, more proactive warning screens and wider customer education. The firm said the hold-and-release functionality allowed it to investigate payments before release, reducing the risk of funds being lost where fraud was later confirmed.

The firm also reported that actual losses were around 50% lower than forecast, despite significant growth in payment volumes.

5.2.3 For CRM firms the reimbursement requirement reinforced existing incentives and strengthened the business case for inbound controls

For PSPs reimbursing victims before the reimbursement requirement the policy reinforced and accelerated existing incentives rather than creating an entirely new rationale for investment. Many of these PSPs emphasised that the financial incentives to prevent fraud already existed prior to the PSR's intervention. They described their fraud prevention activity as part of a broader ongoing strategy, rather than a direct reaction to the October 2024 policy change.

This does not mean that the policy had no effect on CRM firms' behaviour. CRM firms consistently reported that the reimbursement requirement strengthened the internal business case and helped accelerate delivery. One CRM firm said the policy had "*helped us support, accelerate some enhancements"* and had influenced *"priorities and spend",* although it had not "*fundamentally led us down a different path".*

Some CRM firms also indicated that the reimbursement requirement had increased the level of vigilance and reinforced the need to minimise reimbursement exposure, even where activity formed part of an ongoing strategy. One CRM firm said it *was "doing as much as we can so that we don't end up with the reimbursements"* and noted that *"if other firms aren't doing as much, we then need to be more vigilant"*, while also emphasising that this was *"not something we've done in reaction to this policy",* but part of an *"ongoing strategy".* Further detail on the actions taken by this firm is set out in more detail in PSP account 3 in Section 6.2, which describes how enhanced fraud detection systems and expanded human intervention capacity have supported fraud prevention.

The reimbursement requirement appears to have strengthened the business case most clearly for inbound monitoring, mule detection and other inbound controls, with one CRM signatory noting that "*the business case for monitoring inbound undoubtedly changed."* This is also illustrated by Case Study 2, which shows how the 50:50 liability split strengthened the internal case for investment in inbound controls at one CRM firm.

PSP account 2: The reimbursement requirement strengthened the business case for inbound controls at a CRM firm

One large CRM firm told us that the reimbursement requirement did not fundamentally change its outbound fraud prevention strategy. The firm said it was already a CRM Code signatory and that "*the financial incentive… was already there prior to the PSR intervention".* It also said its outbound prevention and detection activity had always been motivated by protecting customers and keeping pace with scammers.

The firm said several outbound changes were already planned before the policy, including a new fraud detection model and system, more targeted digital warnings and a specialist payment review team for higher-risk cases. As the firm put it, *"it isn't a case of the policy's come in, and we've changed our runway of change".*

However, the firm drew a clearer link between the reimbursement requirement and its focus on inbound controls and mule detection. It reported introducing a new detection system for inbound transaction monitoring and improving the models used to monitor inbound traffic and generate alerts. The firm explained that the 50:50 liability split strengthened the internal case for investment:

"Prior to the regulations… there wasn't a 50:50 split. So, I think it would be remiss of any PSP to have ignored that because it's going to impact your P&L. Yes, we were all doing our best to restrict and mitigate mule activity, but obviously with [the] financial driver there as well, it

gives you greater ammunition in terms of a change request… [and] more ammunition from a business case perspective."

The firm also reflected that it was difficult to know the counterfactual, because it may have turned greater attention to mule activity anyway. However, it said that without the reimbursement requirement, they *"wouldn't have been introducing major change on the mule side at the same time as [another significant programme of work] from a bandwidth perspective".*

5.2.4 PSP actions to tackle APP fraud were driven by wider factors in addition to the reimbursement requirement

The evidence suggests that the reimbursement requirement was an important driver of PSP action, but not the only one. Firms report several other important motivations:

- **Protecting consumers:** Many PSPs, across different firm types, emphasised that protecting consumers was a key driver. One PSP said: *"Our primary driver to increase prevention and detection is, and always has been, to protect our customers and their money."*
- **Maintaining customer trust and loyalty:** Some PSPs argued that investment in fraud prevention by smaller and specialist PSPs was driven by the need to maintain customer trust and loyalty. One industry organisation argued that smaller and specialist PSPs *"didn't need reimbursement as an incentive… their growth depends on customer trust and customer loyalty."*
- **Responding to the increasing sophistication of fraud**: Several firms also noted the increasing sophistication of scammers as a driver of recent actions. One PSP said its "*recent actions have been driven by the increase in the scale and sophistication of fraud",* as well as its *"determination to protect customers, and our responsibility to manage financial outcome."*

Several PSPs, across different firm types, described an indirect incentive to reduce fraud to reduce the operational costs associated with claims reimbursement. As one PSP put it:

> *"The biggest driver for us is the impact on customers and being honest, operational costs as well. While you're having to deal with scams after they happen, that's actually quite expensive."*

5.2.5 Fraud performance data informed benchmarking and senior discussions, but was not a primary driver of PSP actions

PSPs did not generally identify the publication of fraud performance data as a primary driver of specific fraud prevention actions.

Most stakeholders in our interviews needed prompting to consider the impact of the publication of performance data. When prompted, it was primarily seen as an internal benchmarking tool, used to assess performance relative to peers and inform senior discussions, prioritisation and business case development. As one wider stakeholder put it:

> *"*Nobody wants to be on that list, but… the primary driver was always going to be the regulation."

That said, for a few smaller PSPs the publication of performance data may have contributed to incentives to combat fraud, through reputational and regulatory channels:

- **Regulatory and supervisory incentives:** some PSPs linked published performance data to regulatory scrutiny. They suggested that appearing to perform poorly in the published measures could lead to greater supervisory attention or a more challenging inspection environment. Respondents noted that supervisory engagement, including communications such as Dear CEO letters, remained an important driver of action.
- **Reputational incentives:** several smaller PSPs noted that poor performance in published data could affect external perceptions of the firm. One such PSP said reputation was *"one of the biggest things that we wanted to make sure that we managed really well"*, while another noted that "*negative media reporting… undermines trust in our business".*

PSPs and consumer groups both believed that published performance data is unlikely to significantly influence consumer choice of service provider. One non-CRM PSP said that performance data *"didn't seem to have an impact on our customers' positions and what they thought of us as a bank".* This is supported by our analysis of Current Account Switching Service data, which found no clear evidence that PSPs identified as low performers in the performance data experienced higher customer loss shares than other PSPs.[58] Nor did we observe a significant increase in customer loss share, as measured with CASS switching data, for these PSPs following publication of the performance data.

However, published rankings may still have exerted indirect pressure through media and consumer advocacy channels. Which? publishes annual commentary on APP fraud performance rankings and told us that these articles have significantly outperformed benchmarks for similar content.[59] This suggests that performance data may have helped shape public scrutiny of PSPs, even if there is limited evidence that it directly affected consumer switching behaviour. Organisations such as Which?, with super-complaint powers and wide consumer reach, may also amplify reputational pressure on poor performers and strengthen wider incentives for firms to improve APP fraud controls.

[58] We define "low performers" as PSPs that ranked in the bottom three by value for either Metric A or Metric B in the 2023 and 2024 APP Fraud Performance Report. We define "customer loss share" as the number of consumers gained divided by the sum of consumers gained and lost for each PSP and quarter, using data from the Current Account Switch Service.

[59] For example see: Which? (2023). Fraud victim reimbursement rankings revealed - how did your bank fare?; Which? (2026). Nationwide refunded 85% of fraud losses - how does your bank compare?

Overall, the evidence suggests that fraud performance data had limited effect on most PSPs' behaviour. It supported benchmarking, reputational awareness and senior-level discussions, but stakeholders did not generally identify it as a primary driver of fraud prevention actions.

6 Theme 2 Findings: Impacts on fraud

In this theme, we first assess how APP fraud has changed since the reimbursement requirement was introduced in October 2024. We consider whether the policy has strengthened PSP incentives to prevent fraud. We also examine how effective PSPs interventions have been in preventing fraud. We then consider evidence on whether the observed trends could reflect changes in customer awareness, willingness to claim, customer caution, or first-party fraud. Finally, we consider whether changes in APP fraud in scope for the reimbursement requirement have been accompanied by shifts in other fraud types, such as out-of-scope APP scams and unauthorised fraud.

6.1 How has the level of APP fraud changed?

This section assesses how APP fraud outcomes have changed since the reimbursement requirement was introduced. We focus first on the overall level of APP fraud, using the value of APP scams, the number of scam transactions and the average value per transaction. We then consider how these changes differ by scam type, to assess whether overall trends reflect broad-based changes in APP fraud or shifts in the mix of scams.

The analysis shows that APP fraud values have fallen since implementation, and that this reduction is not explained by changes in overall FPS activity. APP scam transaction volumes also fell around implementation, although they increased again in spring and summer 2025. The evidence suggests that this recent increase was concentrated in lower-value scam types, particularly purchase scams and, to a lesser extent, advance fee scams. [60]

Focusing on the change in APP fraud since 2023 implicitly assumes that APP fraud would have remained constant in the absence of the reimbursement requirement. In practice there are reasons to think APP fraud may have increased over time, including the growth in online payments, and the increasing availability of Artificial Intelligence enabled tools that allow fraudsters to target victims in increasingly sophisticated ways. The change in APP fraud relative to a world in which the reimbursement requirement was not introduced may therefore be greater than estimated in this review, although the scale of this effect cannot be quantified.

[60] As defined in the PSR (2024) Fraud Enabler Report, a purchase scam is where "The victim pays for a good or service that they do not receive, and the seller had no intention of providing. The scammer may create a fake website or advertise a false product on social media." An advance fee scam is where "The fraudster convinces the victim to pay a fee which they claim will result in the release of a much larger payment or a deposit for goods or service that they never receive, and the fraudster never intended to provide."

6.1.1 APP fraud total and average values have reduced

In this section, we assess changes in APP fraud using three measures: the total value of APP fraud, the number of APP scam transactions, and the average value per scam. Together, these measures show that APP fraud total and average scam values have reduced. Scam transaction volumes also fell around implementation, although they increased again in spring and summer 2025. We interpret these volume trends alongside changes in fraud value and average transaction value, because they may reflect a shift towards lower-value scam types or more transactions per scam.

We first set out the methodology used to compare fraud outcomes over time. We then consider the value of APP scams, the volume of scam transactions and average scam values in turn.

Methodology

FPS is the primary channel by which APP fraud loss takes place. CHAPS payments are also in scope of the reimbursement requirement but have historically been a small share of fraud cases. Therefore, our analysis primarily focuses on FPS data.

Use of scam transaction data

There are three ways of dating FPS APP scam data that could be used to assess changes in APP fraud outcomes: by the date of the consumer claim, by the date the PSP closes the case, or by the date of the scam transaction.

- **Consumer claims data** attributes fraud to the date on which the victim submitted the claim or the date the claim is closed. Public reporting by UK Finance and the PSR is generally reported in this way. However, there is often a lag between an APP scam taking place and the victim claiming for it, because victims may not yet know that they have been defrauded.

- **Scam transaction data** attributes fraud to the period in which the scam took place, which allows us to assess changes around the implementation of the reimbursement requirement. This transaction-based analysis still needs to account for reporting lags. The length of this lag varies by scam type. For example, victims of purchase scams can identify the scam quickly when the goods they paid for do not arrive. By contrast, victims of investment fraud may continue to believe the investment is genuine and may only realise months or years later that they have been defrauded.

These differences have two implications for the analysis.

- First, consumer claims data is less well suited to assessing changes around the implementation date. Claims submitted after the reimbursement requirement came into force may relate to scams that took place before implementation. This means that this data can overstate the amount of APP fraud taking place after implementation and understate the extent of any reduction in APP fraud occurring around the policy change.

- Second, transaction-date data is better suited to assessing when fraud took place, but recent transaction periods may be incomplete because some scams that took place recently will not yet have been reported. This means recent periods of scam transaction data may look artificially low and may not be directly comparable with earlier periods unless a consistent reporting window is applied.

To allow a like-for-like comparison over time, in this section, we use APP scam transaction data and apply a consistent reporting window after the transaction date. For APP fraud value, we include scams reported within six months of the scam occurring. This captures 80% of the reported APP fraud value for the period April 2023 to December 2023. For APP fraud volumes, we include scams reported within three months of the scam occurring as only a small proportion of high value scams are not reported within this window. This captures 84% of reported scam volumes over the period April 2023 to December 2023.

This approach does not capture every APP scam and is more likely to exclude APP scams with longer reporting lags. However, it provides a consistent basis for assessing the 12-month post-implementation period covered by the data collected from PSPs in December 2025.

Transition period

When analysing the changes in APP fraud during the evaluation period, we define 3 time periods.

- Pre-policy period: April 2023 to December 2023.
- Transition period: January 2024 to September 2024.
- Post-policy period: October 2024 to September 2025.

The pre-policy period begins in April 2023, 18 months before the reimbursement requirement was implemented. This is the earliest month that industry evaluation data is available for.

We end the pre-policy period in December 2023, when the PSR published its final policy statement, because subsequent changes in fraud may reflect PSPs preparing for the reimbursement requirement before it came into force in October 2024. [61]

The post policy period starts October 2024, the month that the reimbursement requirement was implemented. It ends in September 2025 which is the last month that the industry evaluation data was collected for (with the evaluation itself starting in September 2025).

Linear regression analysis

We estimate the difference in the total value of APP scams between the pre-policy and post-policy periods by estimating a linear regression model of the total value of monthly outbound APP fraud from the industry evaluation dataset. The advantages of a regression approach,

[61] The PSR published the PS23/4 APP scams reimbursement policy statement setting out the final details of the policy on 19 December 2023.

rather than just comparing averages for different time periods, are that we can test the statistical significance of any differences observed, and we can control for potential seasonal effects on fraud.

The main model specification can be expressed as follows:

$$Y_t = \alpha + \beta_1 I_{t\in[Jan\ 24, Sep\ 24]} + \beta_2 I_{t\geq Oct\ 24} + \beta_3 I_{t=Jun} + \beta_4 I_{t=Jul} + \beta_5 I_{t=Aug} + \beta_6 I_{t=Sep} + \varepsilon_t$$

Where: Y_t is the value of APP scams in month t;

$I_{t\in[Jan\ 24, Sep\ 24]}$ is an indicator for the transition period and takes the value 1 for the months January – September 2024;

$I_{t\geq Oct\ 24}$ is an indicator for the post-policy period and takes the value 1 for month October 2024 onwards; and

$I_{t=Jun}$, $I_{t=Jul}$, $I_{t=Aug}$, $I_{t=Sep}$ are a set of indicators that takes the value of 1 for each June, July, August and September respectively to control for seasonal effects.

By construction the estimated parameter α is the market-wide average monthly level of APP fraud during the pre-policy period (up to and including December 2023) after controlling for seasonal effects. The estimated coefficients β_1 and β_2 reflect deviations from this level in the transition and post-policy periods respectively. The estimated coefficient β_2 on the post-policy period indicator therefore measures the average change in the monthly value of APP fraud at market level after policy implementation relative to the pre-policy period. Multiplying this figure by 12 yields the estimated annual reduction in total APP fraud.

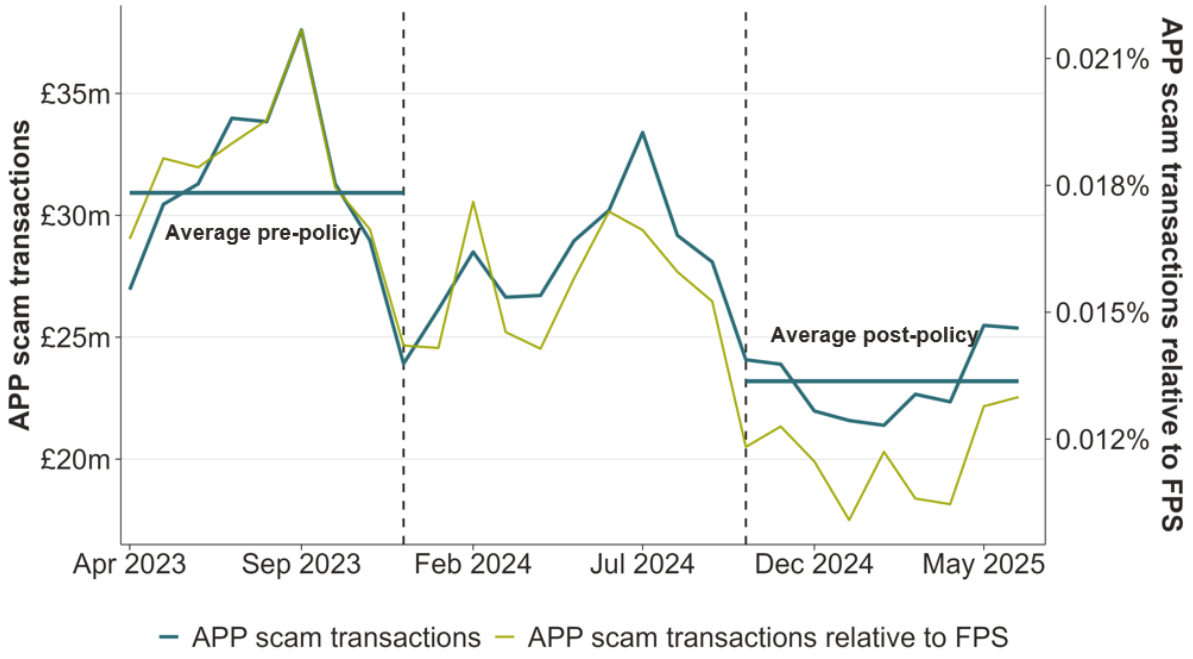
The specification includes indicators for June-September months to control for seasonality in the value of monthly APP fraud levels. The inclusion of this seasonal control was motivated by the observation that the value of monthly APP fraud transactions peaks every summer in the evaluation period. We test the sensitivity of the results to these seasonality controls, and this is discussed below.

Value of APP scams

As shown by the blue line in Figure 13, the value of comparable FPS APP scam transactions was significantly lower in the post-implementation period than in the equivalent pre-policy level in 2023.[62] To control for seasonal spikes observed in APP scams in the summer of each year, we estimate the difference using a linear regression model. Using this approach, we find that fraud has fallen by an average of £6.1m per month or 21% since the reimbursement requirement. This equates to £73 million per year.

[62] The data captures all APP scams as defined in Section 5.3.1 of this report. We note that a few PSPs excluded scams that are not reimbursable under the reimbursement requirement, such as crypto and me to me payments from this dataset.

Figure 13 Value of comparable FPS APP scams by scam transaction date



Source: *Frontier analysis of industry evaluation data*

Note: *Data from 19 PSPs which together account for 95% of FPS transaction volumes and values scaled to market-level using market shares. We only include scams reported within six months of the transaction taking place, which allows a like-for-like comparison over time.*

This reduction is not explained by changes in overall FPS activity. The green line in Figure 13 shows that APP scam losses have also fallen as a proportion of total value sent through FPS. In the pre-policy period, on average £181 was lost to APP scams for every £1 million sent through FPS. In the post-implementation period, this fell to £116 for every £1 million sent through FPS.[63]

As noted above, the analysis does not capture the full impact on scams that had not yet been reported when the data was collected. This is particularly relevant for APP scam types with long reporting lags, such as investment scams. Evidence from the claims management company, Refundee suggests that many investment APP scam claims take 18 months or longer to be reported.[64] As a result, some scams that took place during the analysis period may not have been included in the data collected from PSPs in December 2025. If the

[63] A reduction from £181 to £116 is equivalent to a 36% reduction in the average rate of APP fraud relative to the value of FPS transactions over the same period. We tested this result using a linear regression and controlling for seasonal effects in line with the approach to the changes in the level of APP fraud. We find that the reduction in the APP fraud rate when controlling for seasonal effects (with dummies for June, July, August, September) is 34%.

[64] Refundee (2026). Based on 594 investment fraud cases represented by Refundee. Refundee data submitted to Frontier as part of this evaluation. A public version of this data is available on Refundee Blog: 13-month Reporting Limitation in the New MRR Regulation.

reduction observed for reported APP scam types were also to apply to scams not yet reported, the total market-wide reduction in APP scam losses would be around £91 million per year.[65]

UK Finance Fraud Reporting data shows that APP fraud losses from CHAPS in 2025 were £18m, in line with its 2020-2024 average and significantly lower than APP fraud over Faster Payments.[66] CHAPS' primary use for high value transactions means that the average value of each fraud is very high, about £50,000.[67] The number of APP fraud cases over CHAPS has been falling since 2022 and is now below 200 cases per year.[68, 69] There were 49 CHAPS cases in scope of the reimbursement requirement between its introduction in October 2024 and September 2025.[70]

Sensitivity analysis for estimated value of APP scams

We tested the sensitivity of our findings to different lengths of the transition period and approaches to seasonal controls.

The results vary somewhat if we assume that the transition period was different to the January to September 2024 period used as the central estimate, but we conclude that the central scenario is a plausible central case.

- A transition period that started 3 months earlier (September 2023 to September 2024) would suggest that the monthly reduction in fraud was £7.0m or 15% higher than our central estimate of £6.1m. A transition period that started 3 months later (April 2024 to September 2024) would suggest that the monthly reduction in fraud was £5.5m or 10% lower than our central estimate of £6.1m.

- The scale and direction of the overall findings is broadly similar between the different plausible transition periods. We also note that different PSPs are likely to have started their preparations for the reimbursement requirement at different points in time. We conclude that the central estimate with a January to September 2024 transition period represents a plausible central scenario for our analysis.

The results also vary somewhat if different seasonal controls are included in the regression analysis.

---

[65] The same source also confirms that these scams typically have higher average value than other scam types. PSPs are particularly incentivised to prevent high-value scams as their liability increases with the value of the scam. It is therefore reasonable to assume that the reduction in long-time lag, high-value scams has been similar to the reduction in other types of scams.

[66] UK Finance (2026). Annual Fraud Report 2026.

[67] *Ibidem.*

[68] *Ibidem.*

[69] Because the volume of APP scams carried out over CHAPS remains relatively low, we did not collect transaction data on this payment rail and are only able to report trends at claim level. This means that any changes from the period after the reimbursement requirement policy are likely not observed in the data yet.

[70] Standard A data.

- The main specification includes separate indicators for June, July, August and September. The inclusion of these controls was motivated by the observation that the value of monthly APP fraud transactions peaks every summer in the industry evaluation data. The joint inclusion of June to September controls resulted in a statistically significant coefficient for July (p=0.002), August (p=0.04) and September (p=0.007), while the coefficient for June was marginally significant (p=0.05). Including these seasonal controls reduces the estimated fall in the monthly value of APP fraud after policy implementation by £1.6m compared to the specification where no seasonal controls are used. The post-policy coefficient in the regression with these seasonal controls is highly statistically significant ($p < 0.0001$).

- We tested the specification by controlling for individual months in isolation. July was the only month that was statistically significant (p=0.03) and had an impact on the regression results. With the July control only the estimated reduction in APP fraud in the post-policy period is £7.2m per month relative to the pre-policy baseline, 18% greater than our central estimate of £6.1m. We use the specification with June to September controls due to the higher significance of the individual month coefficients and the more conservative estimate of the change in value of APP fraud.

- We also tested the regression with indicators for additional months beyond June to September. None of these specifications changed the value of the point estimate of the change in APP fraud between pre-policy and post-policy periods by more than 6%, and the change in APP fraud remained statistically significant in all.

We conclude that the central specification with controls for June to September is a plausible core estimate and is more conservative than making no allowance for possible seasonal effects in APP fraud values.

Reconciliation with UK Finance's Annual Fraud Report data

The UK Finance Annual Fraud Report 2026, published on 12 June 2026, shows an increase in reported APP scam claims in 2025.

- The value of all APP scam claims increased by 19%, from £484 million in 2024 to £576 million in 2025.

- The value of domestic consumer APP scam claims over Faster Payments, which is the UK Finance definition that most closely aligns with the definition used in this report, increased by 20%, from £384 million in 2024 to £461 million in 2025.

The difference between the UK Finance data and the findings from this evaluation reflects an important difference in measurement. UK Finance reports APP scam **claims**, while this evaluation analyses APP scam **transactions**. These are different measures and are therefore expected to produce different results.

The analysis in the section above assesses how the level of APP fraud that occurred between April 2023 and September 2025 changed over time. For this reason, and as explained in the methodology subsection of Section 6.1.1., the analysis is based on the date on which the scam transaction took place.

By contrast, UK Finance reports APP scams according to the date on which the scam claim was closed by the PSP facing the claim. This means that all APP scam claims closed in each month are recorded in that month, regardless of when the underlying scam took place. The UK Finance Fraud Reporting data should therefore be interpreted as measuring the historical level of APP scam claims closed in each month, rather than the level of APP scams that occurred in that month.

There can be a substantial delay between an APP scam taking place and the victim making a claim, because victims may not immediately realise that they have been defrauded. This is particularly relevant for investment scams and romance scams. Evidence suggests that the average time taken to report an investment scam may be as high as 18 months.[71] As a result, the level of investment scams reported in UK Finance's fraud data for 2025 is likely to largely reflect investment scams that took place before the reimbursement requirement was implemented in October 2024.

For this evaluation, we collected industry data on APP scams using both the date of the scam transaction and the date on which the consumer claim was made. When the industry evaluation data is aggregated on the same basis as the UK Finance data, the level and trend of APP fraud are broadly consistent across the two sources. Figure 14 below shows this by aggregating the value of APP fraud shown in Figure 13 by the month in which the customer claim was made, rather than by the month in which the scam occurred. We also show two measures of APP scam claim data from UK Finance's data.

We compare the industry evaluation data with UK Finance's fraud data using two measures: one to compare the reported level of APP fraud claims, and one to compare the trend over time. These comparisons confirm that the industry evaluation data is consistent with the fraud data reported by UK Finance.

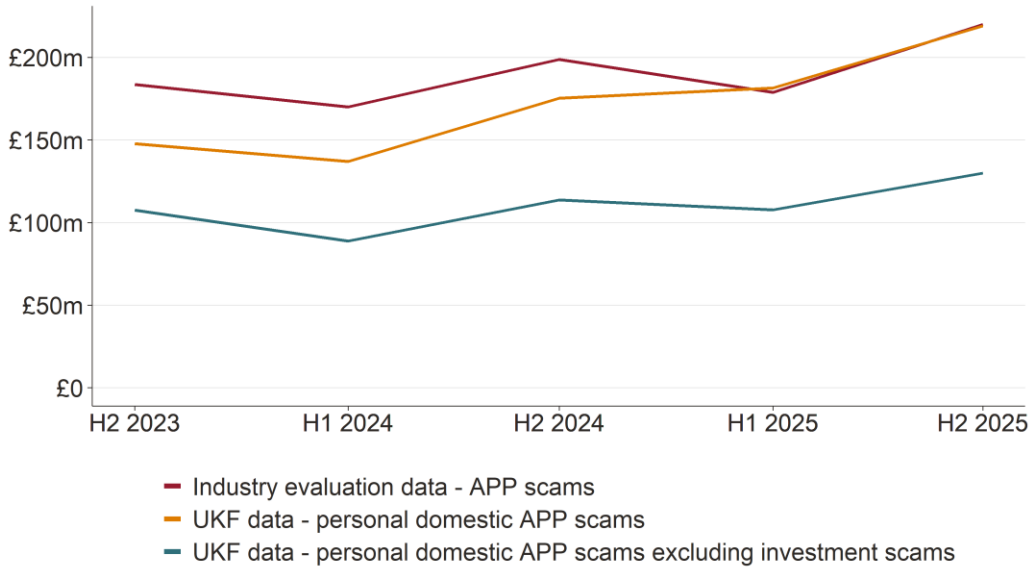
- **Level of APP fraud claims.** To compare the overall level of FPS APP fraud claims between industry evaluation data and UK Finance's data, we compare industry evaluation data on APP scams aggregated by the date of the claim to all domestic consumer FPS APP scam claims reported by UK Finance. Figure 14 confirms that the average value of APP scam claims per half-year over the period is broadly consistent between the two sources: £190m in industry evaluation data and £172m in UK Finance's data.

- **Trend in APP fraud claims.** To compare trends over time, we compare the industry evaluation data with UK Finance's data excluding investment scams. Investment scams

[71] Refundee (2026). Based on 594 investment fraud cases represented by Refundee. Refundee data submitted to Frontier as part of this evaluation. A public version of this data is available on Refundee Blog: 13-month Reporting Limitation in the New MRR Regulation.

are excluded because long reporting lags mean they are captured differently across the two datasets: the industry evaluation data may not yet capture some investment scams that occurred during the evaluation period, while UK Finance's claims data may include investment scams that occurred much earlier. Once investment scams are excluded, Figure 14 shows that the trend is consistent across the two sources: APP scam claims in the industry evaluation data were 20% higher in H2 2025 than in H2 2023, while APP scam claims in the UK Finance data were 21% higher over the same period.

Figure 14 Value of FPS APP scams by scam claim date



Source: *Frontier analysis of industry evaluation data, UK Finance's Half Year Fraud Report 2025 and UK Finance's Annual Fraud Report 2026*

Note: *Monthly industry evaluation data is aggregated to half-year values to allow for a comparison with UK Finance's data which is reported on a half-yearly basis. Industry evaluation data covers the period April 2023 – September 2025. Total value of claims for H2 2025 is derived by assuming that October – December 2025 claims levels are equal to the claims levels in July – September 2025.*

Volume of APP scams

As shown by the blue line in Figure 15, the volume of comparable FPS APP scam transactions fell in the lead-up to the reimbursement requirement and immediately after its introduction. The average number of monthly scam transactions was 39,600 in the pre-policy period. In the post-implementation period, the average was lower, at 34,700 transactions per month. Our data suggests that there is an average of 1.7 transactions per APP scam. This indicates an annual reduction in the number of APP scams of 34,800 if the number of transactions per APP scam has stayed constant.

The number of APP scam transactions increased again significantly since April 2025. By June 2025 it was 44,600 per month, higher than the 2023 peak. This increase may not necessarily correspond to an increase in the number of victims or the overall level of consumer harm. It appears to reflect three factors.

- First, the increase was partly driven by a shift towards higher-volume, lower-value APP scam types. As explained in the next section, in our analysis we observed increases in purchase scams and advance fee scams, including job scams. These APP scam types typically involve lower individual transaction values but can generate many transactions.

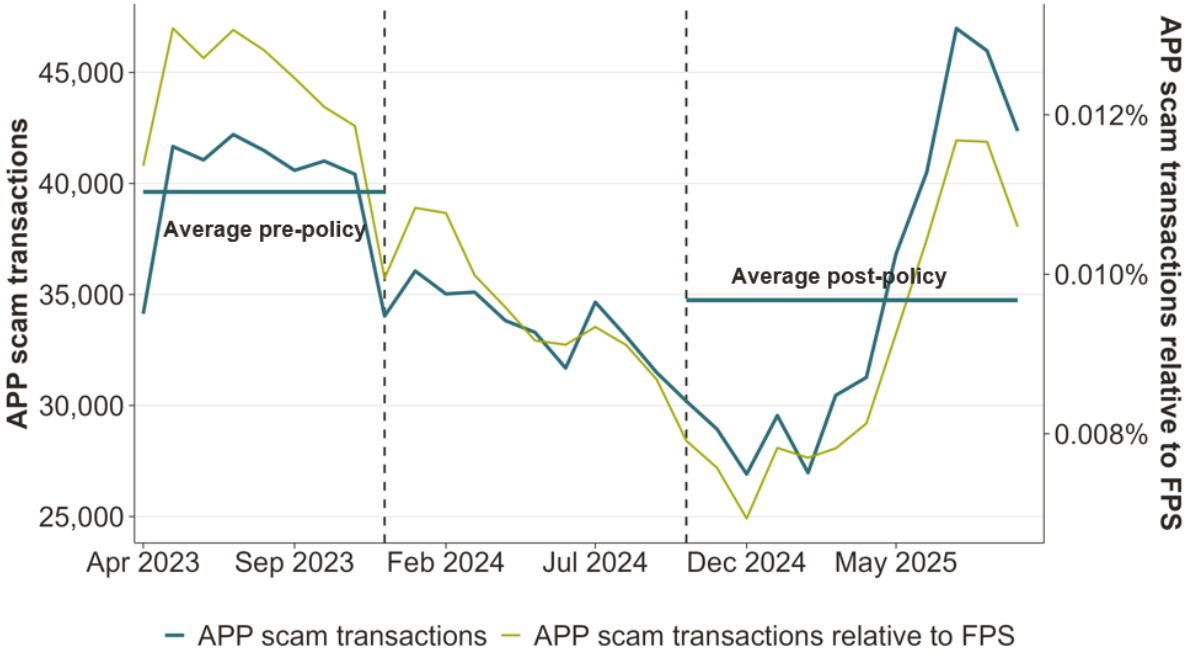
- Second, APP scam transaction volumes do not necessarily measure the number of individual scams. A single APP scam claim often involves multiple transactions and transaction volumes can increase even if the number of individual scams or victims does not increase by the same amount. This is consistent with reports from some PSPs that, after controls on high-value transactions were strengthened, fraudsters encouraged victims to make multiple smaller payments over multiple transactions to avoid triggering scam alarms. An increase in APP scam transaction volumes over this period may therefore be reflective of changes in APP scam methods, such as more transactions per scam, rather than an increase in the number of people falling victim to APP scams.[72]

- Third, the increase took place against a wider increase in Faster Payments activity. As shown by the green line in Figure 15, APP scam transactions have fallen relative to total FPS transaction volumes. In the pre-policy period, there were 122 APP scam transactions for every 1 million FPS transactions. In the post-implementation period, this fell to 90 APP scam transactions for every 1 million FPS transactions.

The first two factors are consistent with the decline in APP fraud value shown in the previous section and the decline in average transaction values shown in the next section.

[72] Analysis from our sample supports this view, showing that the average number of transactions per scam claim spiked at 2 transactions per claim during July 2025, an 18% increase from the long-run average of 1.7.

Figure 15 Volume of comparable FPS APP scam transactions by transaction date



Source: *Frontier analysis of industry evaluation data*

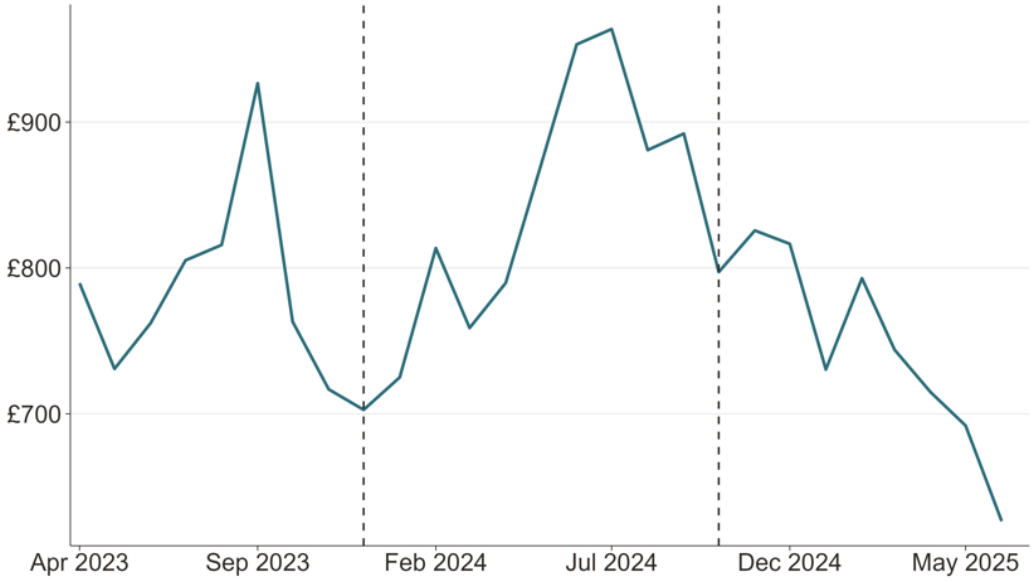
Note: *Data from 19 PSPs which together account for 95% of FPS transaction volumes and values scaled to market-level using market shares. We only include scams reported within three months of the transaction taking place, which allows a like-for-like comparison over time.*

Average value of APP scams

Figure 16 shows that the average transaction value of FPS APP scams has fallen. This combines the value and volume analysis of the preceding sections. The average value was £779 during pre-policy period but has averaged £749 since the reimbursement requirement.

This is consistent with the increase in APP scam transaction volumes being driven by lower-value scam types, particularly purchase scams and some advance fee scams, as well as some increase in the number of transactions per scam.

Figure 16 Average value of comparable FPS APP scams by scam transaction date



Source: *Frontier analysis of industry evaluation data*

Note: *Data from 19 PSPs which together account for 95% of FPS transaction volumes and values scaled to market-level using market shares Average transaction value is calculated by dividing the total value of FPS APP scam transactions in a given month by the number of APP scam transactions recorded in that month.*

6.1.2 APP fraud values have generally fallen, while recent increases in scam transactions were concentrated in lower-value scam types

Figure 17 shows how the value of APP fraud has changed by scam type since April 2023. In April 2023, investment fraud accounted for the largest share of consumer losses, at 29% of APP fraud value. Impersonation fraud and purchase fraud were also significant, accounting for 28% and 23% of APP fraud value respectively.

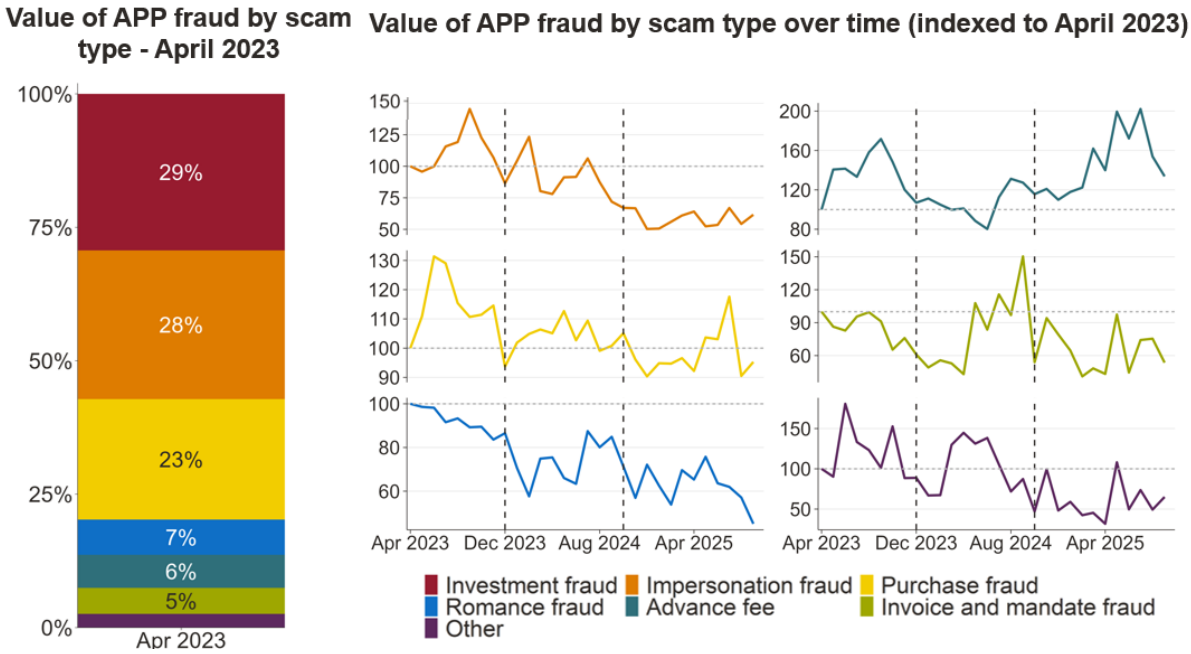
We do not report changes in investment fraud over time because investment fraud is subject to long reporting lags. Victims may only realise months or years later that they have been defrauded, meaning many investment scams that took place during the later part of the analysis period may not yet have been reported by the time the data was collected in December 2025.

For other scam types, the value of APP fraud has generally fallen since April 2023.[73] This is particularly clear for impersonation fraud, romance fraud, invoice and mandate fraud, and

[73] The analysis in this section is based on less granular data than preceding analysis which means it cannot be adjusted to create a consistent reporting window of 3 or 6 months. These results are therefore indicative of the general trend between frauds but are not directly comparable to the preceding analysis.

"other" fraud types. Advance fee fraud is the main exception, with values increasing over the period, although it accounted for a relatively small share of APP fraud value in April 2023. Purchase fraud has remained closer to its April 2023 level by value.

Figure 17 Value of APP fraud by type of scam by scam transaction date



Source: *Frontier analysis of industry evaluation data*

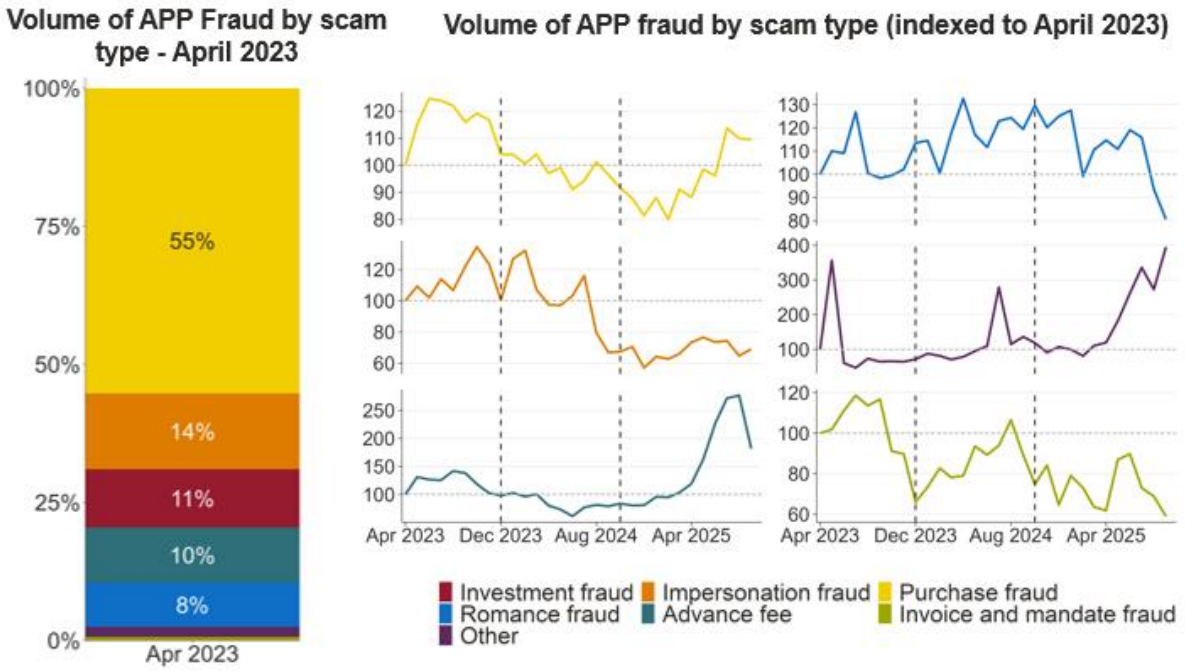
Note: *Data from 18 PSPs. Value of APP fraud by scam type over time is indexed to 100 in April 2023, the start of the evaluation period. Growth in investment scams is not reported as these scams take a long time to be reported and are therefore not fully reflected in our data.*

Figure 18 shows the corresponding trends in APP scam volumes.

Purchase scams accounted for 55% of APP fraud cases in April 2023 and remain the most common type of APP scam. Since implementation, purchase scam transactions have increased by over 10%. Advance fee scam transactions have increased more sharply, rising to around 2.5 times their pre-policy level, but from a smaller base.

As a result, the recent increase in scam transactions was driven mainly by purchase scams, with advance fee scams also contributing to a lesser extent. This is consistent with evidence from PSP, which indicated that recent increases were concentrated in lower-value purchase scams, with a smaller increase in job scams recorded under advance fee scam typologies. This pattern is consistent with the overall fall in APP fraud value and the decline in average transaction values discussed above.

Figure 18 Volume of APP fraud by type of scam by scam transaction date



Source: *Frontier analysis of industry evaluation data*

Note: *Data from 18 PSPs. Volume of APP fraud by scam type over time is indexed to 100 in April 2023, the start of the evaluation period. Growth in investment scams is not reported as these scams take a long time to be reported and are therefore not fully reflected in our data.*

6.1.3 The reduction in APP fraud is small relative to the overall scale of banking fraud

The reduction in APP scams in scope for the reimbursement requirement needs to be considered in the context of the wider financial fraud landscape.

The reimbursement requirement only covers domestic APP fraud payments made by consumers.[74] We estimate that the annual losses from these types of APP scams over Faster Payments were £350m per year in 2025, based on the scam transactions that took place in 2025.

This is a small proportion of the overall financial fraud landscape. UK Finance estimates that a total of £1.3bn was lost to fraud in 2025.[75] £703m was lost to unauthorised fraud in 2025 and APP scam claims for payments to international accounts and via payment systems outside of Faster Payments were £116m in 2025. Not all these losses are suffered by consumers: £76m

[74] We note that not all domestic APP fraud payments made by consumers over Faster Payments are reimbursable under the policy. Further detail on the scope of the policy is set out in Section 3.2.

[75] UK Finance (2026). Annual Fraud Report 2026.

of the APP scam losses were reported by non-personal (typically business) account users of payment systems.

6.2 What impact have the in-scope APP scam policies had on APP fraud?

In this section we assess whether the APP scam policies have contributed to changes in APP fraud. Specifically, we consider:

- whether the incentive changes from reimbursement requirement led to APP scam impacts by examining whether firms with greater pre-policy fraud rates achieved larger reductions in APP fraud than firms with lower pre-policy rates;
- evidence on the effectiveness of PSP interventions, as well as the practical constraints that continue to limit fraud prevention; and
- whether other changes affect how we interpret the observed trends, including changes in customer awareness or willingness to seek reimbursement, changes in the types of cases submitted as APP fraud claims, and potential unintended consequences such as moral hazard, first-party fraud.

6.2.1 The reimbursement requirement has incentivised the PSPs with the most APP fraud to reduce it the most

We examine whether firms with higher pre-policy APP fraud rates reduced fraud by more than other firms after the reimbursement requirement was introduced. This provides evidence on whether the policy changed PSP incentives in the way it was intended to.

When the reimbursement requirement was implemented, firms had very different levels of both inbound and outbound APP fraud as a share of their transaction activity.

For inbound fraud, the PSPs in our sample with the highest pre-policy fraud rates received 25-40 times the value of APP scams, relative to total transaction value, compared with those with the lowest rates. By volume, the PSP with the highest inbound APP fraud rate received 30-70 times the number of APP scams relative to total transaction volumes, compared with those with the lowest rates.

Amongst PSPs, CRM signatories generally had lower inbound APP fraud rates than non-CRM firms, even though receiving PSPs did not face reimbursement costs under the CRM Code.[76] This may reflect differences in firms' strategic priorities and broader approaches to fraud management, irrespective of direct reimbursement incentives. The fact that some non-CRM

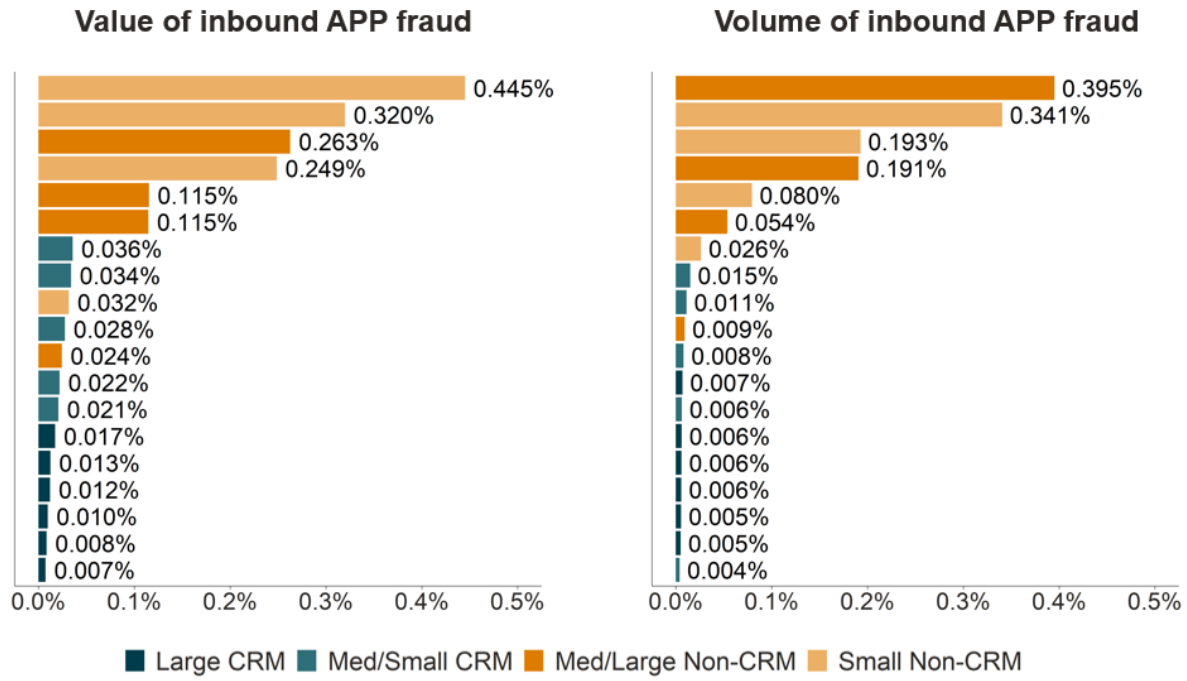
[76] Prior to the reimbursement requirement, TSB offered a fraud refund guarantee and their reimbursement rate in the PSR's 2024 APP Fraud Performance report was estimated at 80%, the second highest in the market. TSB is therefore treated as a CRM firm throughout this analysis despite not being a signatory to the code.

firms had inbound APP fraud rates in line with CRM signatories also suggests that approaches to fraud management varied within the non-CRM group.

Figure 19 illustrates the range in the value and volume of inbound APP fraud before the policy was implemented. These differences suggest that firms had materially different approaches to inbound APP fraud prevention before the policy. This is likely to reflect differences in customer onboarding and vetting, anti-money mule activity, and inbound transaction monitoring.

Annex B shows APP fraud rates during the evaluation period individually for each PSP in Figure 19.

Figure 19 Value and volume of inbound APP fraud relative to total transaction activity before the policy



Source: *Frontier analysis of industry evaluation data*

Note: *Inbound APP fraud is shown as a percentage of inbound FPS transactions before the policy, from April 2023 to December 2023. Inbound fraud rates are constructed using outbound APP fraud and FPS transaction data by beneficiary sort code provided by PSPs and matching sort codes to EISCD data to identify the name of the receiving PSP.*

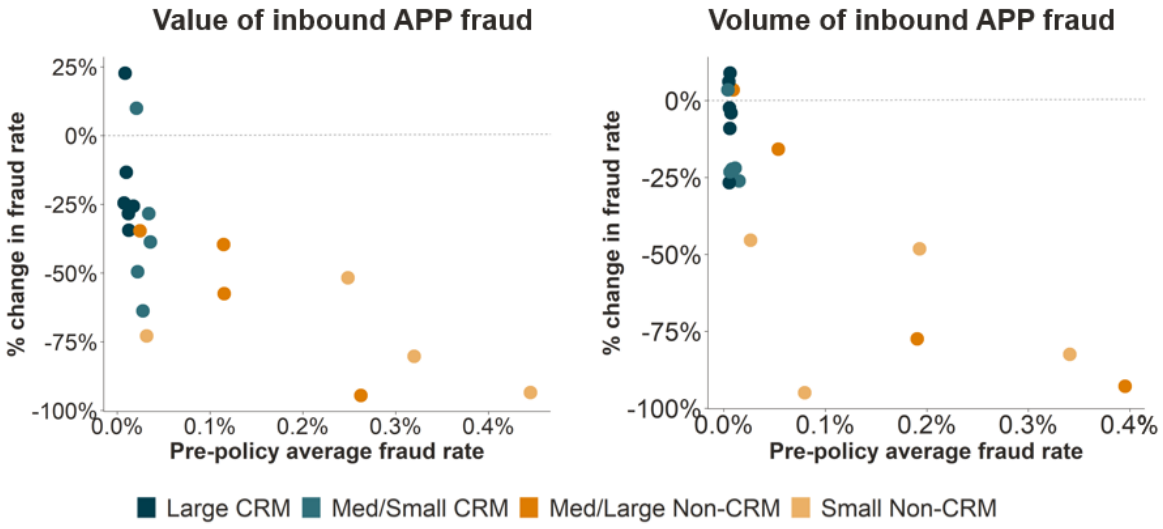
Figure 20 shows that:

- **There is a moderate negative relationship between pre-policy inbound APP fraud rates and subsequent changes in inbound APP fraud across firms**. This pattern is consistent with the policy having the greatest effect on firms with the strongest incentive, and greatest scope, to reduce inbound fraud.

- **The five firms with the highest pre-policy inbound APP fraud rates reduced APP fraud values of transactions by 52% to 94%.** The five firms with the lowest starting levels of inbound APP fraud rates changed by up to 23% and some did not reduce their inbound APP fraud rates at all.

There are many factors that affect APP fraud rates, both the actions of the PSP (such as the rollout of new technology and processes described in Section 5.1 above) and actions of criminals (such as APP fraud attacks exploiting weaknesses in a firm's processes), as well as the wider actions and strategic priorities of each firm. We would therefore not expect to see a perfect relationship between starting APP fraud rates and the reduction in APP fraud since the reimbursement requirement.

Figure 20 Change in the value and volume of inbound APP fraud relative to total transaction activity



Source: *Frontier analysis of industry evaluation data*

Note: *Inbound APP fraud is shown as a percentage of inbound FPS transactions before the policy, from April 2023 to December 2023 and after the policy, from October 2024 to September 2025. The change is calculated by comparing the two periods. Inbound fraud rates are constructed using outbound APP fraud and FPS transaction data by beneficiary sort code provided by PSPs and matching sort codes to EISCD data to identify the name of the receiving PSP.*

For outbound APP fraud, differences between firms were less stark than for inbound APP fraud, but there was still significant variation in the level of APP fraud sent by different PSPs. The PSPs in our sample with the highest pre-policy outbound APP fraud rates sent 12 to 14 times the value of scams, relative to total transaction value, compared with those with the lowest rates.

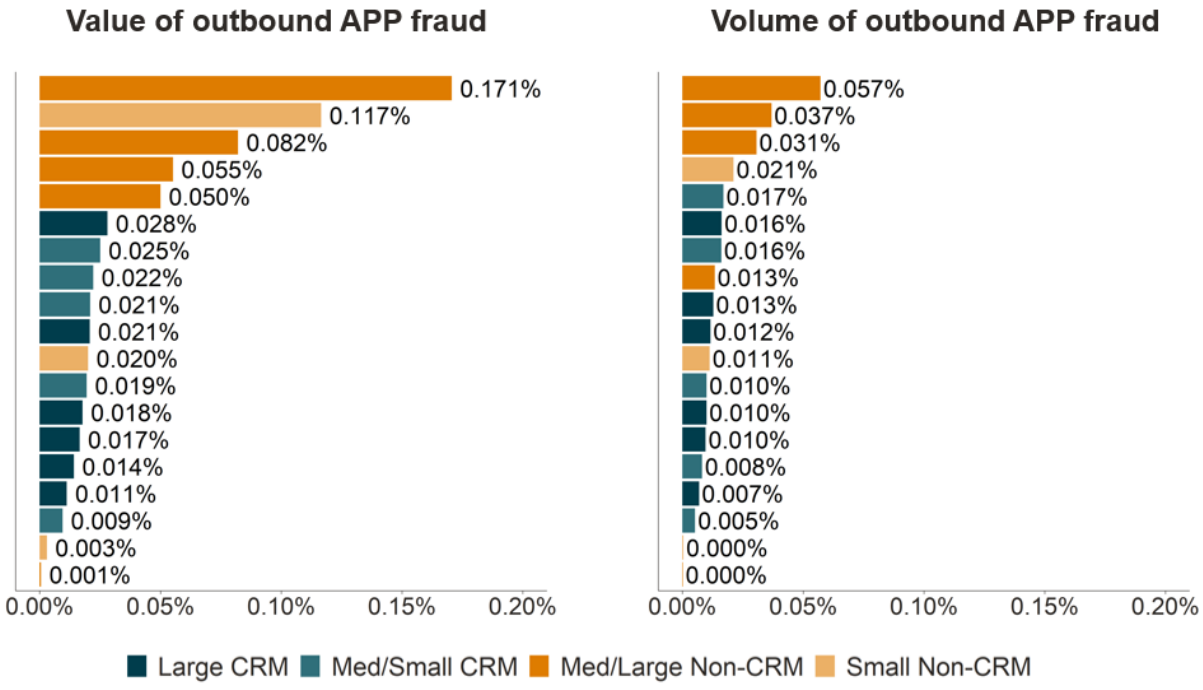
By volume, the PSPs with the highest outbound APP fraud rates sent 7 to 11 times the number of scams, relative to total transaction volumes, compared with those with the lowest rates. Outbound APP fraud rates were generally higher for medium sized and larger non-CRM firms than for small non-CRM firms. Some non-CRM firms also had outbound APP fraud rates in line with CRM signatories, suggesting that approaches to outbound APP fraud prevention

varied within the non-CRM group. As set out in Theme 1, this may reflect wider strategic priorities to protect customers and build trust.

These differences suggest that firms had materially different approaches to outbound APP fraud prevention before the policy. This is likely to reflect differences in customer warnings, outbound transaction monitoring, and processes to intervene in and stop suspicious payments.

Figure 21 illustrates the range in the value and volume of outbound APP fraud before the policy was implemented. Annex B shows fraud rates during the evaluation period individually for each PSP in this figure.

Figure 21 Value and volume of outbound APP fraud relative to total transaction activity before the policy

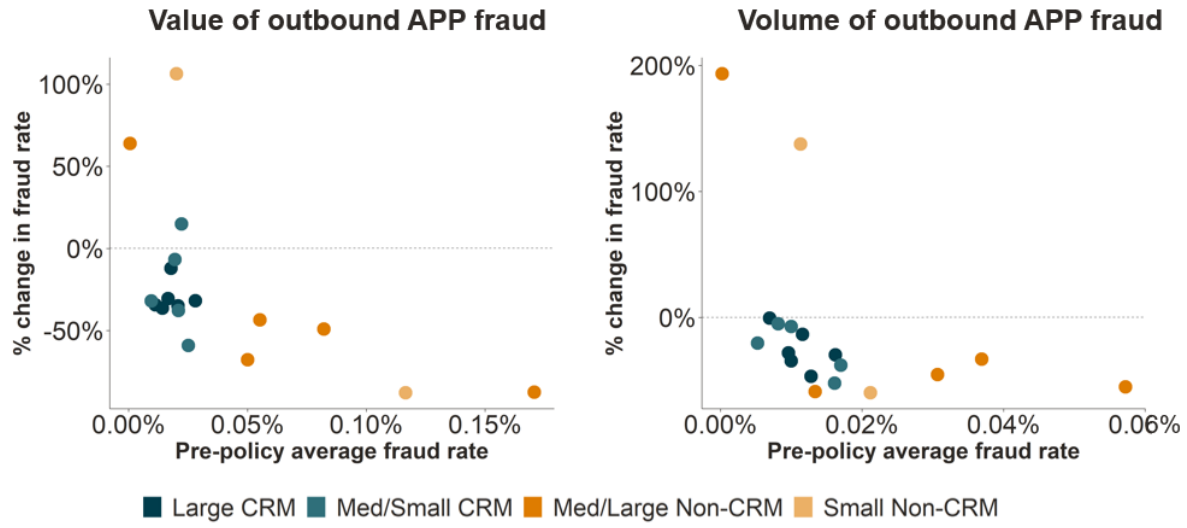


Source: *Frontier analysis of industry evaluation data*

Note: *Outbound APP fraud is shown as a percentage of outbound FPS transactions before the policy, from April 2023 to December 2023.*

As shown in Figure 22, the firms with the highest pre-policy outbound APP fraud rates reduced outbound APP fraud the most after the reimbursement requirement was introduced. The five firms with the highest pre-policy outbound APP fraud rates reduced fraud values by 43%-88%, compared with a reduction of 36% to an increase of 64% among the five firms with the lowest levels of outbound APP fraud levels. Across firms, there was a moderate negative relationship between pre-policy outbound APP fraud rates and subsequent changes in outbound APP fraud. This pattern suggests that firms with the greatest incentives and scope to reduce outbound fraud also reduced it the most.

Figure 22 Change in the value and volume of outbound APP fraud relative to total value of transactions



Source: *Frontier analysis of industry evaluation data*

Note: *Outbound APP fraud is shown as a percentage of outbound FPS transactions before the policy, from April 2023 to December 2023, and after the policy, from October 2024 to September 2025. The change is calculated by comparing the two periods.*

6.2.2 PSP interventions have been effective at reducing APP fraud

The firm-level evidence suggests that PSPs with the greatest incentives to reduce APP fraud because of the reimbursement requirement made the largest reductions. Evidence from stakeholder interviews and the voluntary evaluation PSP survey helps explain how these reductions may have been achieved because of actions taken by PSPs.

PSP interventions have been effective at reducing APP fraud in several different contexts. Section 5 sets out evidence around the actions that PSPs have taken to reduce APP fraud including new technologies, processes and operational changes to improve fraud detection and prevention. PSPs also provided evidence around how specific actions they have taken have delivered measurable improvements in APP fraud rates. Examples of these are set out in case studies 3-5 and include enhanced fraud monitoring systems, greater use of customer-facing warnings and verification tools, expanded fraud prevention teams, and the use of external scoring and behavioural analytics providers.

The case studies below draw primarily on responses from CRM signatories, reflecting the level of detail provided in survey and interview evidence. However, non-CRM PSPs also reported improvements in their APP fraud prevention controls. For example, one non-CRM PSP reported that, during 2025, it had invested in its ability to scale the volume of alerts generated for review by fraud investigators where authorised payment fraud was suspected. It reported a 207% increase in the rate of alerts generated per week, contributing to a 193% increase in the value of fraud prevented. In addition, PSP account 1 in Section 5 shows how a CEO-

sponsored change programme at a non-CRM PSP was reported to have reduced expected reimbursement rates by 50%.

PSP account 3: Enhanced fraud detection systems and expanded human intervention capacity

A large PSP reported that targeted investment in fraud detection and prevention has materially improved its ability to identify and stop APP fraud before losses occur.

Since 2021, the PSP has invested in technology solutions designed to detect unusual or out-of-character customer payment activity. These systems help identify higher-risk payments and flag them for further review. In parallel, the bank expanded its human intervention capacity, recognising that technology-led alerts are most effective when supported by teams that can engage directly with customers before a potentially fraudulent payment is completed.

The PSP invested £3.6 million in operational resource (a 42% increase in APP fraud prevention capacity). This was delivered both by increasing full-time equivalent staff numbers and by raising the corporate grade of many colleagues working in fraud prevention roles. The additional capacity allowed the bank to speak to more customers where payments were assessed as higher risk.

The PSP reported that these investments have contributed to a 43% increase in its APP fraud value detection rate since 2021, reaching 53% in 2025. [77]

PSP account 4: Targeted controls to reduce bank impersonation scams

One CRM PSP reported that it had implemented targeted controls to reduce bank impersonation scams, where fraudsters contact customers pretending to be from their bank and persuade them to make payments or disclose information.

The PSP introduced a real-time call status indicator on the in-app home screen. This enabled customers to see whether the bank was genuinely calling them, helping them identify suspicious calls from fraudsters claiming to represent the bank. The PSP also introduced enhanced fraud detection rules specifically designed to identify and flag payment activity associated with bank impersonation scams.

The PSP reported that the combination of customer-facing technology and enhanced detection rules had a significant impact. Since implementation in 2024, these controls have contributed to a reduction of more than 70% in bank impersonation scams reported to the PSP. The PSP also reported a significant reduction in the value of losses attributable to this scam type.

[77] The PSP defines value detection rate as the proportion of scam transaction value it detects before completion. For example, if £100,000 of scam transactions were attempted in a month and the bank detected £50,000, the value detection rate would be 50%

PSP account 5: Use of external providers

One CRM PSP reported that external fraud detection tools had supported improvements in its ability to identify potentially fraudulent payments. The PSP used external scoring and behavioural analytics providers to supplement its internal fraud detection controls.

The PSP reported that, following an upgrade to one external scoring model in October 2025, the value of detected fraud increased significantly compared with the previous month. Detected fraud in October 2025 was around 55% higher than in the previous month. The PSP also reported that, as of October 2025, average monthly detection in the current financial year was around 62% higher than in the previous financial year.

6.2.3 However, preventing APP fraud remains challenging

Although PSPs provided evidence that some interventions have reduced APP fraud, stakeholders highlighted a range of behavioural, detection and coordination constraints that continue to make preventing APP fraud challenging. These challenges may explain why APP fraud remains a significant issue across the industry despite the incentives of reimbursement.

Specific challenges highlighted include:

- **Behavioural barriers**: APP fraud often involves considerable victim manipulation. Victims may be psychologically committed to completing the transaction, particularly in romance and investment scams where trust may have been built over time. Stakeholders noted that customers may ignore warnings or refuse to believe they are being scammed. In these cases, *"breaking the spell"* is often most effective through human engagement and direct conversation with the customer. However, this can be resource intensive. PSPs reported that these cases can require multiple calls, sometimes lasting hours, with experienced fraud prevention staff. Even then, some customers remain unwilling to accept that they are being scammed.

- **Detection constraints**: APP scams can be harder to detect than unauthorised fraud because the customer may appear to be acting normally. Stakeholders noted that authorised push payments contain less transaction data than card payments, and behavioural or device-level signals may be weak, absent or suppressed through social engineering. These constraints are particularly acute for purchase scams and single, low-value payments, which may not appear sufficiently unusual to justify intervention. One PSP described prevention in these cases as *"almost non-existent",* noting that alerts for small, one-off payments risk overwhelming operational teams or creating disproportionate friction for legitimate customers.

- Some PSPs also reported investing in **device-level behavioural or biometric profiling to support detection**. However, respondents acknowledged the limits of these approaches. For instance, one fraud tech provider noted that in some cases "*you don't*

know anything because actually your customer doesn't appear to be a victim of fraud", highlighting the inherent challenges of identifying social engineering where behavioural signals are subtle or absent.

- **Coordination constraints:** As set out in Theme 1, stakeholders highlighted that fraud intelligence remains fragmented, with limited real-time data sharing between firms. This can reduce PSPs' ability to identify suspicious accounts, scam typologies and cross-firm patterns.

Overall, the evidence suggests that PSP interventions can reduce APP fraud, but prevention remains inherently constrained by the nature of APP scams. As one fraud technology provider put it, *"There are only so many payments you can stop. There are only so many customers you can interact with. And that is a fundamental constraint on the opportunity for you to push down on this problem, in addition to the fact that you only know what you know."*

6.2.4 No evidence that consumer awareness and willingness to claim have changed

Changes in consumer awareness or willingness to claim could affect how recorded APP fraud trends should be interpreted. If the reimbursement requirement increased awareness that victims may be eligible for reimbursement, a higher proportion of victims may have notified their PSP after experiencing APP fraud. All else being equal, this would increase recorded claims relative to the underlying level of APP fraud. As a result, if awareness has increased, the observed fall in comparable APP fraud rates may understate the extent to which APP fraud experienced by consumers has fallen.

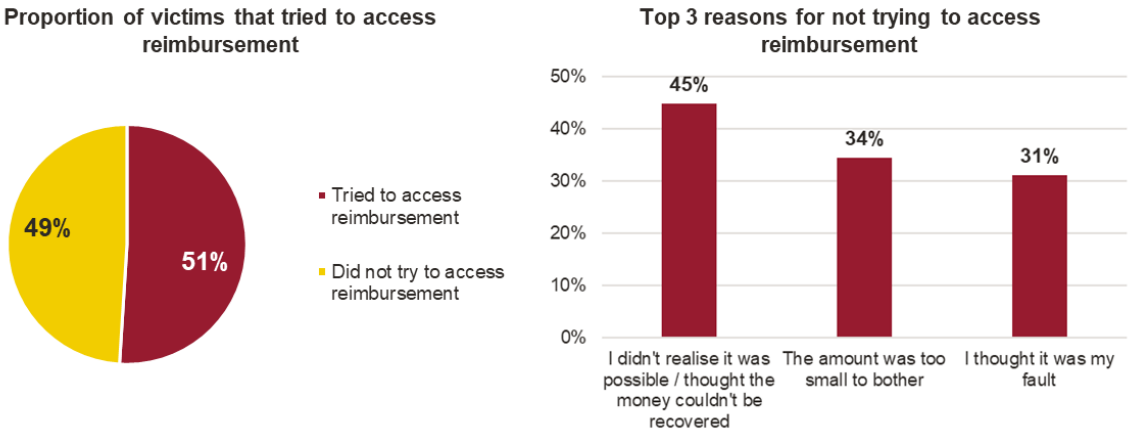
We were unable to find conclusive evidence on how customer awareness or willingness to claim has changed since the reimbursement requirement was introduced. It is therefore unclear whether the observed fall in comparable APP fraud rates is understated for this reason.

- Participants in our stakeholder interviews had mixed views on whether consumer awareness and willingness to claim had changed since the reimbursement requirement was introduced. Some stakeholders perceived increased awareness and willingness among consumers to come forward after an APP scam. One non-CRM PSP observed that "*consumers were changing their behaviours… more willing to come forward… more customers will be aware that they could seek reimbursement".* A consumer group and some PSPs also pointed to increased discussion on public forums and the use of AI and search engines to identify ways to recover funds after scams, suggesting greater informal awareness of claim routes.

- However, awareness of the policy remains low. Data from the PSR APP Fraud Consumer Survey, carried out in January 2025, suggests that only 24% of consumers are aware of the policy and just half of consumers experiencing APP fraud try to access reimbursement. As shown in Figure 23, among surveyed victims, 51% tried to access

reimbursement, while 49% did not. The most common reason for not doing so was that victims did not realise recovery was possible or thought the money could not be recovered, cited by 45% of those who did not try to claim. This suggests that low awareness and low confidence in recovery may still prevent some victims from seeking reimbursement.

Figure 23 Proportion of victims that tried to access reimbursement and reasons for not doing so



Source: *Frontier analysis of PSR APP Fraud Consumer Survey*
Note: *Data only covers victims since the introduction of the reimbursement requirement*

6.2.5 Claims include some cases on the boundary between civil dispute and APP fraud

We also considered whether the reimbursement requirement has changed which transactions are identified or claimed as APP fraud. This matters because recorded APP fraud claims may change not only because the underlying level of fraud changes, but also because consumers or firms identify, present or classify more cases as APP fraud. For example, an increase in cases on the boundary between civil disputes and APP fraud could increase the volume or value of claims received by PSPs, even if the underlying level of APP fraud had not increased. Theme 3 considers the implications for consumers whose claims are classified as civil disputes rather than APP fraud.

Stakeholders highlighted this issue in relation to claims that sit on the boundary between APP fraud and civil disputes. Some PSPs raised concerns that the reimbursement regime could increasingly be used as a chargeback-type route for complaints that are more appropriately treated as civil disputes and therefore outside the scope of the APP fraud regime. This could include, for example, consumers seeking reimbursement through the APP fraud process for goods or services that were unsatisfactory or not delivered as expected.

Doorstep scams were identified as a particular area of concern by consumer groups and those involved in APP scam enforcement, as it can be difficult to determine whether the consumer was deceived or whether the case is better characterised as a dispute over the underlying transaction.

Firms also reported that these cases can be difficult to identify and communicate about at the point a claim is raised, as it may not initially be clear whether the case involves deception amounting to APP fraud or a dispute over the underlying transaction.

Industry evaluation data shows that a significant proportion of APP scam claim value is rejected due to being ruled a civil dispute: on average for every £100 losses confirmed as an APP scam there is £16 worth of claims rejected due to being classed as a civil dispute and for every 100 confirmed APP scams 7 cases are rejected as civil disputes.

However, the available data does not show whether this has changed since the reimbursement requirement was introduced. We do not have comparable pre-policy data on claims rejected as civil disputes. We therefore cannot determine whether the reimbursement requirement has led to more boundary cases being claimed as APP fraud.

6.2.6 No evidence that the level of customer caution has changed

The reimbursement requirement could have unintended consequences on customer caution. Specifically, it could create moral hazard, which would occur if consumers were less cautious or take greater risk when making payments because they do not face the full costs of their actions.

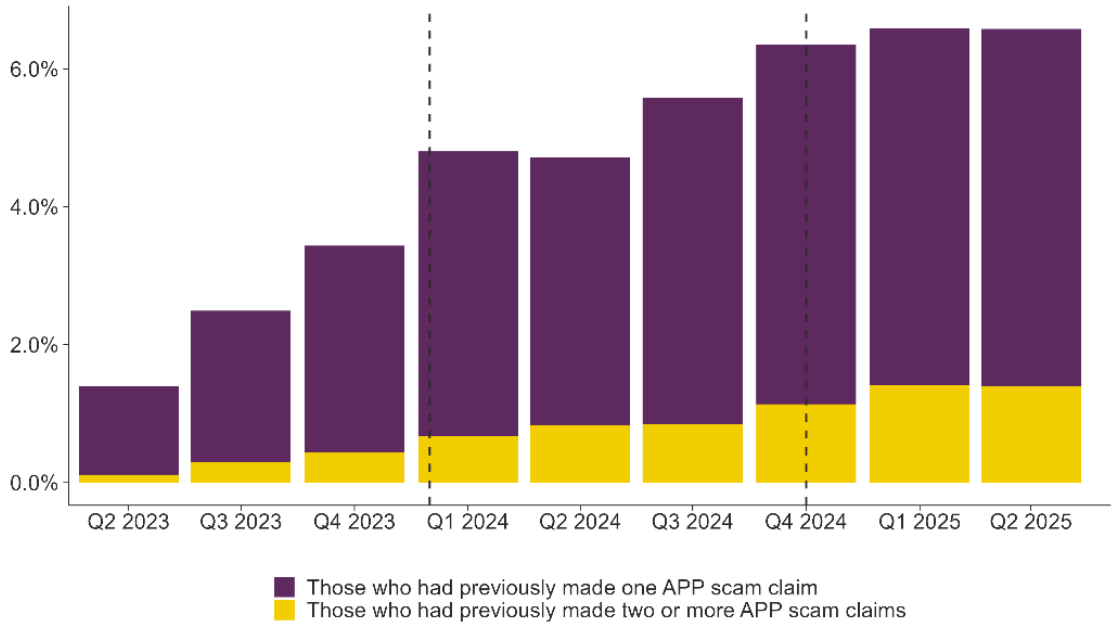
We find no evidence that the reimbursement requirement has increased moral hazard. If customer caution had declined, we might expect to see an increase in scams linked to repeat claimants, a high level of claims rejected under the CSOC exception, or qualitative evidence that consumers are changing their behaviour. Overall, the evidence does not suggest a material change.

Repeat claimants

Survey evidence from the PSR APP Fraud Consumer Survey shows that consumers who have previously been reimbursed feel more confident that they would be reimbursed again if they sent money to a fraudster. 53% in this group were confident that they would receive their funds back compared to 30% of those who had not been reimbursed and 25% of those that had not fallen victim to APP fraud. This indicates that receiving reimbursement makes consumers more confident about making future claims.

There is no evidence however that the reimbursement requirement has increased the likelihood of repeat claims. Figure 24 shows that repeat claims have been increasing but that this increase began before the reimbursement requirement was introduced and it does not appear to have accelerated. A rising share of repeat claims will naturally occur to some extent as time passes and more people are exposed to multiple frauds.

Figure 24 Share of APP fraud claims where the customer had previously made a claim



Source: *Frontier analysis of industry evaluation data*

Note: *Data from 18 PSPs. Repeat claims, in our industry evaluation data, are identified only where multiple claims are made to the same PSP. The data does not capture whether the same individual has made claims across different PSPs.*

Claims rejected under CSOC

The Consumer Standard of Caution (CSOC) allows firms to reject reimbursement claims if they believe that consumers have not been cautious enough when making a payment. A high proportion of claims being rejected could be indicative of a low level of consumer caution. Since implementation, CSOC rejections have remained relatively low at market level, representing around 3% of scam claims by value and 4% of cases. However, CSOC was not tracked before the reimbursement requirement, so we cannot assess whether rejection rates have changed over time. In addition, some PSPs have argued that the CSOC threshold is too high or difficult to apply, meaning low rejection rates may not fully reflect firms' views on whether customers are taking sufficient care. There is also evidence that PSPs apply the CSOC exception differently. CSOC and differences in firm approaches to it are further discussed in Section 7.2.

Qualitative evidence

Most stakeholders reported no clear evidence that there is a change in consumers' caution when making payments because of the reimbursement requirement. Consumer groups strongly rejected the idea that reimbursement has materially altered behaviour, stating that there is *"no evidence whatsoever"* of widespread moral hazard.

However, some PSPs expressed concern that the mandatory reimbursement requirement may reduce incentives for customer caution, particularly for low-value, high-volume transactions such as purchase scams. Several respondents noted that, if moral hazard were to emerge, it would most likely be visible in these lower-value transactions rather than in higher-value scams. As one PSP put it:

> *"You won't bother to check when you're buying a pair of expensive trainers from somebody you've never met before on Facebook Marketplace, because [we've] got your back. You'll just say, I've been scammed. They're the wrong colour. They didn't turn up. I've lost my money [and] we'll refund you within 24 hours..."*

> *"So what possible incentive is there for a customer to do any checks. We can't prove it's a consequence, but we know undoubtedly that the caution, the incentive for customers to be cautious has been taken away."*

When respondents were asked how moral hazard could be influencing behaviour despite low consumer awareness of the reimbursement requirement, views focused less on explicit knowledge of the policy and more on the difficulty of persuading customers to take warnings seriously where they believe they are unlikely to bear the loss. One PSP argued that simple messaging is necessary to engage customers and it is inherently difficult to encourage vigilance where the perceived consequences of loss are reduced, noting that *"it's very difficult for us to get consumers to be alert because they could lose money because in theory they're not going to."*

6.2.7 Confirmed first-party fraud is low, although suspected cases may be rising

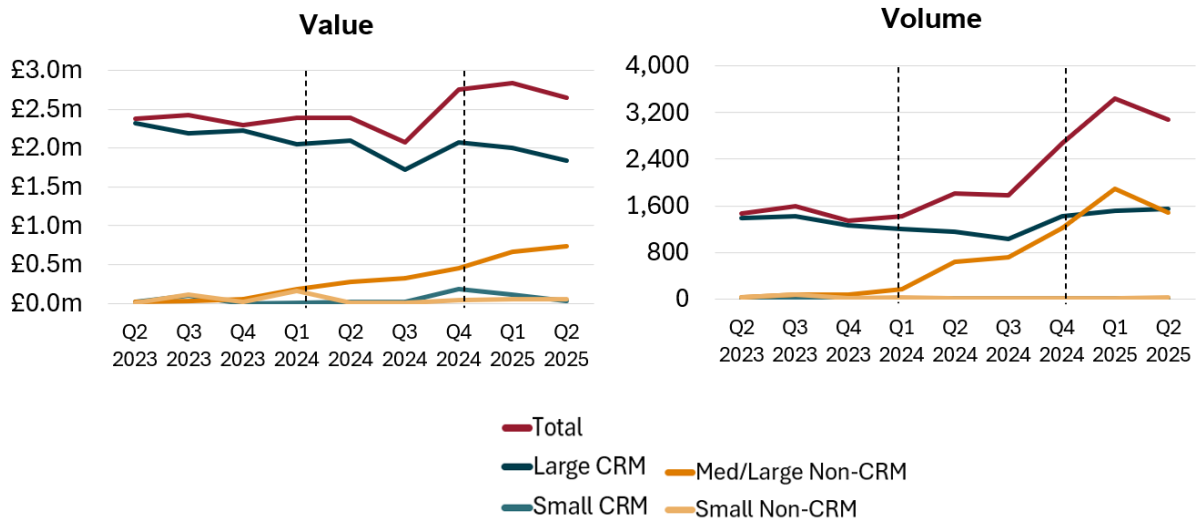
The logic model identifies first-party fraud as a potential unintended consequence of the reimbursement requirement. First-party fraud occurs where a consumer falsely claims fraud. The reimbursement requirement could increase first-party fraud if it makes it more likely that a false claim is accepted. This may occur because, as PSPs report, first-party fraud is often difficult to detect. In many cases, firms may suspect that a claim is fraudulent but not have enough evidence to reject it, particularly given the timescales for assessing APP fraud claims. Consumer groups have also pointed out that PSPs can "stop the clock" to investigate suspicious claims more thoroughly, and argued that where this option is not used, concerns about first-party fraud may not always be sufficiently well-founded to justify rejecting reimbursement.

As shown in Figure 25, data from the FCA-PSR Joint Survey suggests that reported suspected first-party fraud has increased since the reimbursement requirement was introduced. By value, suspected first-party fraud increased from a quarterly average of £2.4m (between Q2 2023 and Q2 2024) to £2.8m (between Q4 2024 and Q2 2025). By volume, suspected cases increased from 1,500 to 2,600 over the same period.

However, this appears to be driven by a small number of PSPs. As can be seen in Figure 25, this increase in suspected first-party fraud is entirely driven by the increase experienced by

medium/large non-CRM firms. Interpreting this finding as a market-wide trend should therefore be treated with caution.

Figure 25 Suspected first-party fraud cases



Source: *Frontier analysis of FCA PSP APP Fraud survey*

Note: *The data reflects the submissions of 18 PSPs, not scaled to market level. Figures are presented without controlling for changing transaction values over time, however doing so does not materially change our findings.*

This is consistent with reports from stakeholders in interviews. Consumer groups and some PSPs reported no clear increase in first-party APP fraud. However, one PSP had estimated that first-party fraud had increased by 10-20% since the introduction of the reimbursement requirement. They stated that *"a first-time fraudulent claim is highly likely to be refunded as they are difficult to identify under tight timescales applied."* Some other PSPs did not have data but cited emerging concerns around potential abuse of the reimbursement process.

So far, confirmed first-party fraud is low at market level. Claims rejected due to first-party fraud account for 0.5% of claims by value and 0.2% of claims by volume. This is further discussed in Section 7.2 below. However, there is inherent uncertainty over the true level of this fraud.

Overall, the evidence suggests that while total APP fraud has fallen, first-party APP fraud may be rising. While confirmed cases are a small share of claims there is also inherent uncertainty over the true level of the fraud.

6.3 How have levels of other fraud changed?

In this section, we consider whether other types of fraud have changed over the same period as APP scams. The extent to which any observed changes in other frauds may be driven by the APP scam policies is discussed in Section 7.4.

The evidence in this section needs to be interpreted cautiously because the data for many out-of-scope fraud types is measured by claim date rather than scam transaction date and is not collected as consistently as APP scam data.

6.3.1 Out-of-scope APP fraud has grown significantly

Some APP scams are outside the scope of the reimbursement requirement. This includes APP scams involving international payments, payments to crypto exchanges, Bacs payments and intrabank transfers.

Evidence shows that out-of-scope APP scam claims have increased between 2023 and 2025. Annual losses form international APP scams, which are generally not reported in overall UK APP scam statistics, have increased by £39m. Annual losses from Crypto APP scams have increased by £106m, but much of this increase is captured in the overall APP fraud trends discussed in the sections above and therefore should not be treated as incremental APP fraud.

International APP scams

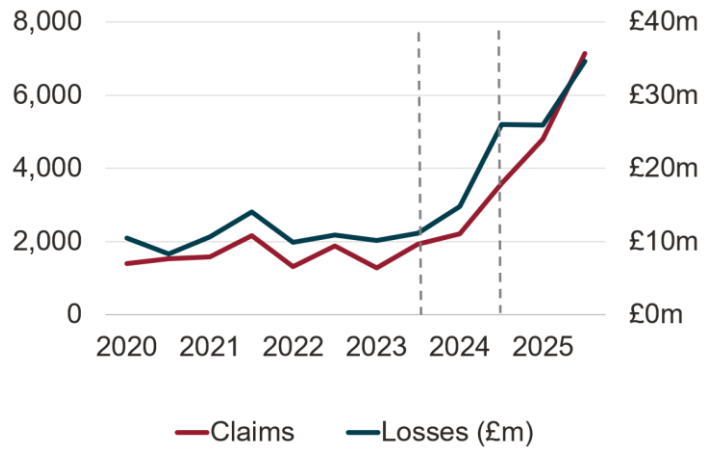
The losses from international APP scams (all APP scam payments sent to non-UK bank accounts), as reported by UK Finance, were relatively constant during 2020 to 2023, but then rose sharply starting in 2024.[78] As shown in Figure 26, annual losses for consumers from international APP scams have more than doubled from £21m/year in 2023 to £60m/year in 2025.[79] This increase happened around the same time as UK domestic APP scams reduced. Volumes have also increased: by 8,700 per year from 3,200 claims in 2023 to 11,900 claims in 2025.

It is not possible to say, based on quantitative evidence, whether this increase is due to displacement of APP fraud or an increase that would have happened anyway. PSP actions to combat inbound fraud into UK accounts may have resulted in more fraudsters using international accounts as the destination for funds, which would fuel a shift from in-scope APP fraud to international payments. On the other hand, PSP actions to tackle outbound in-scope APP fraud may also have helped increase the detection and prevention of fraud payments to international accounts, which would lower this form of fraud relative to what it otherwise would have been without the APP scam policies.

[78] UK Finance (2026). Annual Fraud Report 2026.

[79] UK Finance (2026). Annual Fraud Report 2026. We estimate the international APP fraud that relates to personal accounts by assuming that the proportion of international APP fraud from personal accounts is the same as the proportion of total APP fraud from personal accounts. We do not measure the increase in international APP scams as a proportion of all consumer international payments due to lack of robust data on the value of consumer international payments for 2024 and 2025.

Figure 26 Estimated value and volume of international APP scams



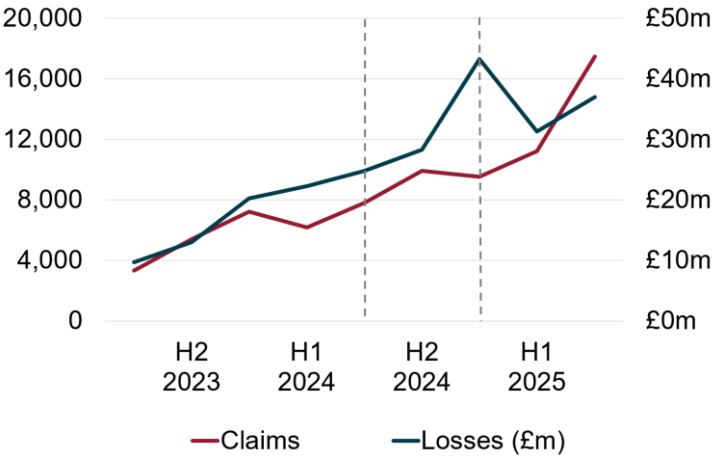
Source: *Frontier analysis of UK Finance's Half Year Fraud Report 2025 and Annual Fraud Report 2026*

Note: *Data shown is APP fraud from personal accounts only. We calculate the international APP fraud that relates to personal accounts by assuming that the proportion of international APP fraud from personal accounts is the same as the proportion of total APP fraud from personal accounts*

Crypto scams

Payments to crypto exchanges are not covered by the reimbursement requirement, even when the customer has fallen victim to an APP scam. We use data from the FCA-PSR Joint Survey to estimate the approximate scale of crypto APP scams in the UK. As shown in Figure 27 APP scam claims for payments to crypto exchanges have grown significantly. In 2025, annual losses are estimated to be around £153 million, up from £59 million in 2023. The volume of claims has also increased, from 22,000 claims in 2023 to 52,000 claims in 2025.

Figure 27 Estimated value and volume of APP fraud claims for payments to crypto exchanges



Source: *Frontier analysis of FCA-PSR Joint Survey*

Note: *The estimate is scaled to market total from the reported crypto fraud of 13 PSPs that cover 58% of the FPS market. The levels reported by one fintech were much higher than the rest of the sample. This firm's data is excluded from the average used for market scaling to reflect the fact that it is not representative of most of the market.*

The value of crypto scams was already on a growing trajectory before the reimbursement requirement policy was finalised in December 2023. This pattern is likely to at least partially reflect wider growth in crypto payments and crypto-related scams.[80] The growth rate of crypto APP scam value increased significantly during the transition period until the implementation of the policy in October 2024. Since the reimbursement requirement came into effect, losses to crypto scams have slightly reduced. This means the growth in crypto APP scams cannot necessarily be attributed to displacement from in-scope APP scams.

The number of crypto APP scams has increased significantly since the policy came into effect in October 2024, suggesting a shift towards a greater number of lower value crypto scams.

These estimates of crypto APP scams should not be interpreted as entirely additional APP fraud on top of other types of UK APP fraud discussed in Section 7.1. Many PSPs record crypto APP scams as part of their total APP scam reporting. Much of the growth in crypto APP scams is therefore a subset of the general APP fraud trends shown in Section 7.1. However, not all PSPs reported crypto scams as part of the industry evaluation data and some of the estimated reduction in APP scams is likely to be offset by increases in crypto scams. We cannot quantitatively estimate the scale of this, nor how much of this change could be attributable to the reimbursement requirement.

Bacs and interbank scams

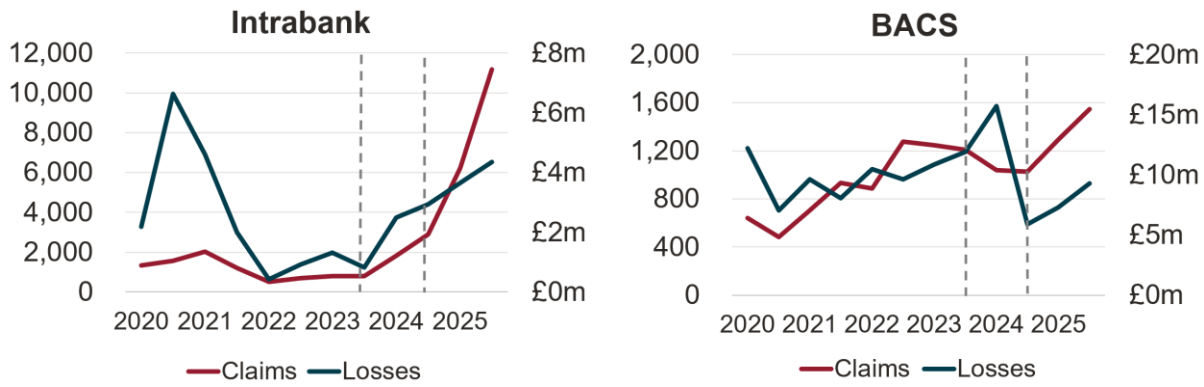
APP scams over Bacs and intrabank payments (transfers between two accounts held at the same PSP)[81] are not in scope for the reimbursement requirement. The evidence suggests that there has been a change in APP scams over intrabank payments, but not in Bacs.

- There has been a significant increase in the number of intrabank APP fraud cases. They have grown from under 2,000 cases in 2023 to nearly 18,000 cases in 2025. The number of cases remains relatively low to the number of scams over FPS (over 480,000 cases in 2025). The average losses from intrabank APP fraud have not increased by the same extent, suggesting that there is a larger number of smaller scams taking place over intrabank rails since 2023.
- APP scam losses over Bacs have fallen since 2024 to levels consistent with 2020 APP scam losses. The number of APP scam cases over Bacs remains low.

[80] The trend in crypto APP scams as a proportion of all crypto payments was not analysed due to lack of robust data.

[81] Sometimes called an ‘on us’ transactions.

Figure 28 APP fraud claims and losses over intrabank and BACS transfers



Source: Frontier analysis of UK Finance's Half Year Fraud Report 2025 and Annual Fraud Report 2026

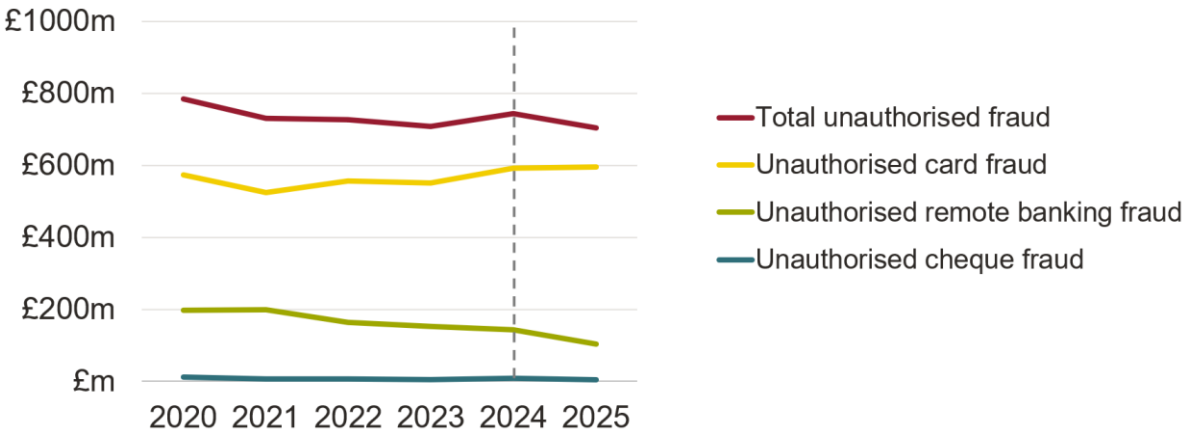
6.3.2 Unauthorised fraud has remained constant

Unauthorised fraud is fundamentally different to APP fraud. It relates to cases where a customer's card or remote banking details are compromised and used without the victim's consent. Unauthorised fraud is not in scope for the reimbursement requirement.

Unlike APP fraud, there is typically no material delay between unauthorised fraud transactions happening and customer claims, so unauthorised fraud claim data is a reasonable measure of contemporaneous unauthorised frauds.

As shown in Figure 29, UK Finance Fraud Reporting data shows that unauthorised fraud losses have remained broadly unchanged since the policy was introduced, with total losses of £703m in 2025, close to the £709m recorded in 2023. Over the same period, card fraud losses increased from £551m to £595m, while remote banking fraud losses fell from £152m to £104m. Cheque fraud remained a small component of unauthorised fraud losses throughout.

Figure 29 Value of unauthorised fraud losses



Source: Frontier analysis of UK Finance's Half Year Fraud Report 2025 and Annual Fraud Report 2026

6.4 To what extent are the changes in other fraud attributable to the APP scam policies as opposed to driven by other factors?

In section 6.3 we set out evidence for changes in out-of-scope fraud, finding that there is evidence that some such frauds have increased. This could be driven by many factors, including the rise in fraudsters making use of Artificial Intelligence-enabled tools that allow fraudsters to target victims in increasingly sophisticated ways. In this section we set out the available evidence on the extent to which the reimbursement requirement may have contributed to these increases by diverting the activities of fraudsters or changing the behaviour of PSPs. There is:

- clear evidence that fraudsters have changed their focus and will have done so quickly; and
- mixed evidence on whether PSP behaviour has changed, with some evidence that smaller PSPs may have had to divert investments from out-of-scope fraud prevention to actions focused on reducing in-scope fraud.

6.4.1 Fraudsters have moved their efforts away from APP fraud to other frauds

Given the observed increases in some out-of-scope fraud types, we considered whether tighter controls on in-scope APP fraud may have contributed to these trends by prompting fraudsters to shift activity to other fraud types or payment channels.

Recent evidence from academic literature suggests that when controls reduce opportunities for one type of fraud, criminals may divert activity to other types of fraud or other payment channels. Balasubramaniam et al. (2025), using 1.19 million posts from underground cybercrime forums to evidence, find that fraudsters adapt their methods in response to anti-fraud technologies.[82] It showed that anti-fraud technology deployments, discussion of circumvention techniques rises, indicating a shift toward harder-to-detect approaches.

Consistent with these findings, the UK Finance Annual Fraud Report 2025 documents that reductions in APP fraud losses and cases coincided with increases in other fraud types, most notably remote purchase fraud. UK Finance explicitly interprets this pattern as evidence of fraudster adaptation, noting that "*closing one vulnerability in isolation only leads criminals to adapt and exploit others*".[83]

This is consistent with stakeholder views. Across interviews, stakeholders frequently described fraud as displacing across payment methods rather than being eliminated. Respondents used metaphors such *as "fraud is like the balloon, you squeeze it, it goes*

[82] Balasubramaniam, V., Mosk, T.C. and Uettwiller, A. (2025) *Who pays for payment fraud? Detection and liability rules under strategic fraudster adaptation*. Available at SSRN: https://ssrn.com/abstract=5703762 or http://dx.doi.org/10.2139/ssrn.5703762 (Accessed: 1 May 2026).

[83] UK Finance (2025). Annual Fraud Report 2025.

somewhere else" to illustrate how tightening controls in one area can lead to increased fraud activity elsewhere.

Several stakeholders supported the view that, as controls on APP transactions have tightened, fraudsters have increasingly shifted towards out-of-scope fraud that are perceived to involve fewer controls or lower risk. These included cash withdrawals, card fraud, and more complex, layered scam structures.

Stakeholders did not believe that published APP fraud performance data affected fraudster targeting, as the reporting lag limits its relevance to current system changes. They argued that the reporting lag limits the relevance of published data to fraudsters, who adapt more quickly to operational changes. As one PSP put it, *"If a new change is put in a system… the fraudsters are there within a couple of days."*

6.4.2 Impact of investments in APP fraud on other fraud types is unclear

We also considered whether PSPs' increased focus on in-scope APP fraud had affected their ability to prevent other types of fraud. PSPs reported mixed effects. On the one hand, many PSPs in our stakeholder interviews said that investment in APP fraud prevention had improved their overall fraud prevention activity and contributed to tackling other fraud types. On the other hand, several PSPs interviewed reported that the focus on APP fraud prevention had diverted resources from other fraud control activity and negatively affected their efforts to tackle other fraud types.

Positive spillover effects

Many PSPs reported that investments in APP fraud prevention had also strengthened their broader fraud and financial crime capabilities. These investments included enhanced monitoring, analytics and ongoing surveillance, which can be applied across multiple fraud typologies rather than only APP fraud.

One non-CRM bank said that these investments had *"contributed to a more holistic, cross-typology control framework, improving our overall fraud risk management."*

This suggests that some PSP responses to the reimbursement requirement may have generated positive spillovers beyond APP fraud, by improving firms' wider ability to detect, monitor and respond to suspicious activity.

Shift of attention away from other types of frauds

At the same time, some qualitative evidence suggests that greater focus on APP fraud may have diverted resources from other fraud risks, particularly for smaller PSPs.

Many PSPs described APP fraud as receiving heightened attention because reimbursement losses from the new requirements are immediate and visible on the profit and loss account. This created incentives to allocate engineering, analytical and operational resources towards

APP fraud controls. This may be a stronger incentive compared to fines for poor performance in addressing other financial crime.

The impact appears to vary by firm type. Larger PSPs generally reported being more able to absorb trade-offs and to stand up dedicated programmes without displacing other work. Smaller PSPs faced proportionally greater constraints, with some indicating that resources had been diverted from other fraud or financial crime priorities.

7 Theme 3 Findings: Impacts on consumer welfare

In this theme, we consider the impact of the policies on consumers and businesses. We look at the extent to which victims of fraud are reimbursed and treated consistently between PSPs. We next consider what reduction in harms consumers may have benefited from given the reduction of APP fraud outlined in Section 8.1. We also summarise stakeholders' views as to whether the policies have created additional payment friction or affected use of Faster Payments and Open Banking.

7.1 What has been the impact of the policies on victims of APP fraud?

This section assesses the impact of the reimbursement requirement on victims of APP fraud who make claims. We find:

- clear evidence of an increase in the reimbursement rate for victims of fraud; and
- evidence that reimbursement still varies between PSPs which is driven by differences in approach and interpretation of the rules, as well as the types of APP scams victims fall for.

7.1.1 Consumer reimbursement has increased

Section 7 examined scams according to the timing of transactions to understand the impact of the policy on scam levels over time. This section focuses on the impact of the policy on victims who have made APP fraud claims. The analysis is therefore based on APP fraud claims data, rather than transaction-level APP fraud data.

To examine changes over time in reimbursement rates, we use industry evaluation data and Standard A data. We calculate the reimbursement rate before the policy using industry evaluation data: the value of reimbursements made divided by the number of confirmed APP scam transactions raised as a claim during the same period. We calculate the reimbursement rate after the policy by dividing reimbursements as reported in Standard A by an estimation of the relevant claims from the industry evaluation data: the number of confirmed APP scam transactions raised as a claim in the same period, where the transactions happened after October 2024.[84]

[84] We take this approach, rather than dividing by the value of 'in-scope' APP scam claims as reported in Standard A, because there are significant inconsistencies in how firms report APP scam claims in Standard A. The PSR and several PSPs that we engaged with have noted that there are differences in how firms triage and record in-scope APP scams in Standard A depending on their business model. Some firms will record all potential claims they receive (e.g. through an online portal) while others may not record claims that are deemed ineligible for consideration (e.g. due to timing or definitions). Using all confirmed APP scam claims from the industry evaluation data allows for a like-for-like comparison between PSPs and over time.

This is not a perfect measure of reimbursement rates. There are differences in recording practices both across datasets and between PSPs. However, our approach provides the best available measure of APP scam reimbursement that can be compared over time.

It is important to note that our measure includes claims that are not reimbursed due to policy limits and exceptions such as the CSOC, the optional excess and the reimbursement cap. Reimbursement rates after the introduction of the policy are therefore not expected to be 100%. For several PSPs, the data also includes APP scams that are out of scope of the reimbursement requirement, such as crypto APP scams and me-to-me APP scams.

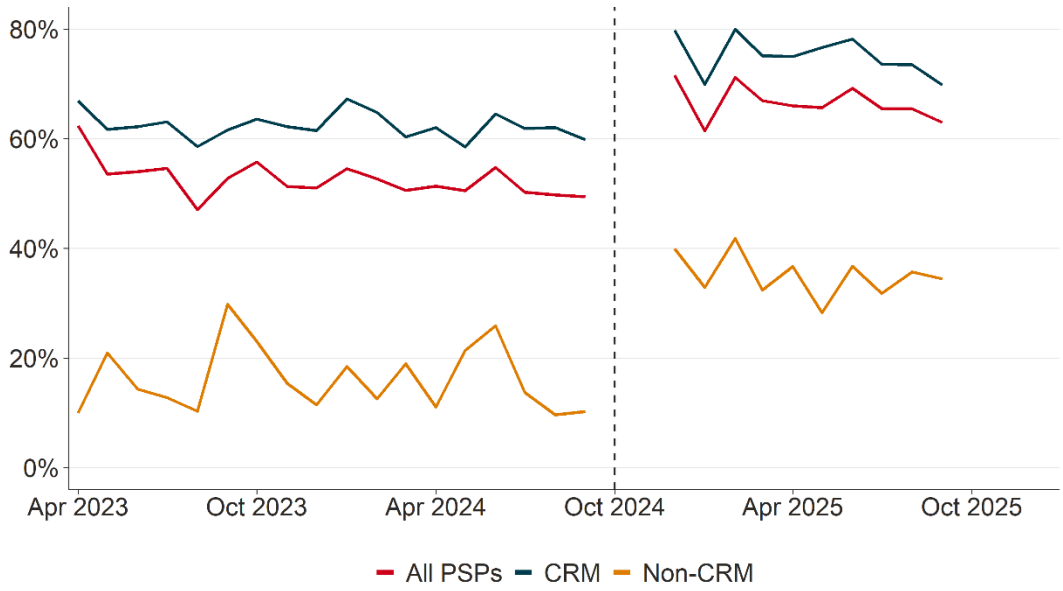
Our measure suggests that reimbursement to APP fraud victims has increased since the introduction of the reimbursement requirement.[85] As shown in Figure 30:

- 65% of APP fraud losses were reimbursed to victims by their PSP after the policy was implemented, compared to 54% before.
- For CRM firms that already reimbursed consumers at a high rate before the policy, the difference in the reimbursement rate is moderate, 73% after the policy compared to 64% before. The average reimbursement rate for non-CRM firms is just over twice as high after the introduction of the policy as compared to before, 35% compared to 16%.
- The reimbursement rate of non-CRM firms remains nearly 40 percentage points or under half that of CRM firms.

This increase in market-level reimbursement rate would equal a £39m/year increase in total consumer reimbursement if the level of APP fraud had remained unchanged since pre-policy levels in 2023. This is explained further in Section 9.1.

[85] We define the pre-policy period as April 2023 – September 2024 and post-policy period as January – September 2025. Unlike in Theme 2, there is no transition period before October 2024 as we do not expect firms to change their reimbursement rates in anticipation of the policy. The data confirms this: reimbursement rates have been relatively stable throughout the pre-policy period. Reimbursement rates post-policy stabilise starting from January 2025, which we use as the starting point for the post-policy period.

Figure 30 Total proportion of FPS APP fraud value reimbursed, by month of claim



Source: *Frontier analysis of industry evaluation data*

Note: *Data from 17 PSPs. Reimbursement rate is measured as reimbursements paid out as a proportion of all confirmed APP scam claims in the same month. Data pre-policy relates to all scam claims reported in that month. Data post-policy only relates to scam claims for transactions since October 2024.*

Our estimate of the proportion of APP fraud reimbursed is materially lower than the 88% reported by the PSR.[86] The figures reported by the PSR measure 'reimbursable claims', which are claims where the PSPs have assessed at least part of the claim as meeting the requirement for reimbursement. It does not include claims that are not reimbursed due to policy exclusions. For this reason, we believe our measure is a more accurate representation of the reimbursement of in-scope APP scams.

Our estimate of the reimbursement rate in the post-policy period is in line with the 64% reimbursement rate of personal APP scams reported by UK Finance.[87]

Our estimate of reimbursement rate in the pre-policy period differs from the 61%-68% reported by UK Finance.[88] This is likely driven by: our estimate not including "on-us" transactions which are not in scope for the reimbursement requirement, differences in how crypto and me-to-me scams and repatriated funds are treated, and by the differences in how the date of claim is reported.

[86] The PSR reports quarterly reimbursement statistics on its Reimbursement Dashboard based on Standard A data. PSR reported that in total 88% of claims had been reimbursed in the first year since the reimbursement requirement.

[87] UK Finance's Annual Fraud Report 2026 reports that out of £500m of personal APP scam losses £320m was returned to victims in 2025.

[88] UK Finance's Annual Fraud Report 2026 reports that £256m out of £376m APP scam losses was returned to victims in 2023 and £241m out of £399m was returned to victims in 2024.

Figure 31 below summarises the main differences between the reimbursement rates reported by the PSR and UK Finance and those reported in this evaluation.

Figure 31 Comparison of reimbursement rates and how they are calculated across different sources

Source	Time period	Reimbursement rate	Variable	Data used	Crypto and me-to-me	Losses subject to policy exclusions	"On-us" payments	Funds repatriated to consumers	Date claim recorded
This evaluation	Pre-policy (Apr 2023 – Sep 2024)	54%	Reimbursement value	Industry evaluation data	Included for most PSPs	n/a	x	✓	By month raised
			Claims value						
	Post-policy (Jan 2025 – Sep 2025)	65%	Reimbursement value	Standard A	x	x	x	x	By month closed
			Claims value	Industry evaluation data	Included for most PSPs	✓		✓	By month raised
PSR	Post policy (Oct 2024 – Sep 2025)	88%	Reimbursement value	Standard A	x	x	x	x	By month closed
			Claims value						
UKF	2023 (Jan – Dec 2023)	68%	Reimbursement value	UKF Annual Fraud Report data	✓	n/a	✓	✓	By month closed
			Claims value						
	2024 (Jan – Dec 2024)	61%	Reimbursement value		✓	x	✓	✓	By month closed
			Claims value			✓			
	2025 (Jan – Dec 2025)	64%	Reimbursement value		✓	x	✓	✓	By month closed
			Claims value			✓			

Source: *Frontier analysis of Standard A data, industry evaluation data, UK Finance's Annual Fraud Report 2026 and PSP interviews*

Note: *UK Finance's claims value refers to personal APP scams only Source*

During the final three months that Standard A data is available for (July-September 2025) the monthly average reimbursement of in-scope claims was £20m. This level of reimbursement would amount to £240m on an annual basis.

Over 20,000 victims per month have been reimbursed under the policy during July to September 2025, which would add up to more than 240,000 victims annually.

APP scams sent over CHAPS are also covered by the reimbursement requirement. CHAPS APP scams contributed to just £18m of all APP scam losses in 2025 and the number of cases

per year is under 200. Reimbursement rate for CHAPS has been 38% by value and 86% by volume of claims since the policy came into effect.

7.2 How consistently have consumers been treated by different PSPs?

The reimbursement requirement was expected to improve consistency by replacing a largely voluntary approach with a mandatory framework that applies common rules to in-scope PSPs. Section 7.1 shows that the proportion of claims reimbursed has increased and there has been convergence between CRM and non-CRM firms. That said, there remains a significant gap between PSPs in their reimbursement rates.

In this section we further detail differences we observe in the reimbursement of consumers. These differences need to be interpreted with caution. There are three main reasons why we observe differences in PSP reimbursement rates.

- First, some losses are not reimbursed because they fall outside the scope of the reimbursement requirement. This includes payments to crypto exchanges and payments between two accounts held by the same individual. For many PSPs, APP fraud data includes these types of claims, and this leads to a lower reported reimbursement rate, particularly if those PSPs have a customer base who are particularly exposed to these types of fraud.
- Second, some losses are not reimbursed due policy limits and exceptions. This includes cases where the consumer is deemed not to have taken sufficient caution (the Customer Standard of Caution exemption), the optional up to £100 excess, and the £85,000 reimbursement cap. Reimbursement rates are lower for PSPs with more cases that are not reimbursed, or not reimbursed fully, due to these exclusions.
- Third, the industry is still transitioning to the Standard A reporting standard which requires PSPs to report reimbursement and claims data. These are the data used for the analysis of reimbursement rates. Several PSPs have reported that they have encountered difficulties in reporting accurate data to Standard A. The PSPs with known data issues have been excluded from this analysis, but it is plausible that the reimbursement rates of other PSPs in the dataset are also affected by these issues.[89]

With these limitations in mind, we explore how reimbursement rates vary across PSPs and set out evidence for how PSPs appear to be applying different choices and judgements in their applications of the rules.

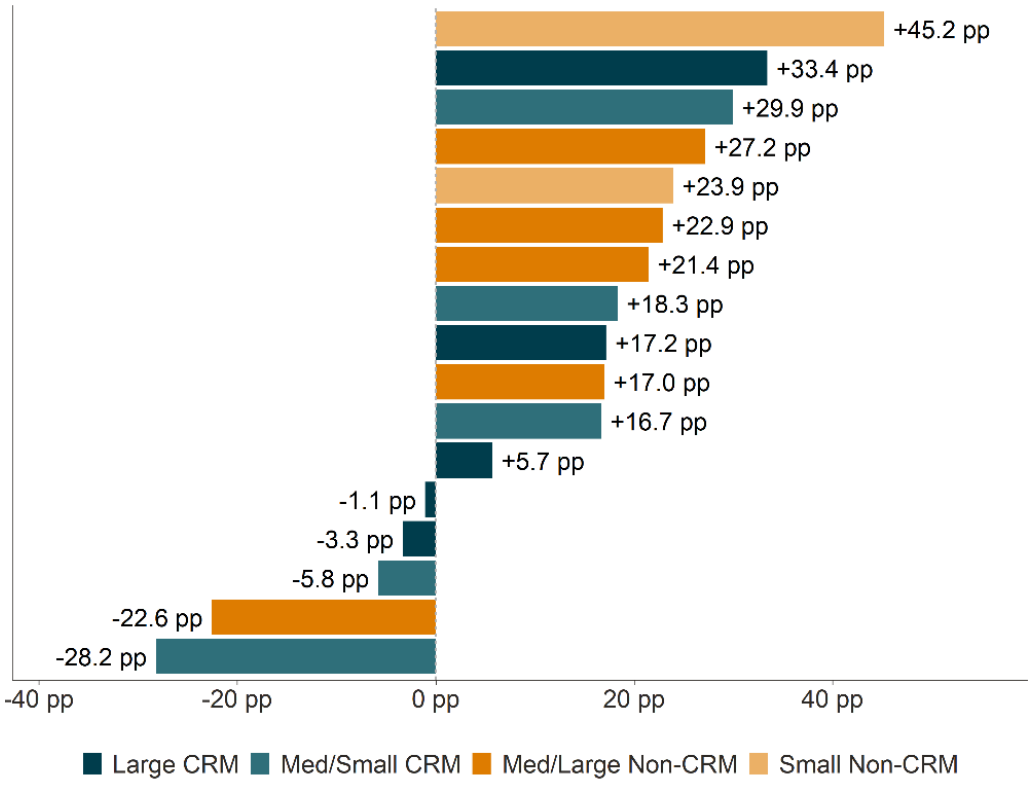
[89] Examples of this include one PSP's Standard A submission not including the reimbursement of low value claims where the PSP reimbursed customers without pursuing the 50% liability share from the receiving PSP and cases where PSP claims were underreported because they were not correctly marked on the system as "closed" and therefore did not get submitted to Standard A.

7.2.1 There is significant variation in reimbursement among PSPs

In section 7.1 we demonstrated that there is a general increase in reimbursement following the policy. Figure 32 shows that there has been significant variation between PSPs.[90]

- For all but one non-CRM firms, reimbursement rate has increased by between 18 and 45 percentage points. The smallest non-CRM firms have increased their reimbursement rates the most.
- The impact on CRM firm reimbursement rates has been mixed with some increasing reimbursement rates by up to 35 percentage points and others reducing them by up to 34 percentage points.

Figure 32 Change in proportion of FPS APP fraud claim value reimbursed compared to pre-policy rate



Source: *Frontier analysis of industry evaluation and Standard A data*

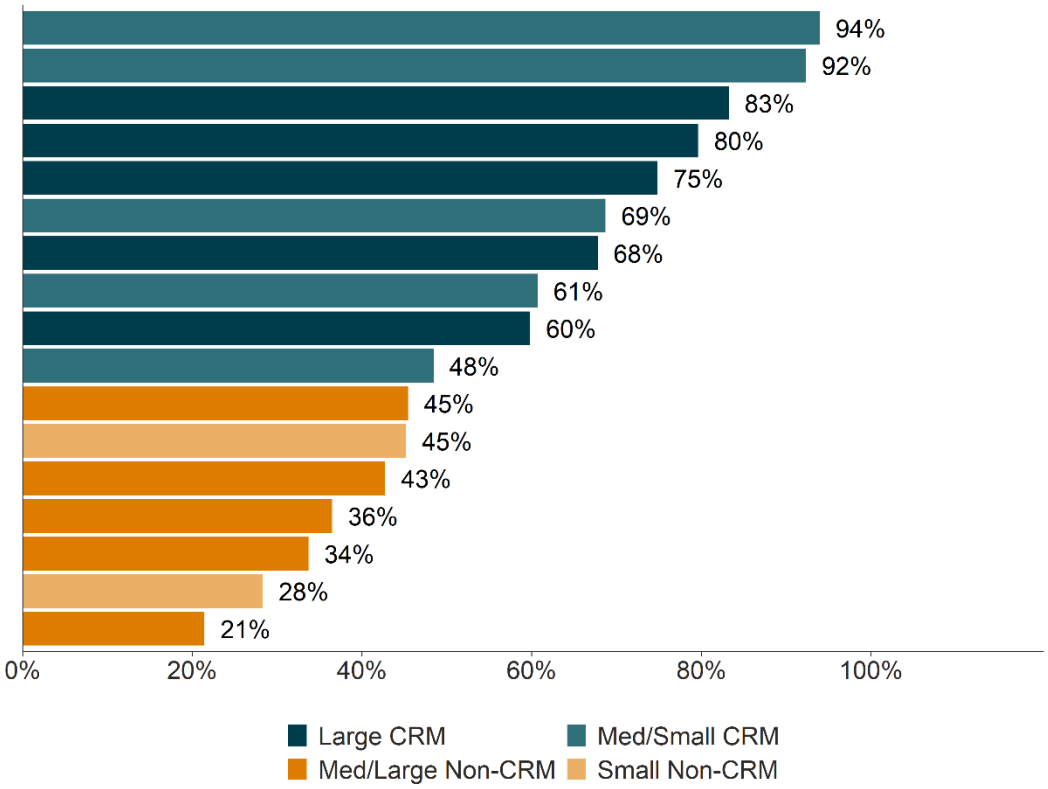
Note: *Pre-policy reimbursement rates are calculated for the period Apr 2023 - Sep 2024. Post-policy reimbursement rates are calculated for the period Jan - Sep 2025. Reimbursement rate is measured as reimbursements paid out as a proportion of all confirmed APP scam claims in the same month. Data pre-policy relates to all scam claims reported in that month. Data post-policy only relates to scam claims for transactions since October 2024.*

[90] We use the industry evaluation data for reimbursement values pre-policy and Standard A data for reimbursement values post-policy. We note that Standard A data is reported by sending firm. Firms that have only received and reimbursed APP scam claims as receiving firms do not appear in the data and we are not able to estimate their reimbursement rates post-policy, despite them being part of the industry evaluation data sample.

These variations will in part reflect differences in approach to reimbursement prior to the policy. CRMs typically had higher reimbursement rates, and we would expect to see a smaller increase compared to most non-CRMs. As noted earlier in this section, some of these observed differences may be driven by differences in how PSPs recorded data and should therefore be interpreted with caution.

Figure 33 shows there is still wide variation in reimbursement rates between PSPs. Our measure of the reimbursement rate ranges from 21% to 94%. Reimbursement rates are still uniformly higher among firms that were previously CRM signatories than among firms that were not.

Figure 33 Proportion of APP fraud claim value reimbursed after the policy



Source: *Frontier analysis of industry evaluation data and Standard A*

Note: *Data for Jan - Sep 2025. Reimbursement rate is measured as reimbursements paid out as a proportion of all confirmed APP scam claims in the same month. Data only relates to scam claims for transactions since October 2024.*

As set out above, these differences in reimbursement rates between PSPs need to be interpreted with caution. In some cases, they will be driven by how PSPs record data rather than genuine differences in reimbursement outcomes. However, there appear to be some differences in how firms judge eligibility for reimbursement, and in the choices, firms make regarding whether an excess is applied or whether reimbursements are voluntarily made where claims exceed the cap on mandatory reimbursement.

7.2.2 Firms take different approaches to classifying claims as reimbursable

All stakeholders broadly agreed that most PSPs are operating within the reimbursement framework.[91] However, many PSPs and consumer groups raised concerns related to the interpretation of the rules in some cases and by some PSPs. As one respondent summarised:

> *"Some areas are pretty cut and dry. Other areas are more subjective."*

The differences we observe in reimbursement rates may partly be explained by these differences in interpretation, particularly around the grounds for rejecting a claim.[92] The rationales for rejection that firms can use include:

- consumer standard of caution (CSOC);
- claims reported outside the 13-month time limit;
- first-party fraud; and
- a claim being a civil dispute rather than an APP scam.

The application of these rationales requires judgement from firms. In the industry evaluation data, we collected information from PSPs to assess whether there is evidence that these rationales are consistently applied. We explore these below.

We find evidence that there is significant variation of the use of these rationales which will partly explain the divergence we observe between CRM and non-CRM firms' reimbursement rates. Specifically, there are a small number of non-CRMs that significantly diverge from the rest of the market in the proportion of claims rejected in several categories.

The data in the following sections is based on the PSP assessment of the proportion of "in-scope" APP scam claims recorded in Standard A data that has been rejected for reimbursement. Standard A "in-scope" scam claim data is different to the confirmed APP scam values used in Section 7.1 above, but we use it here as it is the appropriate denominator for the analysis of the reasons why claims that are recorded as "in-scope" have been rejected for reimbursement.

91 Based on evidence from stakeholder interviews, the voluntary evaluation PSP survey and the FCA PSP APP Fraud survey.

92 The differences we observe in reimbursement rates will also partly be explained by how claims are triaged and recorded. Some firms will record all potential claims they receive (e.g. through an online portal) while others may not record claims that are deemed ineligible for consideration (e.g. due to timing or definitions).

CSOC

The CSOC is the standard of caution expected from consumers when sending payments. Reimbursement is not required where the consumer has, because of gross negligence, failed to meet at least one of the following standards.[93]

- Consider warnings: consumers must consider any clear warnings or interventions that indicate the payment is likely a scam
- Report to PSP promptly: consumers must report the suspected scam to the PSP as soon as they are aware of it, and within 13 months of the last fraudulent payment.
- Respond to PSP requests: consumers must cooperate by responding to reasonable requests for information from their PSP to help it assess their claim.
- Report to police if required: after making a claim, consumers must consent to their bank reporting the details to the police on their behalf or report it themselves if asked.

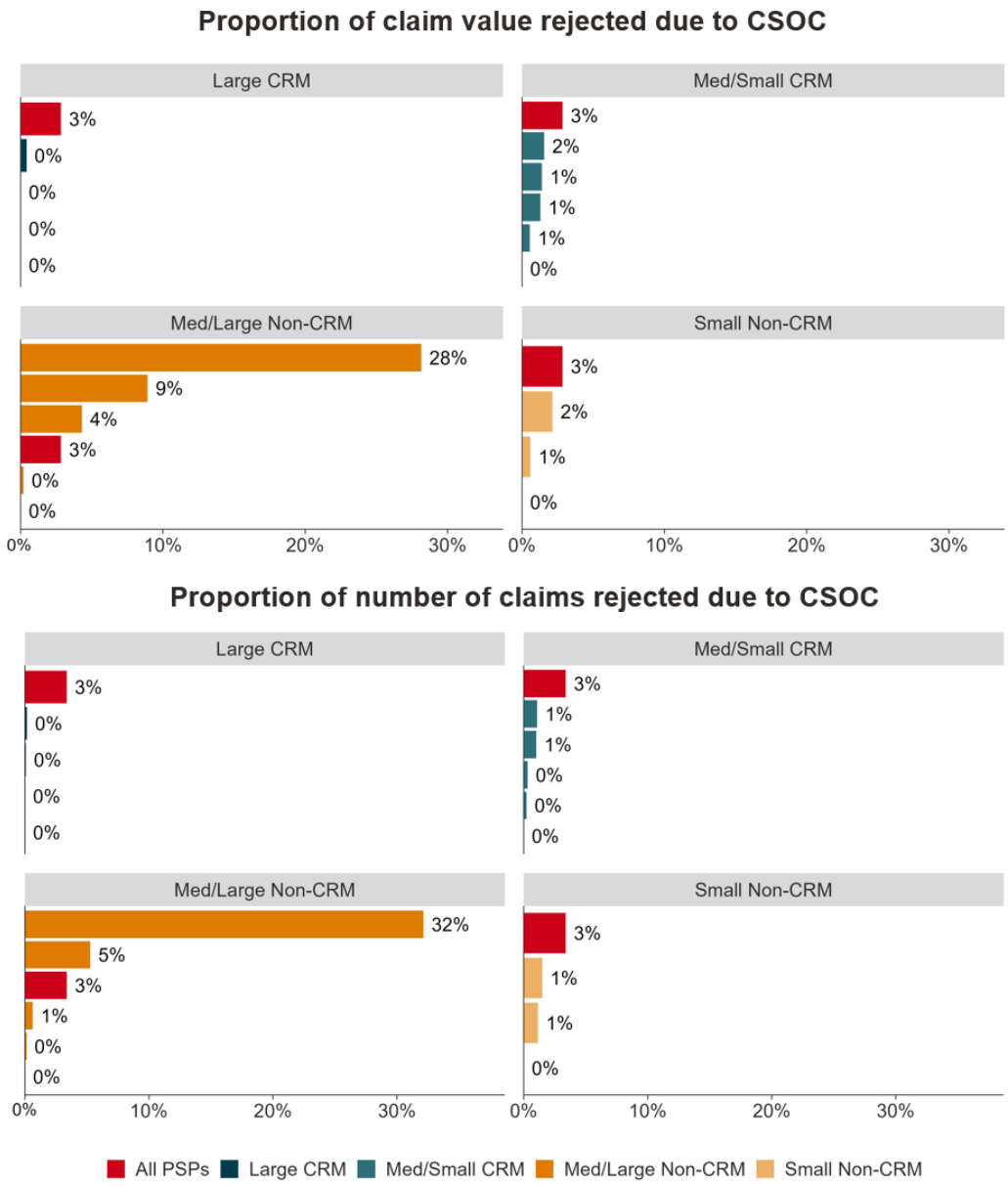
As Figure 34 shows, on average 3% of in-scope scam claims market wide have been rejected due to failure to meet CSOC since October 2024.

However, firms take very different approaches to how CSOC is applied. We can observe that:

- One non-CRM firm applies it to 28% of claims by value and 32% of cases by volume.
- Most larger firms (CRM or otherwise) do not apply CSOC or only for a small number of cases (<1%).
- Among small firms, CRMs and non-CRM firms apply the CSOC exception at broadly similar rates (1-2%).

93 PSR (2023) Specific Requirement 1: Faster Payments APP Scam Reimbursement Rules. The Consumer Standard of Caution Exception

Figure 34 Standard A in-scope claims rejected due to CSOC



Source: *Frontier analysis of Standard A and industry evaluation data*
Note: *Data for Oct 2024 - Sep 2025.*

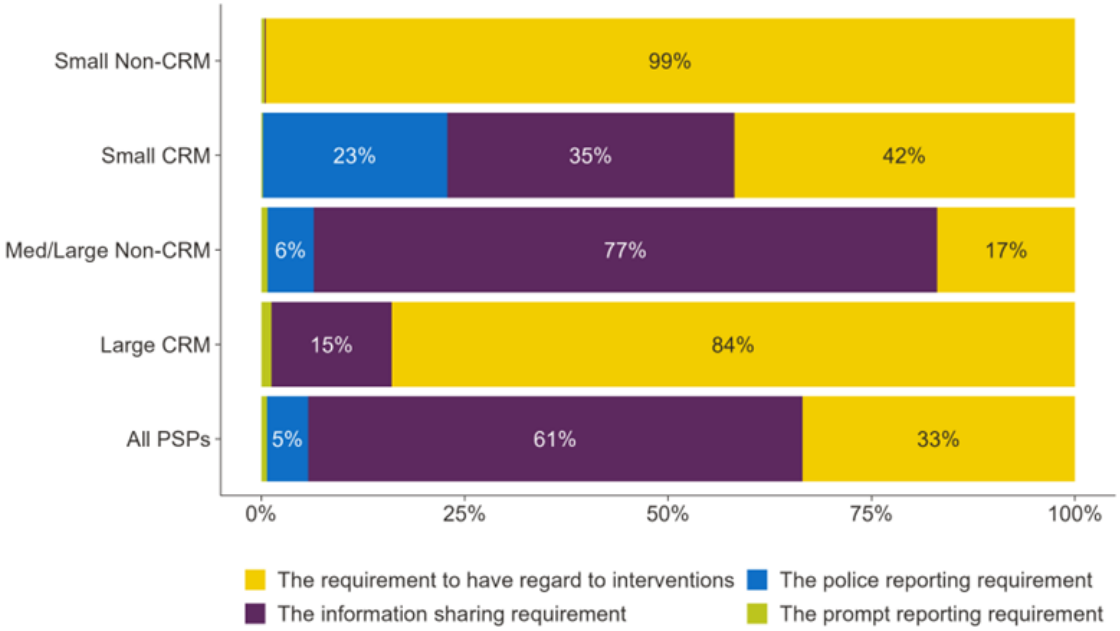
Some PSPs have suggested that the reason they do not apply CSOC is that the standard of caution required from consumers is too high for it to apply in any case. One CRM PSP noted in their FCA-PSR Joint Survey response:

> *"Since the reimbursement requirement came into effect, we have not declined any claims under CSOC, which reflects the extremely high threshold set for PSPs to apply the gross negligence exception. As currently designed, only one of the four criteria for declining a claim under CSOC focusses on actions the customer must take as part of the payment (having regard to interventions)."*

For those firms applying CSOC, the main reason for rejection is the information sharing requirement – that is, consumers must cooperate by responding to reasonable requests for information from their PSP to help it assess their claim. There are, however, significant differences between different types of firms. This is shown in Figure 35 below.

- Large CRM and small non-CRM firms are much more likely to reject claims due to the requirement to have regard to interventions.
- Medium and large non-CRM firms reject claims due to the information sharing requirement more than other groups.
- Small CRM firms reject a relatively greater proportion of claims due to the police reporting requirement.

Figure 35 Proportion of claims rejected due to each CSOC criteria



Source: *Frontier analysis of industry evaluation data*
Note: *Data from 12 PSPs. Data for Oct 2024 - Sep 2025.*

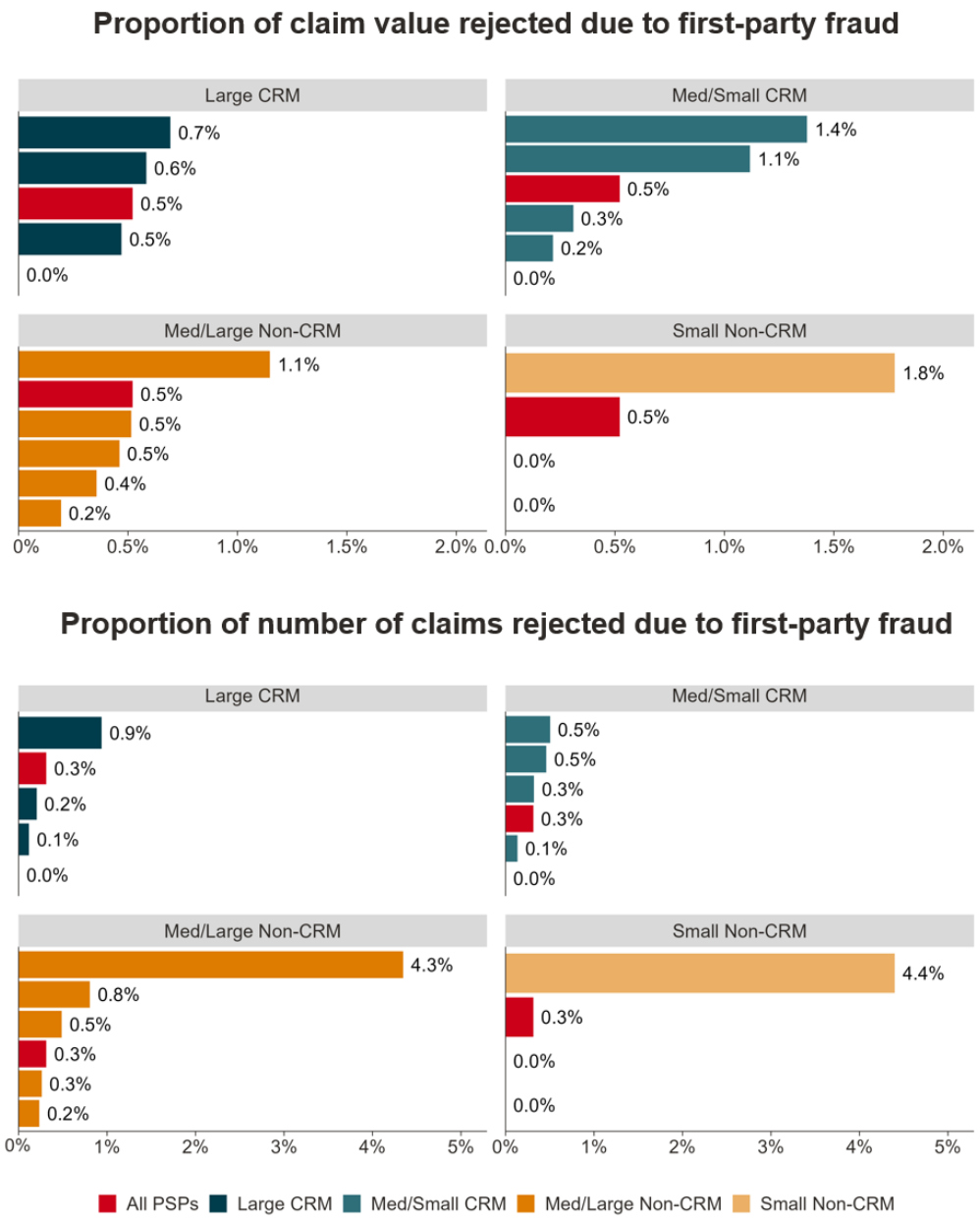
First-party fraud

There is also considerable variation in the proportion of in-scope claims that are rejected due to first-party fraud, as shown in Figure 36. While most PSPs reject few claims on this basis, a small number reject a significantly higher proportion. In particular:

- Four non-CRM and two small CRM firms reject more than 1% of claim value (and up to 1.8%) compared to a market average of 0.5%.
- Smaller firms (both CRM and non-CRM) reject on average more claims by value than larger firms.

- Two non-CRM firms reject over 4% of cases due to first-party fraud, compared to fewer than 0.9% for the rest of the market.

Figure 36 Standard A in-scope claims rejected due to first-party fraud

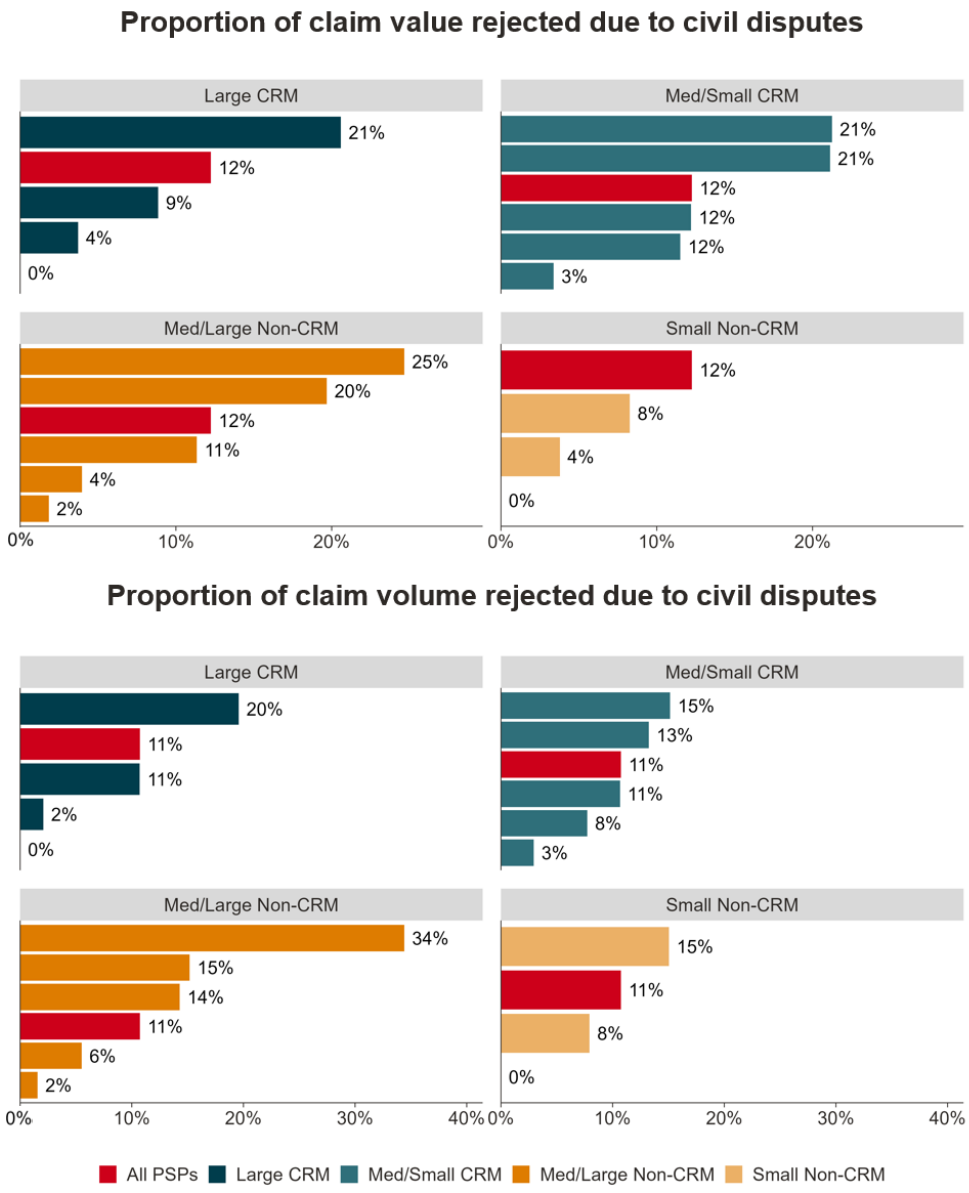


Source: *Frontier analysis of Standard A and industry evaluation data*
Note: *Data for Oct 2024 - Sep 2025.*

Civil disputes

Figure 36 shows that there is also significant variation between PSPs in terms of how many claims are rejected due to being civil disputes.

Figure 37 Standard A in-scope claims rejected due to being classed as a civil dispute



Source: *Frontier analysis of Standard A and industry evaluation data*
Note: *Data for Oct 2024 - Sep 2025.*

There are some firms in both the CRM and non-CRM group that reject over 10 times more claims due to civil disputes than the firms with the lowest level of rejections for this reason. Five firms reject 20% of in-scope claims by value as civil disputes, while others only reject 2% or less. In terms of number of cases, there are both CRM and non-CRM firms that reject over 10% of all in-scope claims as civil disputes, while others reject 1% or fewer cases.

This suggests that firms may be taking different approaches to interpreting what constitutes a civil dispute versus an APP scam. These differences do not appear to be driven by size or CRM status.

We note that these differences may at least partly be explained by the process used by different firms to triage claims. Claims that can be easily assessed as a civil dispute over an initial telephone call when the claim is raised may be excluded from APP scam records by the PSPs that use call centres for triage, but not by PSPs that use an online form.

However, several stakeholders also highlighted that there is a significant number of cases that fall on the border between civil disputes and APP scams. Some PSPs reported that consumers are raising APP scam claims for transactions that the PSP would classify as a civil dispute. At the same time, other organisations felt that too many cases are rejected due to being classified as civil disputes. An organisation involved in preventing fraud reported:

> *"We have seen quite a lot of cases… where the sending bank has decided that something [is a] civil dispute when it's clearly not from our perspective… Even though the guidance is quite good."*

Me-to-me and crypto cases

Payments between two accounts held by the consumer are not in scope of the reimbursement requirement, except for cases where the consumer is not in control of the receiving account. Stakeholders reported that firms can take different views on what it means for a customer to be "in control" of an account, leading to different outcomes in similar cases.

This issue often arises where funds are transferred to a crypto or trading account in the customer's own name. In interviews, some PSPs argued that these cases should be treated as out-of-scope because the payment is made from the customer's account to another account also held by the customer:

> *"Banks not recognising that me to me is out-of-scope… The payer has used their own bank account to pay their own trading account… That's sent through to us as an APP scam. It's me to me, so that's definitely out-of-scope."*

Other interviewees highlighted that customers may argue they were not genuinely in control of the receiving account, particularly where they were manipulated by a fraudster during the scam:

> *"Our customers [say] they were not in control… but the crypto firms [are] adamant that they were in control."*

Some PSPs also described cases where claims were rejected due to the receiving firm being a crypto exchange and out-of-scope for reimbursement, but the decision being overturned by FOS.[94] One firm responding to the FCA-PSR Joint Survey stated:

> *"The bank has seen evidence of FOS finding in favour of the customer in these claims, despite APPR being clear that we held no liability for the customer's loss."*

This creates uncertainty for firms and consumers. Similar claims may be assessed differently depending on how the relevant PSP interprets whether the customer was in control of the receiving account. It may also influence firms' wider risk controls, with some PSPs introducing restrictions on payments to cryptocurrency firms in response to fraud and reimbursement risks.

7.2.3 Uncertainty over in-scope firms may be contributing to inconsistent treatment of claims

Several firms have also raised concerns that some PSPs may be interpreting the scope of the reimbursement requirement differently, with some firms appearing to treat themselves as outside the regime. Stakeholders said this issue is particularly relevant to indirect participants that rely on sponsor banks for access to FPS, where it may be less clear in practice which entity is responsible for handling and contributing to reimbursement claims.

As set out in Section 2, the PSR defines firms as in scope where they participate in FPS, directly or indirectly, and provide relevant accounts. The PSR also states that there are no exemptions based on business or firm type. However, it notes that firms are responsible for determining their own legal obligations and that its list of participants is not guaranteed to be complete.[95] This leaves some scope for uncertainty in practice, particularly where firms access FPS indirectly.

This concern was reflected in the FCA-PSR Joint Survey, where four firms raised concerns about firms interpreting the scope of the reimbursement requirement differently or treating themselves as outside the regime. One non-CRM firm argued that this complexity had *"allowed firms that introduce risk, particularly remittance and cryptocurrency firms, to deem themselves outside the policy's scope."*

In a follow-up after an interview, one industry organisation suggested that this uncertainty may arise because the PSR's legal instruments and Pay.UK's reimbursement rules do not map neatly onto one another in all cases. It noted that this can create practical uncertainty over whether responsibility sits with the customer-facing PSP, the sponsor bank, or another entity in the payment chain. The organisation said this could result in different interpretations of

[94] Though we note that FOS decisions are not based on purely APPR rules, but also take into account the relevant law and regulations, regulator's rules, guidance and standards, codes of practice and – where appropriate – good industry practice that applied at the time of the event.

[95] PSR (2024). Faster Payments (FPS) participants (June 2024).

whether a firm is captured by the reimbursement requirement and where liability sits. As the industry organisation put it:

> *"As a result, indirect participants may face genuine uncertainty about whether they are captured, and this is exactly why you may see inconsistent industry behaviour and feedback in relation to APPR."*

This uncertainty can affect consumers where a receiving firm says it is outside the regime. In those cases, sending PSPs may respond differently. Some may reimburse the customer in full and absorb the cost, while others may reject the claim or dispute liability. As a result, consumers with similar APP fraud claims may receive different outcomes depending on which firms are involved and how those firms interpret the scope of the regime. In some cases, this only becomes clear after a claim has been raised and the receiving PSP tells the sending PSP that it considers itself out-of-scope.

Due to inconsistency in how the rules are interpreted, stakeholders raised examples of situations where cases could face different outcomes depending on the PSP that is assessing the claim, or sometimes even depending on the part of the PSP that is interpreting the rules.

Consumer organisations noted that consumer outcomes can differ depending on the part of the organisation that the victim's case is handled by within the same PSP.

- One consumer group described two cases with similar facts: *"Bank A refunded within five days, and Bank B has flatly refused… The facts of the case are the same… PSPs have applied the rules differently."*
- A consumer organisation noted: *"It's then gone to another department within that bank, and the decision's been overturned."*

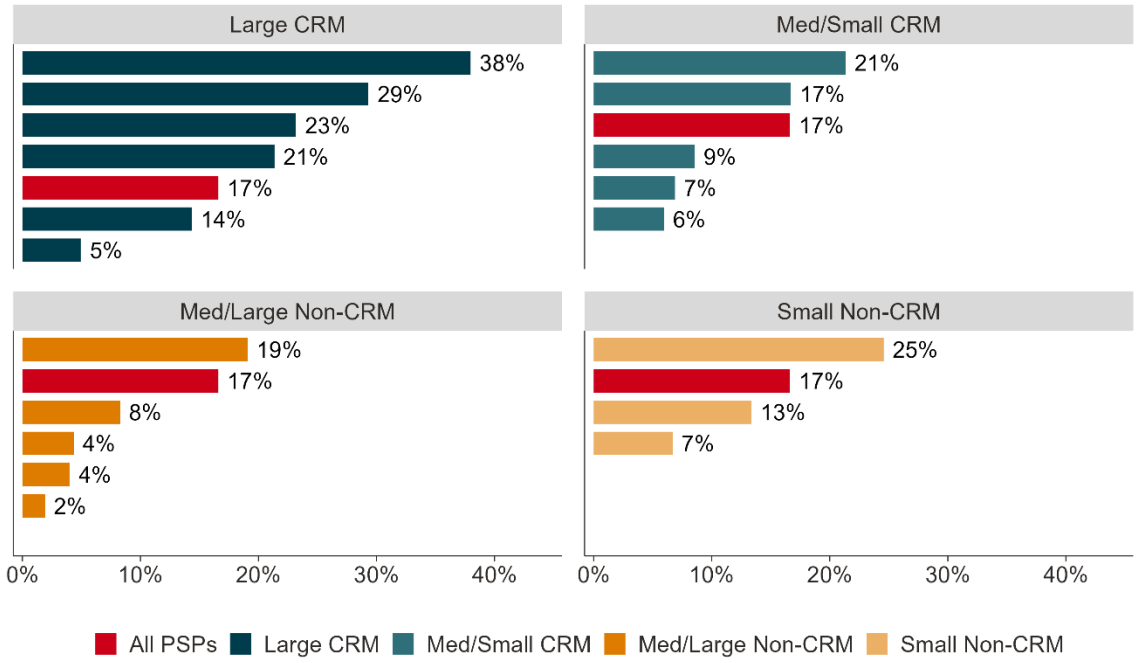
7.2.4 Large CRM firms tend to class more of their APP fraud victims as vulnerable than other firms

The consumer standard of caution and claim excess cannot be applied to vulnerable consumers, where this had a material impact on their ability to protect themselves from the scam. Across our sample, 17% of claims were made by vulnerable consumers.

There are differences between PSPs in how many consumers they identify as vulnerable. As shown in Figure 38 below, the proportion of claims made by vulnerable consumers ranges from 38% to just 2% between PSPs. Large CRM PSPs generally identify a higher share of victims as vulnerable than other firms.

Differences in the proportions of victims classed as vulnerable may reflect differences in the customer base between different firms. However, it may also reflect differences in how firms interpret and apply the FCA's definition of vulnerability.

Figure 38 Proportion of claims that are made by vulnerable consumers



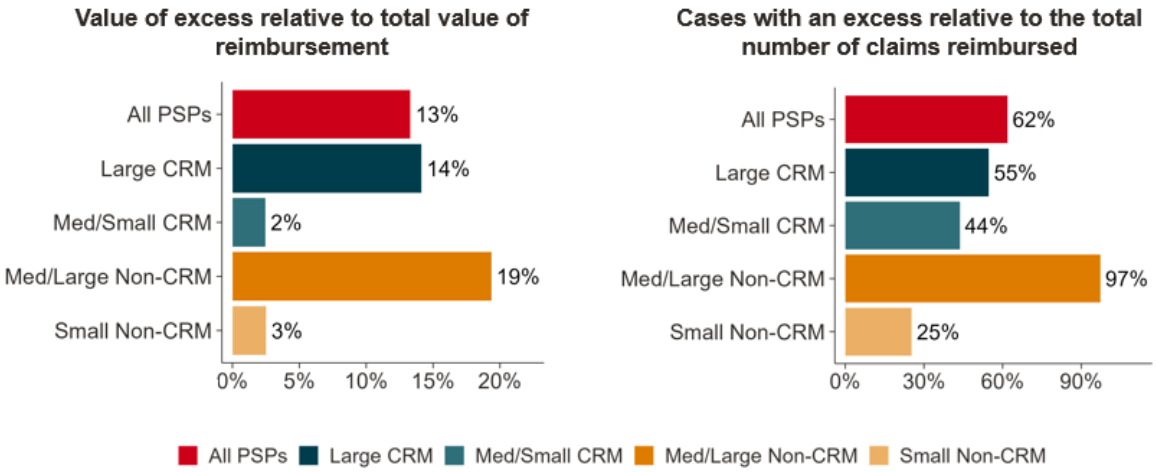
Source: *Frontier analysis of Standard A and industry evaluation data*
Note: *Data for Oct 2024 - Sep 2025. Claims measured as the number of in-scope claims from Standard A data.*

7.2.5 Non-CRM firms apply an excess more frequently than CRM firms

Even where claims are assessed as reimbursable, consumers may receive different reimbursement outcomes depending on whether their PSP applies the voluntary excess. The reimbursement requirement allows firms to apply a voluntary excess of up to £100 on all claims made by consumers that have not been identified as vulnerable.

PSPs have taken different approaches to applying the excess: it is used by 9 out of 10 non-CRM firms that data is available for, compared to 5 out of 11 CRM firms. Firms generally apply it to all eligible customer claims, leading to an excess being applied to 93% of all non-CRM firm claims, compared to just 53% of all CRM firm claims. Differences across groups of firms by size and whether they were a CRM signatory is shown in Figure 39 below. Part of this difference will be choice of the PSP but also variation in vulnerability assessments noted above.

Figure 39 Proportion of APP fraud claims where an excess has been applied



Source: *Frontier analysis of Standard A and industry evaluation data*
Note: *Data from 19 PSPs. Data for Oct 2024 - Sep 2025*

7.2.6 CRM firms are more likely to offer reimbursement above the maximum cap

The reimbursement requirement only mandates that PSPs reimburse consumers up to a cap of £85,000 per APP scam claim. Consumers with higher-value claims may receive different reimbursement outcomes depending on whether their PSP voluntarily chooses to reimburse losses above this mandatory cap.

Between October 2024 and September 2025, firms in our Industry evaluation data sample received 108 reimbursable APP fraud claims that exceeded the maximum reimbursement cap of £85,000. This means that reimbursable claims that exceeded the maximum reimbursement cap accounted for 0.07% of all reimbursable claims.[96] This is within the PSR expectations that the "maximum limit of £85,000 would cover over 99% of APP scam claims."[97]

The total claim value for claims that exceed the max cap was £17.4m. Of this, £9.2m fell within the £85,000 maximum cap and therefore had to be reimbursed, while the remaining £8.2m relates to claim values above the cap. This means that APP fraud losses above the maximum reimbursement cap but otherwise reimbursable accounted for 4.7% of total reimbursable APP

[96] Standard A data shows that, across our Industry evaluation data sample, 156,982 claims were reimbursed between October 2024 and September 2025.

[97] This is within the PSR expectations that the "maximum limit of £85,000 would cover over 99% of APP scam claims." PSR (2024) PS24/7 CBA.

fraud losses.[98] This is within the PSR expectations that the "maximum limit of £85,000 would… protect consumers from around 90% of APP fraud losses".[99]

Some PSPs have chosen to voluntarily reimburse some consumers for claims values above the max cap. In total, of the £8.2m total claim value above the maximum cap, £2.9m, or 36%, has been reimbursed on a voluntary basis. £5.3m, or 65%, has not been reimbursed.

The maximum reimbursement liability was originally proposed to be £415,000, in line with the FOS award limit, but was reduced to £85,000 following consultation in September 2024.[100, 101] Of the £5.3m not voluntarily reimbursed on claims above £85,000, £4.9m was on claims under the once proposed £415,000 limit and so would have been reimbursed had the reimbursement requirement policy been implemented with that higher limit.[102] This £4.9m is significantly lower than the £30m annual reduction in mandatory reimbursement coverage estimated in the PSR's 2024 cost benefit analysis when the maximum reimbursement level was reduced from £415,000 to £85,000.[103]

As noted previously in this report, data collected up to November 2025 is unlikely to fully capture investment APP scams that have occurred since October 2024, given the long reporting lags associated with this scam type. These scams are typically higher value, and may be more likely to exceed the max cap. That caveat aside, in the first year of the policy, consumer protection does not appear to have been meaningfully lessened by the £85,000 maximum cap on reimbursable claims: more than 99% of reimbursable APP scam claims and more than 95% of reimbursable APP scam value is covered under the cap. Furthermore, the impact on consumers of the lower cap than originally planned has been smaller than previously estimated.

Figure 40 shows how voluntary reimbursement has varied across PSPs. CRM firms have reimbursed, on average, 37% of claim values above the cap. However, reimbursement behaviour varies considerably across firms, with some CRM firms reimbursing almost all above-cap claim value and others providing no voluntary reimbursement. Among non-CRM firms, one firm reimbursed 62% of above-cap claim value, while two have provided no voluntary reimbursement.

[98] Standard A data shows that, across our Industry evaluation data sample, £167m claims were reimbursed between October 2024 and September 2025.

[99] This is within the PSR expectations that the "maximum limit of £85,000 would… protect consumers from around 90% of APP fraud losses". PSR (2024). PS24/7 CBA.

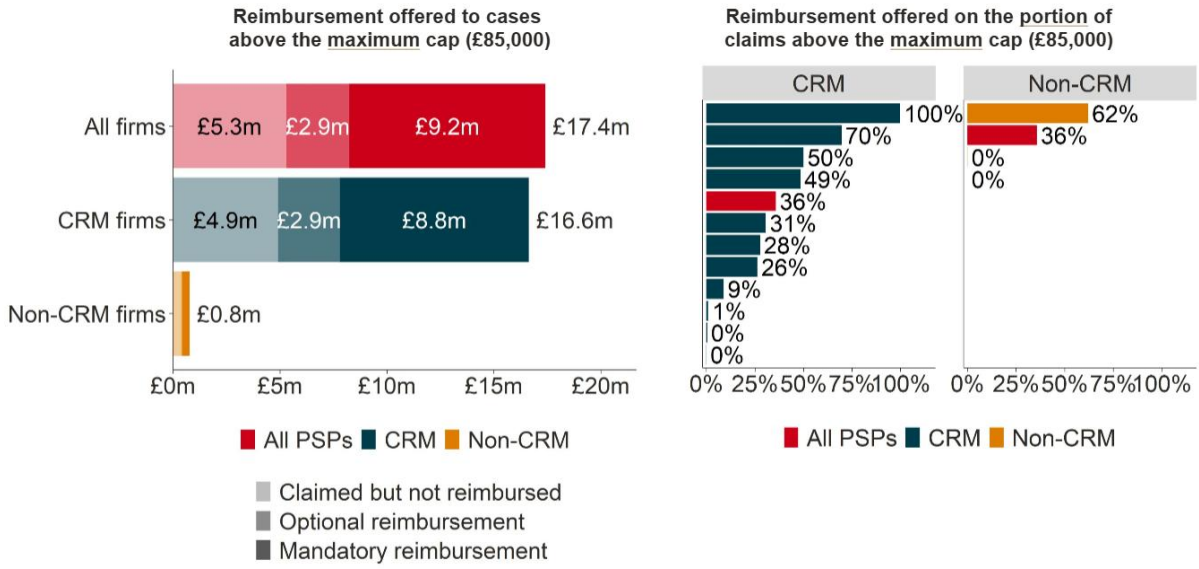
[100] PSR (2024). PS24/7.

[101] At the time, this was aligned with the FSCS deposit protection limit, although the FSCS limit has since increased to £120,000 from 1 December 2025. PRA (2025) PS24/25 – Depositor protection

[102] The remaining £0.4m claimed but not reimbursed was on the portion of claims over the once proposed £415,000 limit and so would not have been reimbursed even under that higher limit.

[103] PSR (2024). PS24/7 CBA

Figure 40 Reimbursement offered on claims above the maximum cap



Source: Frontier analysis of industry evaluation data

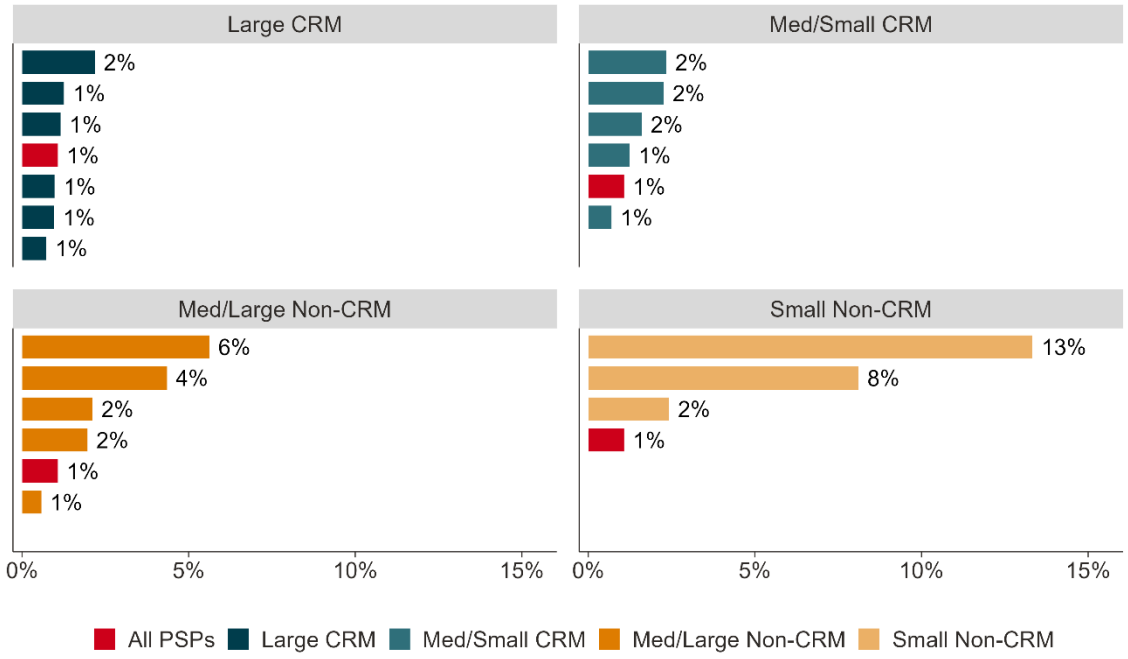
Note: Data for Oct 2024 - Sep 2025. In the LHS graph, on claims above the £85,000 limit to non-CRM firms, £0.34m has been reimbursed mandatorily, £0.05m of optional reimbursement, while a further £0.38m has been claimed but not reimbursed.

7.2.7 Some non-CRM firms face more customer complaints than CRM firms

Complaint rates are a useful indicator of whether consumers accept firms' reimbursement decisions and how consistently claims are being handled. Consumers that are not satisfied with the decision in their claim can raise a complaint with the FOS. Most firms in our sample face between 1 and 2 customer complaints per 100 reimbursement claims.

There are four non-CRM firms that face a significantly higher proportion of complaints than others: between 4% and 13% of all claims. This may indicate a lack of consistency in customer treatment between different PSPs.

Figure 41 Proportion of customer claims that have resulted in a FOS complaint



Source: *Frontier analysis of industry evaluation data and FOS complaints data.*
Note: *Data for Oct 2024 - Sep 2025. Claims measured as the number of in-scope claims from Standard A data.*

7.2.8 Most cases are resolved within 35 business days

The speed with which claims are resolved is another important aspect of consumer treatment. Delays can leave victims without access to lost funds for longer and prolong uncertainty about whether they will be reimbursed. Under the reimbursement rules, firms are generally expected to assess and reimburse eligible APP scam claims within five business days. However, where additional investigation is required, firms may apply the "stop the clock" provisions, subject to an overall longstop of 35 business days.

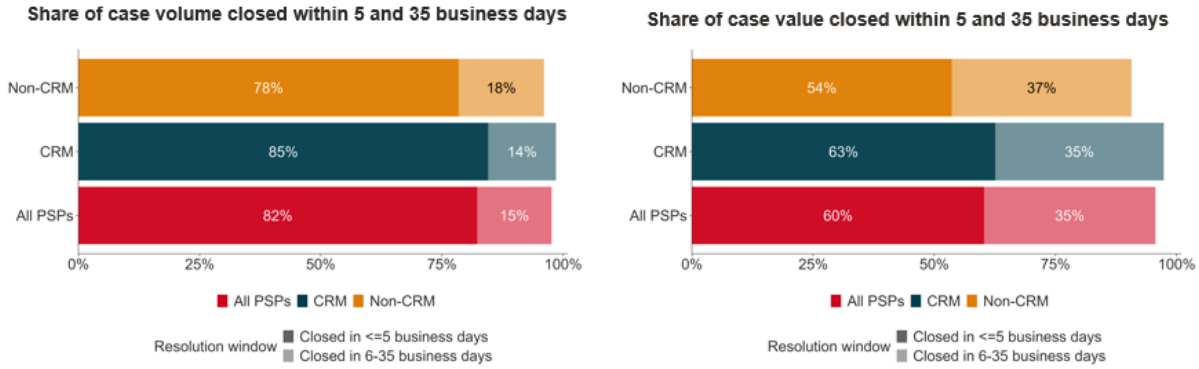
At the market level, 97% of claims by volume have been closed within the 35-business day statutory deadline, with 78% closed within five business days. CRM firms have achieved a slightly higher closure rate, with 99% of claims closed within 35 business days, compared with 96% for non-CRM firms.

A similar pattern is observed when considering claim value. Across the market, 95% of claim value has been closed within the 35-business day deadline, while 60% has been closed within five business days. CRM firms again achieve a higher closure rate, closing 98% of claim value within 35 business days, compared with 91% for non-CRM firms.

The lower closure rate by value than by volume suggests that a small number of higher-value claims have taken longer to resolve. This may reflect the greater complexity of larger claims,

which are more likely to require additional investigation before a reimbursement decision can be reached.

Figure 42 Share of cases closed within 5 and 35 business days



Source: Data from 19 PSPs. Frontier analysis of Standard A data

7.3 How has the change in the level of APP fraud impacted consumers?

This section assesses how changes in the level of APP fraud have affected consumers. Prevented APP scams reduce financial losses and avoid the emotional harm that victims can experience even where they are reimbursed.

The evidence suggests that:

- consumers have benefited financially from the reduction in APP fraud, because some of the avoided losses would not otherwise have been reimbursed;
- the reduction in APP fraud has also generated non-financial benefits, as fewer consumers experience the distress, loss of trust and anxiety associated with being scammed;
- these consumer benefits are difficult to quantify precisely because some scams take longer to report and because emotional harm varies significantly between victims; and
- the benefits may be partly offset if fraud has shifted towards out-of-scope channels, such international payments, where consumer losses and the number of cases have increased.

7.3.1 Consumer financial outcomes have improved due to the reduction in APP fraud value

Consumers have benefited financially from the reduction in the volume of APP fraud described in Section 6.

Losses from APP fraud have fallen by an estimated £73m per year. As set out in section 6.2, 54% of these losses were reimbursed by PSPs prior to the reimbursement requirement. Consumer financial outcomes from reduced levels of fraud have therefore improved by the proportion of these losses that would not have been reimbursed by their PSP: £34m/year. The

remainder of the benefit from reduction in fraud – £39m/year – is attributable to PSPs as they would have funded these costs through reimbursement.

The estimate of consumer financial benefits from changed APP fraud rates will also be affected by changes in fraud that are harder to quantify and attribute to the policies.

- As set out in Section 6.1, benefits from a reduction in scams that take more than 6 months to report are not quantified in the £73m overall APP fraud reduction because data on these scams is not yet available. However, if the scams that take longer to report have fallen to the same extent as other scams, the overall reduction in APP scam value is estimated to be £91m/year. Given the reimbursement rate above, consumer benefits from reduced APP scams increase to £42m/year if these scams are included in the assessment.
- As Section 6.3 shows, annual losses from out-of-scope international APP scams increased by £39m between 2023 and 2025. These increases are not directly attributable to the policy, but qualitative evidence from stakeholders indicates that fraudsters may be switching away from in-scope scams towards alternatives that are perceived to involve fewer controls and lower risk (see Section 6.4). Some stakeholders also noted that investments in tackling in-scope APP fraud had led them to deprioritise investment in tackling other frauds (see Section 6.4). Consumers would suffer financial harm from these scams that would partially offset the benefits from reduced APP scams.

7.3.2 There has been an improvement in non-financial consumer outcomes from prevented scams

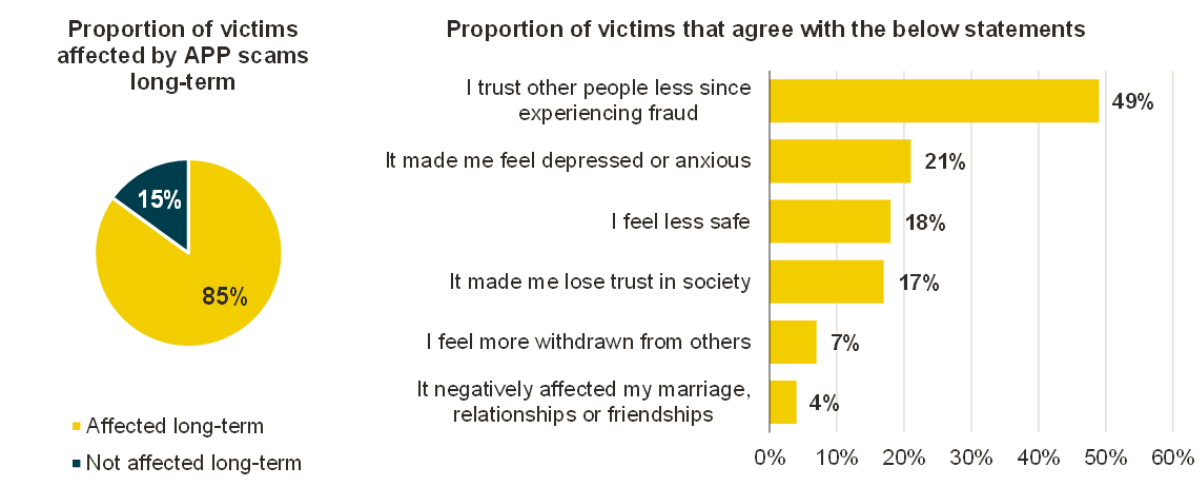
Preventing APP scams can improve consumer outcomes even where victims would otherwise have been reimbursed. Being a victim of an APP scam has not only a financial impact, but also an emotional one. APP scam victims often suffer emotional harm, and reimbursement does not remove it.

In interviews, stakeholders reported that despite being reimbursed, victims continue to experience shame, distress, self-doubt, and vulnerability, particularly in romance and investment scams.

> *"You still may question yourself, you still may then feel vulnerable and that's nothing to do with the policy." – CRM firm*

Evidence from the PSR APP Fraud Consumer Survey presented in Figure 43 below shows that a significant proportion of scam victims experience significant emotional distress. Overall, only 15% of victims stated that being scammed did not affect them long-term. 49% of scam victims reported trusting other people less, 21% of victims felt depressed or anxious and 18% of victims felt less safe.

Figure 43 Proportion of APP scam victims that suffered emotional harm



Source: Frontier analysis of PSR APP Fraud Consumer Survey

Interviewees also highlighted that the reimbursement process can also cause emotional distress to some victims due to secondary victimisation and delays.

- **Risk of secondary victimisation.** Consumer groups and PSPs raised concerns about how some victims are treated during claims processes, particularly in complex or rejected claims.

  > *"She was treated as if she was a criminal … from her perspective, the bank treated her worse than the criminal did…* They're being asked for huge amounts of information when the level of stress and emotional distress will be extremely high." - *Wider stakeholder*

- **Delays in communication can prolong harm.** Stakeholders also raised concerns about consumers whose cases took longer than the 35-day limit. These victims sometimes did not receive sufficient updates, prolonging their distress.

There can be significant consumer benefits if the number of APP fraud cases is reduced and the emotional harm described above is avoided. The scale of these benefits is difficult to quantify. The scale of loss, whether the victim was reimbursed, how they were treated in the process and their level of vulnerability will all contribute to the scale of emotional harm the victim suffers after falling victim to an APP scam. All these factors will therefore contribute to how much consumer welfare increases when more APP scams are prevented.

We use the evidence on changes in the number of fraud transactions from Section 6.1 above and the evidence from the PSR APP Fraud Consumer Survey presented earlier in this section to illustrate the potential scale of these benefits.

As shown in section 6.1 above, the average number of APP scams per month has fallen from 23,300 before the policy to 20,400 after it.[104] This is a reduction of approximately 34,800 scams per year.

If 85% of victims experience long-term impacts after an APP scam, this reduction in scam cases could mean around 29,600 fewer people experiencing long-term impacts each year. Applying the findings illustratively to the PSR APP Fraud Consumer Survey results, this could include around 17,000 fewer people losing trust in others and around 7,300 fewer people experiencing anxiety or depression.

As with the financial benefits from reduced APP fraud value discussed in Section 7.3.1, these non-financial benefits need to be considered alongside changes in out-of-scope scams.

- If we assume that the 15% of APP scams that take longer than 6 months to report and are not included in this analysis (because the data on these impacts is not yet available) have fallen at the same rate as other scams, the total reduction in the number of APP scam cases rises from 34,800 to around 40,000. The non-financial benefits from prevented scams would be greater under this assumption.

- At the same time, the number of consumer international APP scams has increased by about 8,700 cases per year, as shown in Section 6.3. These increases may not be fully attributable to the policy, but the evidence presented in Section 6.4 suggests that this increase may at least partially have been driven displacement from the policy. If all the increase in international APP scams were attributable to the policy, some of the non-financial benefits described above would be eroded. This would imply a net reduction of around 31,300 APP scam cases per year.

Overall, we conclude that the reduction in APP scam cases has generated positive non-financial benefits for consumers, although the scale of these benefits is uncertain.

7.4 Have the policies led to increased payment friction for consumers and businesses?

This section assesses whether the policies have increased payment friction for consumers and businesses. Payment friction matters because APP fraud controls can help prevent scams but may also delay or disrupt legitimate payments. The evidence suggests that the policies have increased friction for some consumers and businesses, although this appears to be targeted mainly at higher-risk payments and customers.

[104] This is calculated by multiplying the average monthly number of scam transactions reported in Section 7.1 by the average number of transactions per scam (1.7).

7.4.1 APP fraud controls have increased payment friction

Stakeholder interviews and FCA-PSR Joint Survey responses indicate that APP fraud controls have increased payment friction for some consumers and businesses. In stakeholder interviews, PSPs described introducing more warnings, checks, payment delays, freezes and follow-up questions. Responses to the FCA-PSR Joint Survey similarly referred to strengthened transaction monitoring, real-time interventions, payment pauses, additional verification questions and greater scrutiny of higher-risk payments.

However, the evidence is mainly qualitative. PSPs did not provide comparable data on average transaction times, payment-hold rates, false positive rates or the number of legitimate payments delayed. This means we can identify the types of payment friction that have increased, and where PSPs report they are most concentrated, but we cannot robustly estimate the scale of friction across the market.

Some PSPs described this as a clear source of inconvenience for customers. As one non-CRM PSP stated: "*We've added friction into the send journey… asked you tons more questions, frozen more payments than we've ever frozen before… That's a friction, that's an annoyance, that's a nuisance.*" This was echoed in the FCA-PSR Joint Survey, where one PSP said additional monitoring "*may result in temporary transaction holds or additional customer verification questions that customers may not have previously encountered*."

However, respondents also emphasised that increased friction is often intended to be targeted rather than blanket. As part of our stakeholder interviews, one CRM firm said: "*We're trying to slow it down for them in a way that works instead of being like additional friction unnecessarily, because there's a difference in alerting on a case versus asking the customer to provide you evidence.*"

Responses to the FCA-PSR Joint Survey similarly suggested that some PSPs were using risk-based controls, with one large CRM firm saying it deployed controls "*in a targeted and risk-based manner so as not to create any material impacts on access to our products and services by genuine applicants or customers*." Another noted that "*increased scrutiny is anticipated, particularly for new or large payment / money movements.*"

The evidence suggests this friction is concentrated on higher-risk payments and customers, including crypto, international payments, suspected mule activity and potentially vulnerable consumers.

- For example, in an interview, one non-CRM described: *"We are focusing on vulnerable customers, customers likely to be scammed, because we don't want to create unnecessary frictions for other customers, so we focus on … those not very tech savvy, the elderly with a lot of balance in their account."*
- Another non-CRM PSP set out in the PSP voluntary survey that: *"our focus [has] shifted to cryptocurrency and international payments, taking the step of implementing outbound*

value restrictions. [We had] been resistant to follow other PSPs in placing blunt restrictions on specific payment types, but with a continued increase in the risks associated with these beneficiaries, this was a necessary step."

Several PSPs suggested that friction may be higher in the short term as firms strengthen monitoring, introduce additional interventions and tune new controls, but could reduce over time as models improve and false positives fall. For example, one respondent to the FCA-PSR Joint Survey said: "*Following the policy's implementation, more payments were held, but our resolution speed improved over time and genuine payments being triggered has reduced*."

Despite added friction to the payment journey, respondents reflected that these outbound controls are broadly seen as positive by consumers. Increased friction does not necessarily imply poorer service quality. Some consumer groups and PSPs reported that targeted interventions can build trust and prevent harm. As one CRM signatory put it, *"there's a difference between friction for the sake of it and friction with tangible next steps."* They reflected that:

> *"Some people had made complaints about … friction in their journey ... But…customers have actually gone, oh, hang on a minute, you … have got my best interests at heart here. I can understand why you've intervened."*

Further, FOS reported relatively low complaint volumes about delays.

However, there was particular concern about the impact of these frictions on business customers. One non-CRM PSP noted that business transactions are typically higher value, and delays may disrupt payroll, supply chains, or property transactions. As they observed: "*If you stop them from paying staff, they're not going to be very happy about it… we're stuck between a rock and a hard place."*

7.4.2 In some instances, APP fraud controls have led to increased friction in consumers accessing banking services

APP fraud controls also appear to have increased friction in access to banking services, particularly on the receiving side. PSPs reported freezing accounts suspected of mule activity, closing accounts, applying stricter onboarding controls and increasing monitoring of inbound payments. Responses to the FCA-PSR Joint Survey supported this, with some firms describing enhanced due diligence, behavioural screening, fraud risk scores, CIFAS checks and machine learning models to identify higher-risk applicants or accounts.

These controls can have significant impacts where legitimate customers are incorrectly flagged or where vulnerable customers rely heavily on banking services. One consumer organisation described the indirect harm caused by account freezes and delays: "*Account freezes, and delays create indirect financial and emotional harm, particularly for vulnerable victims… My victim was highly immobile, so she relied a lot on her online banking.*"

There were also concerns about "debanking" risk, where firms face stronger incentives to restrict or close accounts if they cannot distinguish clearly between legitimate and fraudulent activity. However, this was not universal. Several larger PSPs said they did not expect material access impacts because their existing controls were already designed to manage fraud risk. For example, one large CRM firm stated: "*We have not made any material changes to our customer onboarding or monitoring processes… our existing controls and procedures were already designed to support robust customer due diligence and ongoing monitoring.*" We therefore conclude that the debanking risk is limited.

7.5 Have there been any adverse effects on consumer or business usage of FPS and/or Open Banking?

7.5.1 No clear evidence that the reimbursement requirement is impacting FPS usage

Stakeholders reported no clear reduction in Faster Payments usage as a direct result of reimbursement.

Consumer groups reported that good experiences with reimbursement may enhance overall trust in banking. One consumer group reported, *"71% [of victims they supported] said that the new scheme increased their trust in their banks."* However, *"Really, really poor customer experience led them to losing trust in their banks."*

Data from Pay.UK shows that Faster Payments transaction value and volume has continued to grow since the introduction of the reimbursement requirement: the volume of FPS transactions grew by 12% and value by 8% in the first year since October 2024.

7.5.2 Some qualitative evidence suggests that reimbursement requirement may be impacting Open Banking growth

Evidence on the impact of the reimbursement requirement on Open Banking is limited and is largely based on feedback from a small number of interested stakeholders. Open Banking participation has continued to grow. However, some specialist PSPs raised concerns that additional friction has been introduced into Open Banking payment journeys, which may be affecting the pace of adoption. One PSP argued that "*absent these sources of friction and inconsistency, the growth of Open Banking would likely be accelerating at a materially faster rate."*

Stakeholders identified several sources of friction, including additional customer warnings, step-up authentication, payment delays, more cautious transaction monitoring and, in some cases, blocked legitimate payments. One stakeholder provided examples of Open Banking journeys involving multiple authorisation or warning screens, with between six and 16 screens in the customer journey. They raised concerns that repeated warnings could negatively affect

customer sentiment, describing some messages as “scaremongering” where customers are making payments to legitimate merchants.

The same stakeholder also gave an example of a customer being blocked from accessing online banking after making a £13 Pay by Bank transaction, although this may have been an isolated example. They also shared Open Banking conversion data which appeared relatively stable from June 2025. However, they reported that conversion fell by around 10 percentage points after one PSP introduced card reader challenges for customers making Open Banking payments to merchants for the first time.

However, stakeholders were divided on what controls are proportionate for Open Banking payments. One PSP said it struggled “*put in place controls that are as robust for Open Banking payments because some of the key risk indicators that enable these controls are not visible to us.*” This may become more important as Open Banking payments are adopted by larger retailers and used for a wider range of consumer purchases.

Overall, the evidence suggests that the reimbursement requirement may be contributing to friction in some Open Banking journeys, but it is not clear that this has materially slowed overall Open Banking growth to date. This remains an area to monitor as Open Banking payment volumes increase.

8 Theme 4 Findings: Impacts on PSP and other markets

In this theme, we examine how the policies have affected PSPs and the wider market environment. We explore the impact on PSPs' costs, including reimbursement expenses, fraud prevention investment and administration costs, and consider how these costs vary across PSPs and whether they appear manageable. We consider the costs borne by wider stakeholders in the APP fraud ecosystem.

We also consider the early evidence on potential longer-term effects on competition, innovation and service quality in the payments sector, and on economic growth in the wider economy.

8.1 How have the policies affected the costs faced by PSPs?

The policies can affect PSPs through several cost channels. The most direct channel is reimbursement as the mandatory reimbursement requirement increases the share of eligible APP scam losses reimbursed to consumers. PSPs may also face additional operational costs associated with assessing claims, gathering evidence, engaging with counterparty PSPs and managing disputes. At the same time, the policy may create incentives for PSPs to invest in stronger fraud detection, prevention and customer-warning systems. These investments may reduce scam losses over time but often require upfront expenditure. This section considers reimbursement and non-reimbursement costs in turn.

8.1.1 Total reimbursement costs are unchanged since the policy, but the impact is mixed for individual PSPs

Our analysis of reimbursement costs needs to be treated with caution as there are limitations to the Standard A and industry evaluation data on reimbursements, as discussed in section 7.1.

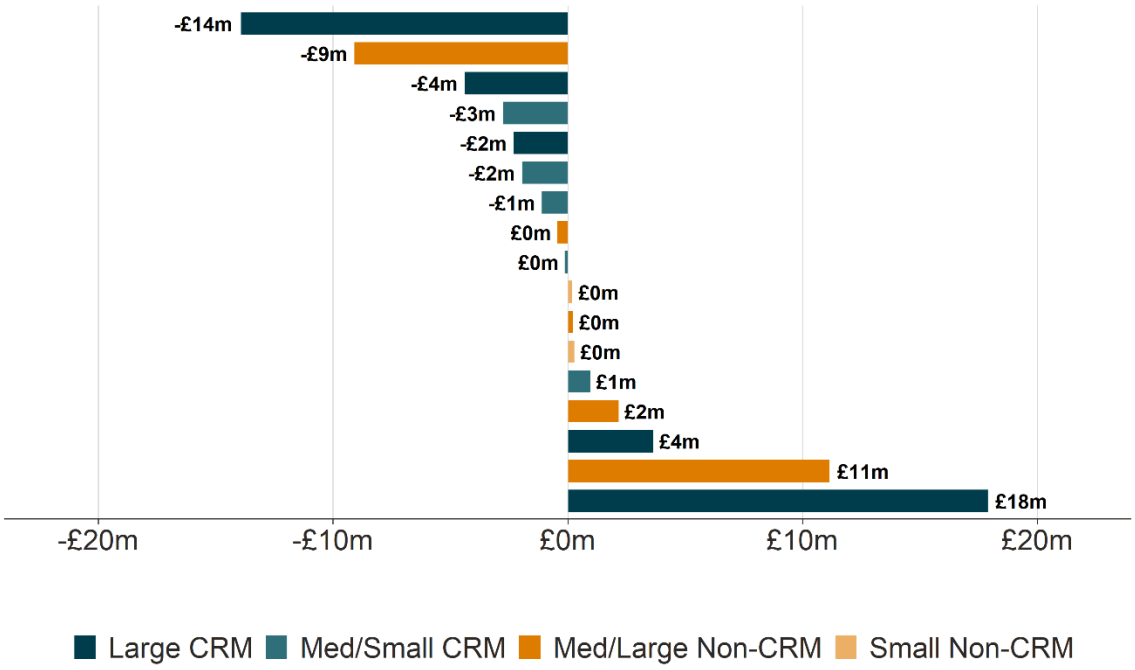
The estimated total annualised reimbursement paid by PSPs market-wide has not changed since the implementation of the reimbursement requirement. Although reimbursement rates increased, the value of APP fraud fell, reducing the pool of losses requiring reimbursement. As shown in Section 8.1, consumer reimbursement which is a cost to PSPs, increased by £39m/year. At the same time, APP fraud fell by £73m as shown in Section 7.1. 54% or £39m of the £73m APP fraud that has been avoided would have been reimbursed to consumers, before the policy. Overall, this reduction in fraud exposure was fully offset by the increase in reimbursement rates leading to zero net impact across the market.

In this section we show how this reduction is broken down between different PSPs. The results should be interpreted as an annualised snapshot of the emerging post-policy position, rather than a settled steady-state estimate.

For half of PSPs, direct reimbursement costs were lower in the post-policy period than in the pre-policy period, and for half of PSPs they were higher. This reflects both changes in reimbursement requirements and changes in underlying APP fraud exposure.

The impact has varied materially across PSPs. As shown in Figure 44, at firm level, the change in annual reimbursement costs ranges from a decrease of £14m to an increase of £18m.[105]

Figure 44 Change in annual reimbursement cost by firm



Source: *Frontier analysis of Standard A and industry evaluation data*

Note: *Change in annual reimbursement costs is calculated as the difference between annualised customer reimbursement in the pre-policy period, April 2023 to December 2023, and the post-policy period, January 2025 to June 2025.*

To understand the drivers of these differences, we have separated the change in annual reimbursement costs between the pre- and post- policy period into two effects:

- changes in fraud exposure, holding reimbursement rates constant; and
- changes in reimbursement rates, holding fraud exposure constant.

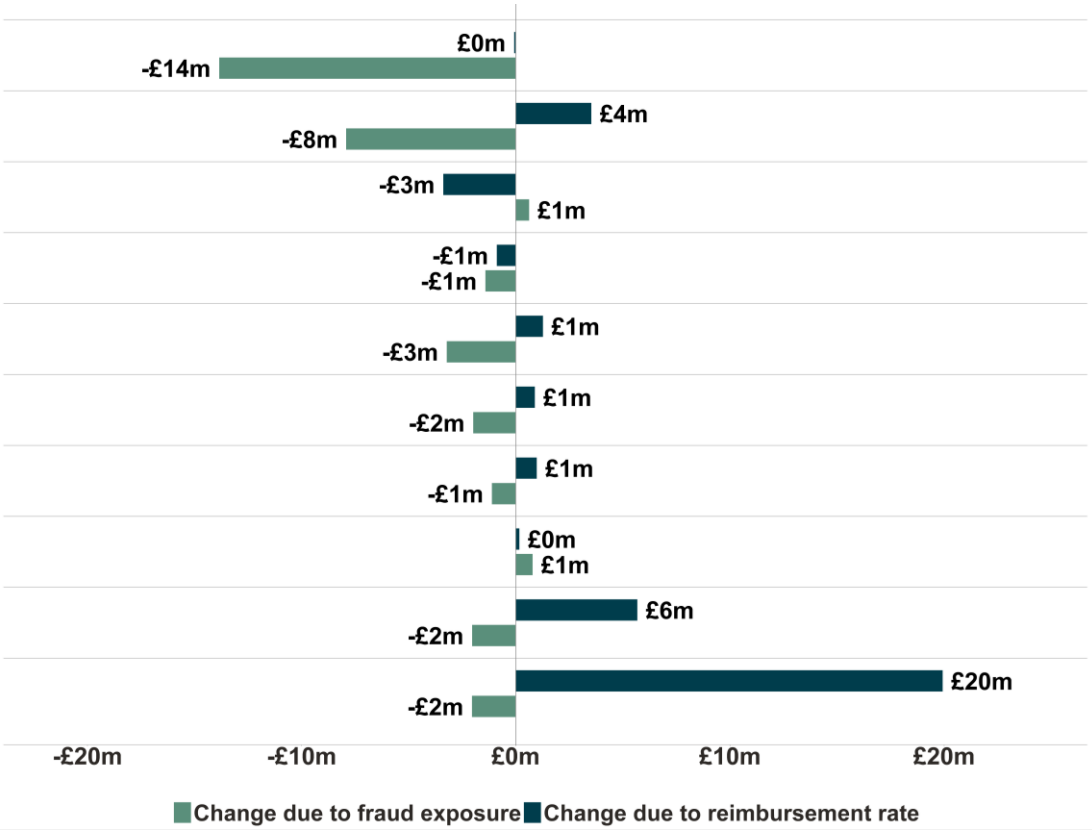
This separation helps distinguish between PSPs whose reimbursement costs changed mainly because the value of APP fraud they sent or received changed, and PSPs whose reimbursement costs changed mainly because a higher share of APP fraud losses were reimbursed.

[105] We use the industry evaluation data for reimbursement values pre-policy and Standard A data for reimbursement values post-policy. We note that Standard A data is reported by sending firm. Firms that have only reimbursed APP scam claims as receiving firms (this includes several non-CRM firms in our sample) do not appear in the data and we are not able to estimate their reimbursement costs post-policy.

Figure 45 and Figure 46 show that changes in fraud exposure and reimbursement rates have affected CRM and non-CRM PSPs differently. The green bars show changes in annual reimbursement due to fraud exposure, while the blue bars show changes due to reimbursement rates. For most CRM firms, lower fraud exposure has reduced reimbursement costs, as shown by the negative green bars. Two firms experienced higher fraud exposure, which increased reimbursement costs.

The impact of changes in reimbursement rates also varies across firms. For some firms, changes in reimbursement rates reduced reimbursement costs, which may reflect cases where they were previously net senders of APP fraud losses and are now able to share liability with other firms. However, this interpretation is not directly shown by the chart and should be treated as a possible explanation rather than a firm conclusion. For several firms, higher reimbursement rates have more than offset reductions in fraud exposure, resulting in an overall increase in annual reimbursement costs.

Figure 45 Change in annualised reimbursement disaggregated between change in fraud and change in reimbursement rate, CRM PSPs



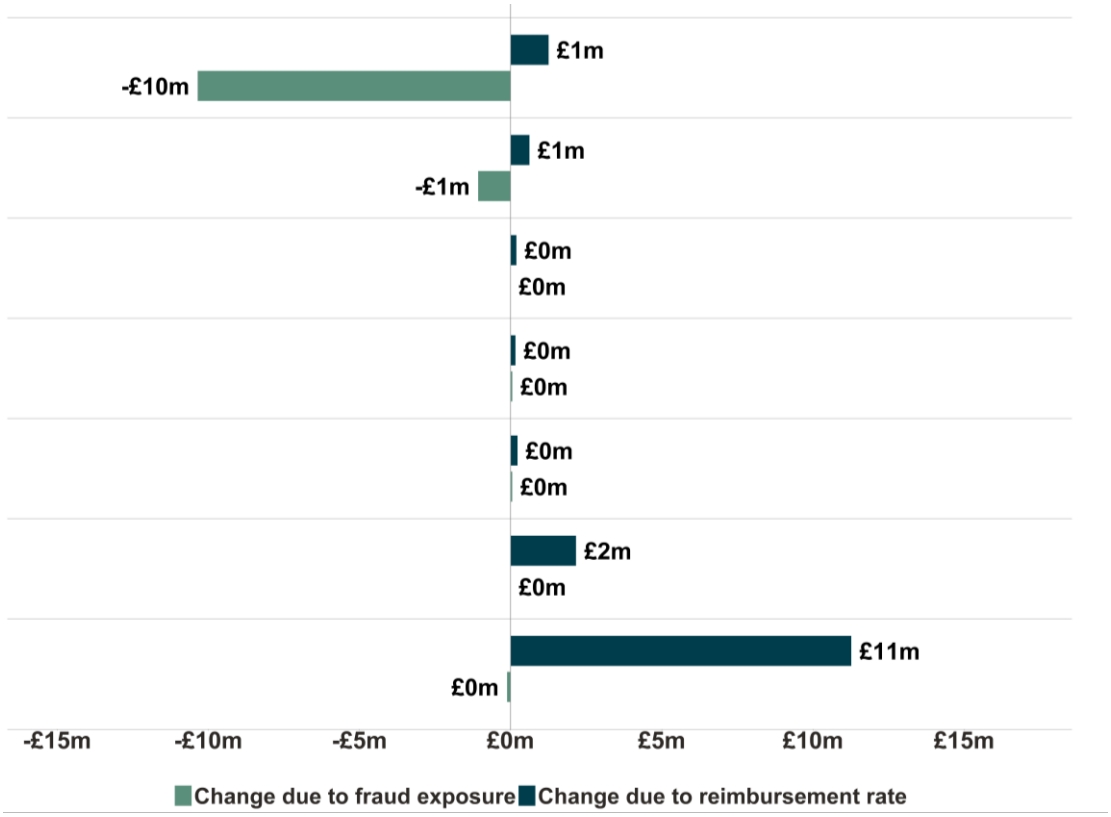
Source: *Frontier analysis of Standard A and industry evaluation data*

Note: *Change due to fraud exposure captures the difference in annualised fraud exposure between the pre-policy period (April 2023 – December 2023) and the post-policy period (January – June 2025), multiplied by the pre-policy reimbursement rate. Change due to reimbursement rate captures the change in reimbursement rate multiplied by post-policy annualised fraud exposure. The pre- and post-policy periods are aligned with the periods used in the analysis of the value of APP fraud over time to account for anticipatory effects in firm actions and reporting lags in APP scam data.*

Among non-CRM firms, the pattern is different. For most non-CRM firms, changes in fraud exposure have only a small effect on reimbursement costs. This is because many of these firms reimbursed little or no APP fraud before the policy, so changes in fraud exposure did not materially affect their modelled reimbursement costs. For these firms, increases in annual reimbursement costs are therefore driven mainly by higher reimbursement rates under mandatory reimbursement.

There is one clear exception. For one non-CRM firm, lower fraud exposure reduced modelled annual reimbursement costs by around £10m. This more than offset the increase due to reimbursement rates, resulting in an overall reduction in annual reimbursement costs of around £9m.

Figure 46 Change in annual reimbursement disaggregated between change in fraud and change in reimbursement rate, Non-CRM PSPs



Source: *Frontier analysis of Standard A and industry evaluation data*

Note: *Change due to fraud exposure captures the difference in annualised fraud exposure between the pre-policy period (April 2023 – December 2023) and the post-policy period (January – June 2025), multiplied by the pre-policy reimbursement rate. Change due to reimbursement rate captures the change in reimbursement rate multiplied by post-policy annualised fraud exposure. The pre- and post-policy periods are aligned with the periods used in the analysis of the value of APP fraud over time to account for anticipatory effects in firm actions and reporting lags in APP scam data.*

For several non-CRM PSPs, overall transaction values and therefore APP scam levels are low compared to other firms in the sample. For three non-CRM firms the reimbursement costs increased but remain low compared to other PSPs and therefore do not appear as a meaningful increase in costs in the chart above.

8.1.2 Non-reimbursement costs have increased

In addition to direct reimbursement costs, PSPs reported increases in a range of non-reimbursement costs following the introduction of the new policies. The evidence in this sub-section is drawn from stakeholder interviews and free-text responses to the voluntary PSP survey. It covers investment in fraud detection and prevention, administrative and dispute-handling costs, and reporting and compliance costs.

Stakeholders consistently reported that these costs had increased. However, PSPs also emphasised that many post-policy investments were extensions or accelerations of existing fraud strategies, rather than entirely new activities. This makes it difficult to isolate precisely the additional costs attributable to the reimbursement requirement and publication of performance data, as distinct from wider fraud, financial crime and regulatory strategy.

Investment in fraud detection and prevention

PSPs reported increased spending on fraud detection and prevention. As set out in Section 5, this included expanding fraud teams, increasing training, hiring specialist analytics capability, investing in enhanced transaction monitoring and additional data sources, and developing new inbound and outbound fraud controls. Several respondents described scam prevention as increasingly labour-intensive, with greater reliance on manual investigation and direct customer engagement alongside automated controls.

However, many PSPs stressed that these investments were broadly aligned with their existing fraud strategies and wider financial crime obligations, including AML requirements, rather than being driven solely by the new APP fraud policies. Consumer groups also acknowledged that PSPs are facing higher fraud prevention costs alongside wider regulatory expectations.

Administrative and dispute-handling costs

PSPs also described significant increases in administrative, reconciliation and dispute-handling costs. These costs relate to the operational work required to assess claims, coordinate with other PSPs, manage reimbursement contributions and resolve disputes. While some of this work is undertaken by fraud teams, it is distinct from activity aimed at detecting or preventing fraud before it occurs. These costs appear to have been particularly material for PSPs that were not previously participating in the voluntary CRM framework, as these firms had to invest in claims-handling infrastructure to comply with the mandatory reimbursement requirement.

APP fraud claims were widely described as more resource-intensive than other scam or fraud case types.

> *"APP Fraud claims… take much longer to work than what a standard scam case would."* – CRM firm

A major cost driver identified by stakeholders was the absence of a single standardised case management system across PSPs. Large banks primarily use BPS, operated by UK Finance, but they also need to use RCMS, operated by Pay.UK, to coordinate with PSPs that are not on BPS. Stakeholders noted that joining case management systems can involve additional fees, which may deter some smaller PSPs. As a result, smaller firms may only be signed up to RCMS or may continue to handle claims by email.

Stakeholders described this fragmented operating model as inefficient and operationally burdensome, as firms may need to manage the same or related claims across multiple systems and communication channels.

> *"We receive some reports via e-mail, some via BPS, some PSPs use RCMS, some don't."* – Non-CRM firm

PSPs also identified additional work associated with reimbursement contribution disputes, reconciliation errors and chasing payments from other firms. Some respondents described delays or disputes in contribution payments as creating substantial extra workload:

> *"We're having to dedicate resource to chase it through and then escalate to Pay.UK."*

Industry-level coordination to resolve operational issues was also described as time-consuming, involving frequent meetings across multiple firms and parties.

Reporting and compliance costs

PSPs also described increased reporting and compliance costs, including new systems, duplicated data entry across platforms, monthly granular reporting across numerous data fields, and additional governance and assurance requirements. One PSP noted that reports initially required CFO sign-off, although this was later changed as processes became more established. This indicates that the burden was particularly high during implementation, before firms were able to streamline their reporting arrangements.

The burden appears to vary by firm size and automation capability. Larger PSPs may be better able to absorb reporting requirements through automated systems and established compliance functions. Smaller PSPs, or firms with less developed fraud and claims infrastructure, may face a higher relative burden where reporting processes rely more heavily on manual data entry, reconciliation and quality assurance.

Illustrative costs

Estimating the additional non-reimbursement costs attributable specifically to the reimbursement requirement and performance data publication is difficult. As shown in Section 5.2, many PSP actions to tackle fraud have been driven by the reimbursement requirement, but wider factors such as protecting their customers and responding to evolving scam tactics

have also been important. Section 6.4 also noted that much of the investment in tackling fraud has been holistic and improved fraud controls beyond in-scope APP fraud.

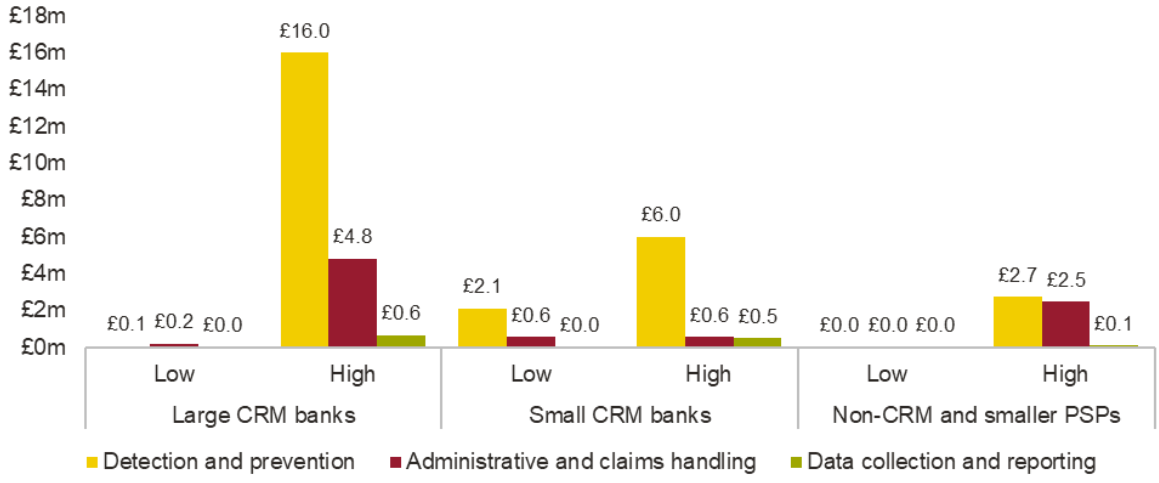
Data on PSP fraud costs therefore captures a wider set of drivers than the PSR policies. Any estimate of the proportion of costs attributable to the reimbursement requirement and publication of performance data is necessarily judgement-based.

We asked firms, through the voluntary evaluation PSP survey and industry evaluation data request, to provide estimates of their additional annual non-reimbursement costs associated with the policies. The estimates below are based on responses from 17 firms, which together account for 75% of FPS transaction volumes.[106]

Figure 47 shows reported annual non-reimbursement costs varied by firm type and category:

- Detection and prevention costs were consistently the largest category, ranging from £0.1m to £16.0m for large CRM banks, £2.1m to £6.0m for small CRM banks, and £0.0m to £2.7m for non-CRM and smaller PSPs.
- Administrative and claims-handling costs were lower, ranging from £0.2m to £4.8m for large CRM banks, £0.6m for small CRM banks, and £0.0m to £2.5m for non-CRM and smaller PSPs.
- Data collection and reporting costs were comparatively small across all firm types, with reported costs ranging from £0.0m to £0.6m.

Figure 47 Range of reported estimates of annual non-reimbursement costs



Source: Frontier analysis of industry evaluation data, the voluntary evaluation PSP survey and the FCA-PSR Joint Survey

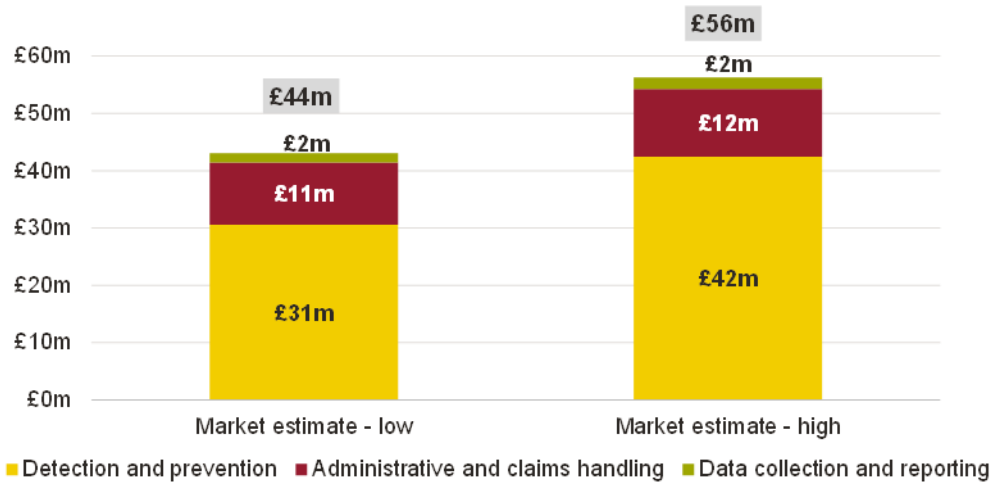
106 We extracted numerical values from free-text responses provided by firms. Where the impact was provided in terms of additional employees or time spent, we converted it into a cost measure. One-off investments were annualised over a five-year period. Expected future costs were also annualised and included in this estimate. Where firms were unable to quantify how much of a particular cost can be attributed to the policy, we assumed a 50% attribution rate in the low scenario and 80% attribution rate in the high scenario.

We scaled the reported costs in each group to market level by using the Faster Payments market share of firms in that group to estimate a plausible range of market-level expenditure. Extrapolating the estimated annual costs provided to whole-market level suggests the total market costs to be in the £44m to £56m per year range. The composition of these market costs is set out in Figure 48.

These are estimated annual costs for at least the first several years since the policy implementation. We have not estimated what the costs may be further in the future, but PSPs highlighted that tackling APP fraud requires ongoing investment to respond to changing scam tactics.

For the reasons set out above, these figures should be interpreted as indicative high-level approximations to provide a sense of scale, rather than precise estimates of the incremental costs caused by the policies.

Figure 48 Illustrative incremental industry annual non-reimbursement costs



Source: Frontier analysis of industry evaluation data, the voluntary evaluation PSP survey and the FCA-PSR Joint Survey

Taken together, the illustrative non-reimbursement cost estimates suggest that total PSP costs associated with APP fraud management have increased overall, although the precise scale of the increase is uncertain.

8.2 What has been the impact on PSPs' financial position?

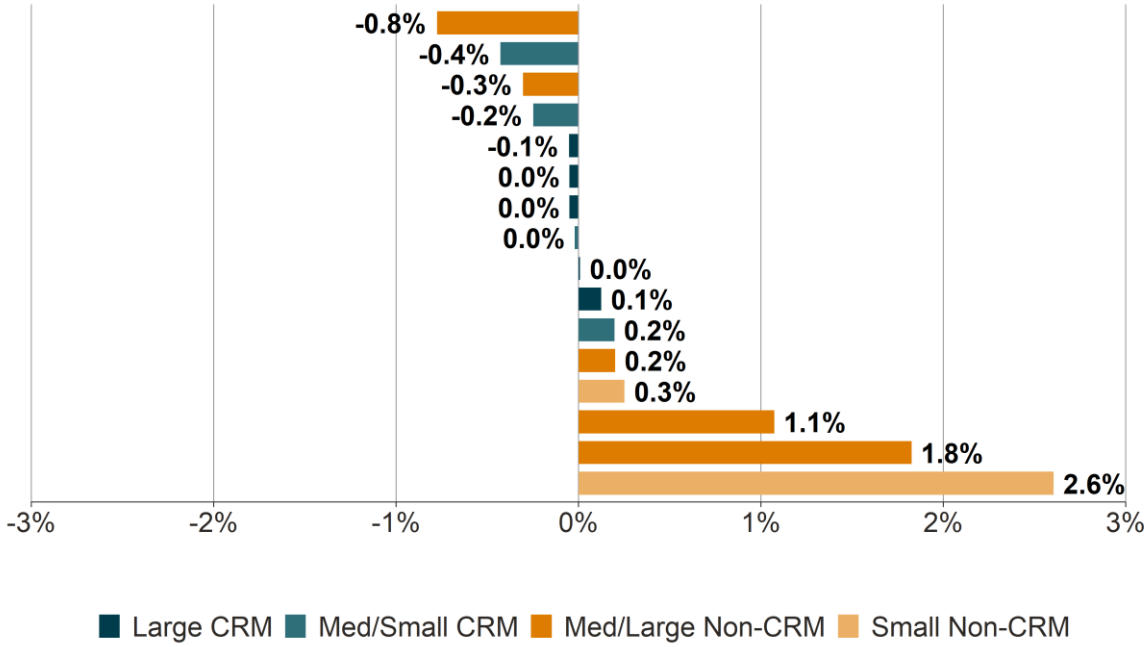
8.2.1 Most PSPs appear able to absorb the cost impact in the short term

Understanding the impact on PSPs' financial position is important because sustained cost increases could affect firms' profitability, investment capacity and financial resilience, even where they do not create immediate solvency concerns.

For most PSPs, the increase in reimbursement costs appears manageable relative to their overall revenues.[107] As shown in Figure 49 Change in annual reimbursement costs as a share of revenue by PSP, for most firms in our sample, the increase in annual reimbursement costs was negative or less than 0.5% of revenue. Three firms have seen increases of over 1% of revenue and one of those firms has seen costs increase by 2.6% as a share of revenue.

For a typical UK bank with a return on equity of 12.5%, a 2.6% reduction in revenue would illustratively be equivalent to a 0.8 percentage point reduction in return on equity to 11.7%.[108] This is a material effect but as per feedback from stakeholders set out below, is unlikely to risk the viability of any PSP.

Figure 49 Change in annual reimbursement costs as a share of revenue by PSP



Source: *Frontier analysis of industry evaluation data and FCA data*

Note: *Change in annual reimbursement costs is calculated as the difference between annualised consumer reimbursement in the pre-policy period, April 2023 to December 2023, and the post-policy period, January 2025 to June 2025. Revenue is based on FCA financial returns for the four quarters from December 2024 to September 2025, with firm-specific adjustments where required due to missing values. Figures are shown only for firms where both reimbursement and revenue data were available*

Findings from stakeholder interviews and the voluntary PSP survey were consistent with this conclusion. Larger PSPs generally reported that reimbursement costs are significant but manageable in the context of their overall revenues and balance sheets. Several described

[107] We compare reimbursement costs to overall revenues, rather than total costs including non-reimbursement costs, as figures for the latter are more illustrative and are less accurate at the individual PSP level, particularly for those PSPs that did not provide their own cost estimates.

[108] UK banks tend to achieve a return on equity of 10-15%. We have taken the midpoint of 12.5%. With an income (revenue) to cost ratio of 60% and constant costs, a 2.6% reduction in revenue means a 6.5% reduction in profit before tax and in return on equity. A 6.5% reduction in return on equity from 12.5% is equal to return on equity of 11.7% or 0.8 percentage points.

these costs as ultimately being absorbed within pricing or distributed across the wider customer base, rather than creating financial stress. However, even where costs were manageable, firms described them as contributing to margin compression and reducing headroom for investment in products and services.

One large PSP described the impact as significant but not existential: *"It's not like killing us like it might kill tiny little firms, but it all adds up."* Another PSP said the policy was *"creating drag on our business and our ability to serve our customers and ability invest in our products and services."*

Some PSPs also raised concerns about tail-risk exposure from complex cases. Stakeholders said the regime could require PSPs to reimburse high-value investment scam cases even where the fraud was difficult to detect at the time of payment. Some firms characterised this as requiring PSPs to "*underwrite*" certain fraud risks that they could not fully control. Firms also noted that these cases can take a long time to assess, including determining whether the case falls within the definition of APP fraud and whether any exceptions apply. This creates uncertainty and means PSPs may have a material level of risk on their books while cases are being investigated. One such example is the 79th group case, where an investment firm has collapsed and is under investigation by City of London police. Victim losses in this case are estimated to be over £200m and some of these losses have been reimbursed by PSPs as APP fraud.[109]

Respondents consistently suggested that the financial impact is more acute for smaller or growing PSPs. For these firms, reimbursement costs, fraud prevention investment and operational costs may represent a larger share of revenue and may be harder to absorb. Several stakeholders noted that APP fraud liability has therefore become more prominent in board-level and investor discussions.

We found no evidence that the policies have caused sector-wide solvency concerns. Firm financial performance data from the FCA shows that the number of PSPs entering insolvency procedures has remained stable over the period. While insolvency data is a relatively high-level indicator and may not capture financial pressure short of firm failure, it does not suggest that the policies have led to an increase in PSP insolvencies to date.

We note anecdotally that the UK fintech Tred exited the PSP market at the start of 2025, citing the reimbursement requirement as a key driver behind this decision.[110]

[109] Isle of Man Today (2026). Banks accused of failing Isle of Man investors caught up in suspected £200m fraud | Isle of Man Today.

[110] Finextra (2025). UK green fintech Tred winds up; blames APP fraud reimbursement rules.

8.2.2 Evidence on investor attractiveness is limited, though some stakeholders reported increased investor concern

The reimbursement requirement could affect the attractiveness of PSPs to investors by increasing PSPs' expected fraud-related losses and creating uncertainty around future liability.

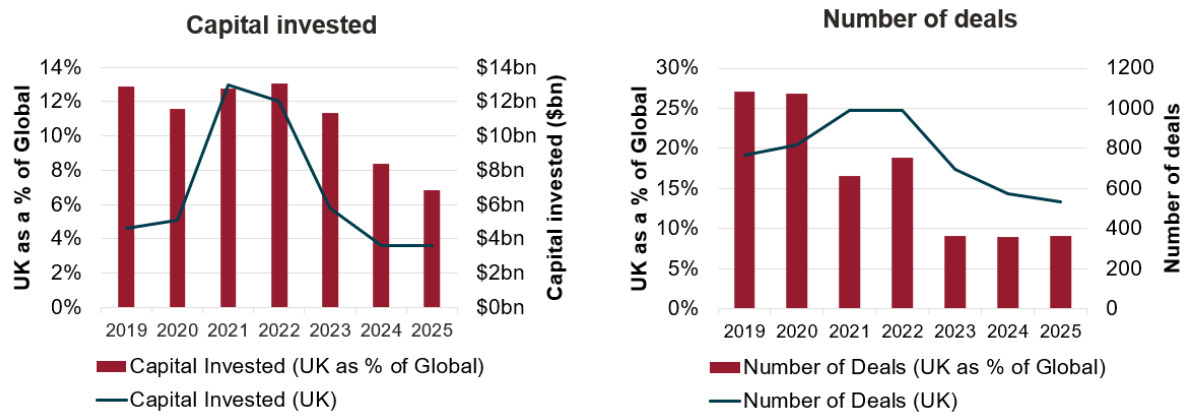
Evidence on the effect of the policies on PSP attractiveness to investors is limited. In our qualitative engagement with stakeholders many respondents declined to comment directly. However, a small number of growing PSPs and fraud technology providers said that APP fraud liability and reimbursement exposure had become more prominent in board and investor discussions. One smaller PSP commented:

> *"Investors can … invest … in the UK, but ... know that ... X per cent of the money … is just going to be … splashed away on reimbursing fraud."*

This suggests that the regime may be increasing perceived regulatory and financial risk for some firms, particularly smaller or scaling PSPs.

There is no clear quantitative evidence yet that the reimbursement requirement has materially reduced investor appetite for the sector overall. Innovate Finance publishes an annual overview of global and UK fintech investment.[111] This data, reproduced in Figure 50, shows a fall in UK fintech capital investment as a proportion of global fintech investment, from approximately 12% before 2023 to 7-8% since 2024. However, there is no evidence to attribute this change to the reimbursement requirement: the shift of global fintech investment towards the United States has been widely cited as the main driver behind this trend. While the UK share of global investment has declined, the UK is still the second leading market for fintech investment globally, with 534 deals and £3.6 billion of capital invested in 2025.

Figure 50 Capital investment in UK fintech companies



Source: Innovate Finance

[111] Innovate Finance (2026). FinTech Investment Landscape 2025.

8.3 How have the policies affected the costs faced by other organisations involved in managing fraud?

The policies were expected to increase costs not only for PSPs, but also for other organisations involved in managing fraud, because the regime requires wider coordination, case management, dispute resolution and familiarisation across the APP fraud ecosystem.

8.3.1 Stakeholders believe the costs of other organisations have increased

Evidence on these costs was more limited than for PSPs and came primarily from stakeholder interviews. These stakeholders indicated that some industry and public bodies have incurred additional costs linked to the policies. The scale of costs was not quantified by stakeholders, but they were not described as very high.

For industry organisations such as UK Finance and Pay.UK there were increased costs such as claims-handling infrastructure and support for industry coordination, including systems used to process and manage reimbursement cases. These costs are ultimately funded by the PSPs via levies and other contributions and covered in the PSP section above.

Some public sector and enforcement stakeholders also described a reallocation of existing resources towards APP fraud. For example, National Trading Standards reported that APP fraud is receiving greater priority in some areas, creating what it described as a *"postcode lottery"* in resource allocation across fraud types.

The FOS indicated that the policies had required some initial familiarisation, noting that *"anything new requires us to learn about it and for our teams to understand it"*. However, it also reported that it had not seen an increase in cases to date.

However, we do not have quantified evidence on the scale of these costs or the extent to which they represent additional spending rather than reprioritisation of existing resources. Due to the lack of stakeholders citing highly significant additional costs, we conclude that the scale of costs has been medium to low.

8.4 What has been the impact on the market for anti-fraud technology?

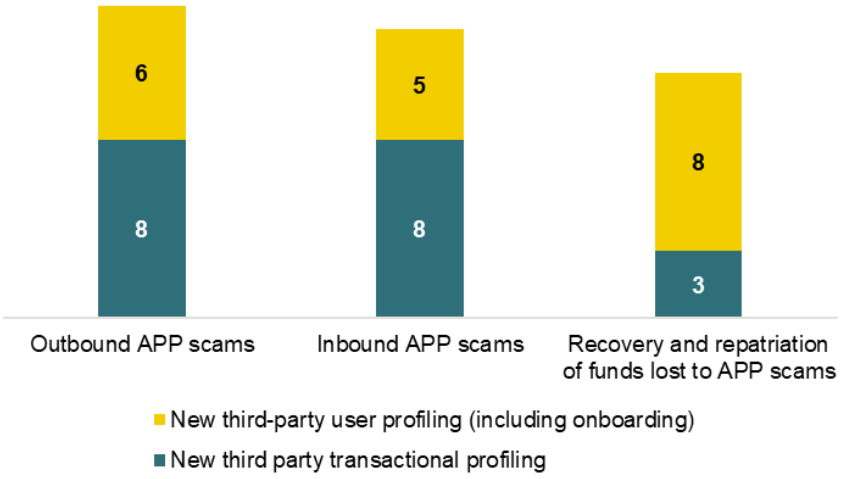
The policies may affect the market for anti-fraud technology by strengthening PSPs' incentives to invest in tools that help detect, prevent and manage APP fraud. This section considers whether there is evidence of increased demand for these technologies, and whether that demand appears to have been driven or accelerated by the reimbursement requirement.

8.4.1 There has been strong demand for anti-fraud technology

There is evidence of strong demand for anti-fraud technology. Our analysis of the industry evaluation data found that 12 out of 23 PSPs reported using third-party providers as part of

their activity to tackle APP fraud since 2023. These providers were used for both user profiling and transaction profiling. As shown in Figure 51, third party providers were most used to prevent outbound fraud.

Figure 51 Number of PSPs that introduced new anti-fraud technology from third party providers since 2023



Source: Data from 23 PSPs. PSPs are counted once in both the user profiling and transaction profiling categories, meaning that the two categories do not add up to the total number of PSPs that used either. Frontier analysis of industry evaluation data and the voluntary evaluation PSP survey

Evidence from stakeholder interviews with PSPs and fraud technology providers also points to increased demand for anti-fraud tools and analytics capability. Stakeholders described significant PSP investment in new anti-fraud technologies, including enhanced transaction monitoring, consortium data, artificial intelligence tools and improved customer risk profiling. Respondents also noted growth in new market participants and expanded services. Some stakeholders cited acquisition activity, such as Visa's purchase of Featurespace, as evidence of wider market growth.

One fraud technology provider said demand had "*definitely increased*" and described the UK as "*pushing the envelope*" in fraud innovation. This suggests that the UK market remains an active environment for anti-fraud technology development, particularly where tools can help PSPs identify scam risk before payments are made.

We are unable to quantify how much of the third-party anti-fraud technology demand was concentrated in UK-based firms compared to international ones. PSPs cited using both domestic anti-fraud tech firms such as CIFAS and international ones such as FeedzAI and BioCatch.

FCA Regulatory Sandbox applications also indicate significant interest in anti-fraud technology. Since August 2023, 86 companies have applied to use the FCA Regulatory

Sandbox for fraud-related technology. This represented 46% of all applicants to the Sandbox over the period, indicating strong interest in the development and testing of anti-fraud technology solutions.

8.4.2 There is some evidence that demand for anti-fraud technology has been driven by the reimbursement requirement

Stakeholder interviews provide some evidence that the reimbursement requirement has increased demand for anti-fraud technology. Some stakeholders suggested that mandatory reimbursement and liability exposure have made anti-fraud investment more commercially salient within PSPs. Reimbursement costs mean that fraud prevention investment can be framed not only as a customer protection or compliance measure, but also to reduce direct financial exposure.

Several stakeholders said APP reimbursement liability now features more prominently in board-level and investor discussions. One fraud technology founder said UK PSR liability was explicitly referenced in investor pitch decks as part of the investment case for anti-fraud solutions.

However, stakeholders generally suggested that the reimbursement regime accelerated demand for anti-fraud technology rather than creating it from scratch. Several PSPs argued that investment in anti-fraud technology was already planned in response to increasing scam sophistication and broader fraud risks. In this view, the reimbursement regime accelerated implementation rather than initiating it. As one PSP stated, "*Standing still is going backwards.*"

8.5 What might be the potential longer-term effects on service quality, innovation, and economic growth?

The long-term impacts of the APP scam policies remain uncertain. Our theory of change identified several mechanisms through which the policies could affect service quality, market innovation and economic growth over time. Stakeholder engagement highlighted perceived effects on these outcomes, but evidence to date mainly reflects stakeholder expectations

rather than observed market outcomes. The findings below should therefore be interpreted as evidence of potential risks and emerging impacts, rather than confirmed effects.

8.5.1 Stakeholders raised concerns about barriers to entry, competition and long-term impacts on innovation in the payments sector but evidence to date is limited

Barriers to entry and market competition

Some stakeholders argued that higher fixed costs and liability exposure may create barriers to entry and favour larger incumbents with stronger capital buffers. One specialist PSP asked: *"How can you enter a market now when you need that much liquid capital available?"*

A small number of stakeholders also suggested that the UK payments and fintech market may be less attractive relative to other jurisdictions if liability exposure remains comparatively high. One industry organisation described the regime as not *"an attractive feature from a UK vis-a-vis Europe point of view."* Some respondents raised broader concerns that the policy may contribute to consolidation or exit among smaller PSPs.

We have not found evidence of a reduction in market competition to date. There is no clear increase in PSP exits, or a slowdown in new entry, that can be linked to the policies. Recent developments suggest that the UK remains attractive to some major fintechs. For example, Revolut secured a full UK banking licence in March 2026, enabling it to expand its UK banking offer. However, it may take more time for the full impact of the reimbursement requirement on PSPs' costs and access to investment to be realised.

Market innovation

One potential unintended consequence of the reimbursement requirement identified in our theory of change is that the increase in PSP resources results in firms having to divert resources and investing less in innovation as a result.

In our interviews some PSPs believed this to be the case, with industry diverting resources towards implementation of the APP reimbursement regime. Stakeholders also suggested that other industry initiatives, including Enhanced Fraud Data, had been delayed or deprioritised as firms focused on compliance with the reimbursement requirement.

Some stakeholders indicated that the policies may have opportunity costs for non-fraud prevention innovation, particularly where specialist teams, technology budgets or industry coordination capacity are redirected towards compliance and operational implementation.

The longer-term impacts of the policies on market innovation will only become evident over time. The qualitative evidence suggests that some firms have diverted resources over the past few years towards implementing the reimbursement requirement, but this may lessen over time once new policies and processes become established. It therefore remains uncertain

whether stakeholders' concerns about future investment and innovation by the market will materialise.

8.5.2 Some concerns were raised about long-term service quality for consumers

Reduced service provision for certain customer segments

In interviews and the voluntary PSP survey, some stakeholders raised concerns that the reimbursement requirement could encourage defensive de-risking by PSPs. This could include offboarding higher-risk customers, applying more cautious controls to certain payment types, or reducing activity in sectors perceived to carry higher APP fraud risk.

There is limited evidence to date that these responses are prevalent across PSPs. The evidence gathered was largely speculative, with stakeholders suggesting that firms may be reassessing their appetite for serving certain customer groups or supporting certain types of payment activity, particularly where fraud losses are high or risks are considered difficult to manage. One CRM firm described its approach to de-risking as risk-based and customer-specific, rather than automatic:

> *"While some customers may be debanked, additional support is offered to those considered vulnerable, and decisions are not made automatically or without due consideration."* – CRM firm

As set out in Section 7.4 on crypto-related activity, crypto, remittance and some higher-risk customer segments were cited by stakeholders as areas where firms may be reassessing participation or applying greater friction. For example, given uncertainty over the scope of the reimbursement requirement, some PSPs reported preventing payments to crypto exchanges. One CRM PSP questioned whether current requirements could have wider implications for the development of crypto-related services in the UK, asking:

> *"Does the UK want to have a successful crypto industry, or does it want to squeeze it really hard with these types of rules?"*

These examples suggest that some PSPs are using more targeted controls to manage specific risks, such as restricting crypto payments or focusing protection efforts on customers considered more vulnerable to scams. This may help reduce unnecessary friction for the wider customer base. However, stakeholders also raised concerns that, if taken too far, de-risking in sectors such as crypto and remittance could reduce access to legitimate services and push some consumers towards less regulated or illegitimate money transfer channels.

Overall, while there is little evidence at this stage that defensive de-risking is prevalent across PSPs, some stakeholders considered that it could be a risk in the future. The longer-term consumer impact will depend on whether firms continue to apply proportionate, risk-based controls, or whether fraud liability leads to broader withdrawal from higher-risk customer segments, sectors or payment types.

8.5.3 Lack of aligned system-wide incentives may weaken long-term fraud outcomes

Throughout the evidence collected for the evaluation stakeholders highlighted that incentives remain distorted across the wider fraud ecosystem. PSPs and wider stakeholders noted that the reimbursement regime places a large share of liability on PSPs, even where the origin of the fraud lies elsewhere, such as on social media platforms or other digital channels. These stakeholders argued that the new policies may reduce incentives for other parts of the ecosystem to tackle fraud, and reduce incentives for consumers to remain vigilant, while requiring PSPs to bear the costs of fraud that they cannot fully prevent.

Over the longer term, the impact of the APP scam policies, and outcomes for consumers, will depend on actions across the wider fraud ecosystem.

8.5.4 Long-term economic and growth impacts remain uncertain

The longer-term economic and growth impacts of the APP scam policies remain uncertain. The data we collected for the evaluation mainly captures the first year after the reimbursement requirement came into force and many potential impacts are not yet observed.

There are multiple positive and negative channels by which the policies may influence growth, many of which are noted in previous sections. These channels include:

- **Competition and innovation in the payments market may be affected.** As noted above, stakeholders have raised concerns that increased fraud prevention costs and liability exposure could affect market entry, exit and the structure of competition in the payments market. If these effects limit competition, this could in turn reduce incentives for innovation. Some stakeholders also raised concerns that investment in tackling fraud may divert funds away from other forms of innovation. This effect could spill over to other sectors that interact with the payments market and ultimately the wider economy. However, there could also be potential pro-competitive effects if PSPs compete on providing the best protections against APP scams or best victim care for their customers.

- **Improvements in consumer confidence benefitting businesses.** The APP scams policies may have helped improve consumer confidence in the Faster Payments system and online commerce. While the PSR APP Fraud consumer survey data discussed in Section 6.2 currently indicates that not all consumers are aware of the policy, over time consumers may become aware of changes in the prevalence of fraud or reimbursement. Increased confidence may support continued adoption of account-to-account payments and other digital payment services, and this could contribute to cost reductions for businesses across the economy.

- **Benefits from growth in the anti-fraud technology market.** There may be benefits to economic growth through the growth of the anti-fraud technology market as the reimbursement requirement appears to have strengthened the commercial case for

investment in anti-fraud technology. However, the demand for anti-fraud technology has not been focussed on UK tech firms: PSPs reported using both UK-based and international providers for their investment in fraud prevention tech from third parties.

- **Keeping money in the UK**. One economic benefit highlighted by stakeholders was an increase in consumer spending power from the reduction in APP fraud. One respondent argued that fraud creates a wider economic cost because much of the money lost to fraud leaves the UK economy: *"the majority of [Fraud] money is going overseas. That money could otherwise be invested in things in the UK. So, there's a growth impact there."*

Achieving the positive case for growth from the policies will depend on the reimbursement requirement continuing to incentivise firms to invest in fraud prevention and prevent increases in fraud going forward.

Annex A

This annex shows how the evaluation questions set out in the Evaluation Framework map to the final questions used in the independent evaluation. The changes are minor and mainly reflect consolidation of overlapping questions or small wording changes to align the questions with the structure of the findings. The overall scope of the evaluation remains unchanged.

Figure 52 Impact evaluation questions

Impact evaluation questions	
Evaluation framework	**Independent evaluation**
Theme 1. Impacts on PSP actions to tackle fraud	
1. Have PSPs taken action to increase detection and prevention of outbound APP fraud?	Covered in "*Have PSPs taken action to tackle APP fraud?*"
2. Have PSPs taken action to increase detection and prevention of inbound APP fraud?	(as above)
3. Have PSPs taken action to increase detection and prevention of onward transfers of inbound APP fraud?	(as above)
4. To what extent are PSP's actions the result of the in-scope APP scam policies as opposed to other factors?	Unchanged
5. How and why have responses differed across PSPs?	Covered throughout.
Theme 2. Impacts on fraud	
1. How has the level of APP fraud changed?	Unchanged
2. What impact have the in-scope APP scam policies had on APP fraud?	Unchanged
3. How have levels of other fraud changed?	Unchanged
4. How have responses to the in-scope APP scam policies affected other forms of fraud?	Covered in "*To what extent are the changes in other fraud attributable to the APP scam policies as opposed to driven by other factors?*"
Theme 3: Impacts on consumer welfare	
1. What has been the impact of the policies on victims of APP fraud?	Unchanged
2. How consistently have consumers been treated by different PSPs?	Unchanged
3. How has the change in the level of APP fraud impacted consumers?	Unchanged
4. Have the policies led to increased payment friction for consumers and businesses?	Unchanged
5. Have there been any adverse effects on consumers and businesses?	Unchanged
Theme 4: Impacts on the PSP and other markets	
1. How have the policies affected the costs faced by PSPs	Unchanged
2. What has been the impact on PSPs financial position?	Unchanged
3. What has been the impact on the market for anti-fraud technology	Unchanged
4. How have the policies affected the costs faced by other organisations involved in managing fraud?	Unchanged
5. What might be the potential longer-term effects on service quality innovation and economic growth?	Unchanged

Source: Frontier Economics

Annex B

In Section 7.1, we showed that the total value of APP fraud has fallen since 2023, and that PSPs with higher pre-policy APP fraud rates tended to reduce APP fraud by more after the reimbursement requirement was introduced. This annex provides additional PSP-level evidence to support that analysis. It shows how inbound and outbound APP fraud rates changed across the PSPs in our industry evaluation sample before and after implementation of the reimbursement requirement.

We present results separately for inbound and outbound APP fraud, and for both APP fraud value and APP fraud volume. APP fraud is shown as a rate relative to each PSP's total Faster Payments activity, rather than as an absolute value. This allows comparisons between PSPs of different sizes and business models and helps distinguish changes in APP fraud exposure from changes in overall payment activity.

For each PSP, the series is indexed to 100 in October 2024, when the reimbursement requirement came into force. This means that the charts show relative changes in APP fraud rates over time for each PSP. Indexing makes it easier to compare trends across PSPs that started from very different levels of APP fraud exposure.

To classify PSPs as having increasing, decreasing or ambiguous APP fraud rates after the reimbursement requirement was introduced, we compare each PSP's average fraud rate before and after implementation. We calculate the pre-policy average using monthly fraud rates up to December 2023 and the post-policy average using monthly fraud rates from October 2024 onwards. PSPs with a change of more than 10% are classified as increasing or decreasing fraud rates, as appropriate. PSPs with smaller changes are classified as showing no clear change. We also classify PSPs as showing an ambiguous pattern if their post-policy average falls by more than 10% but their fraud rate rises sharply at the end of the post-policy evaluation period.

The charts should be interpreted alongside the main analysis in Section 7. PSP-level APP fraud rates can be volatile, particularly for firms with lower transaction volumes or a small number of high-value fraud cases. The annex therefore provides supporting descriptive evidence rather than a standalone causal assessment.

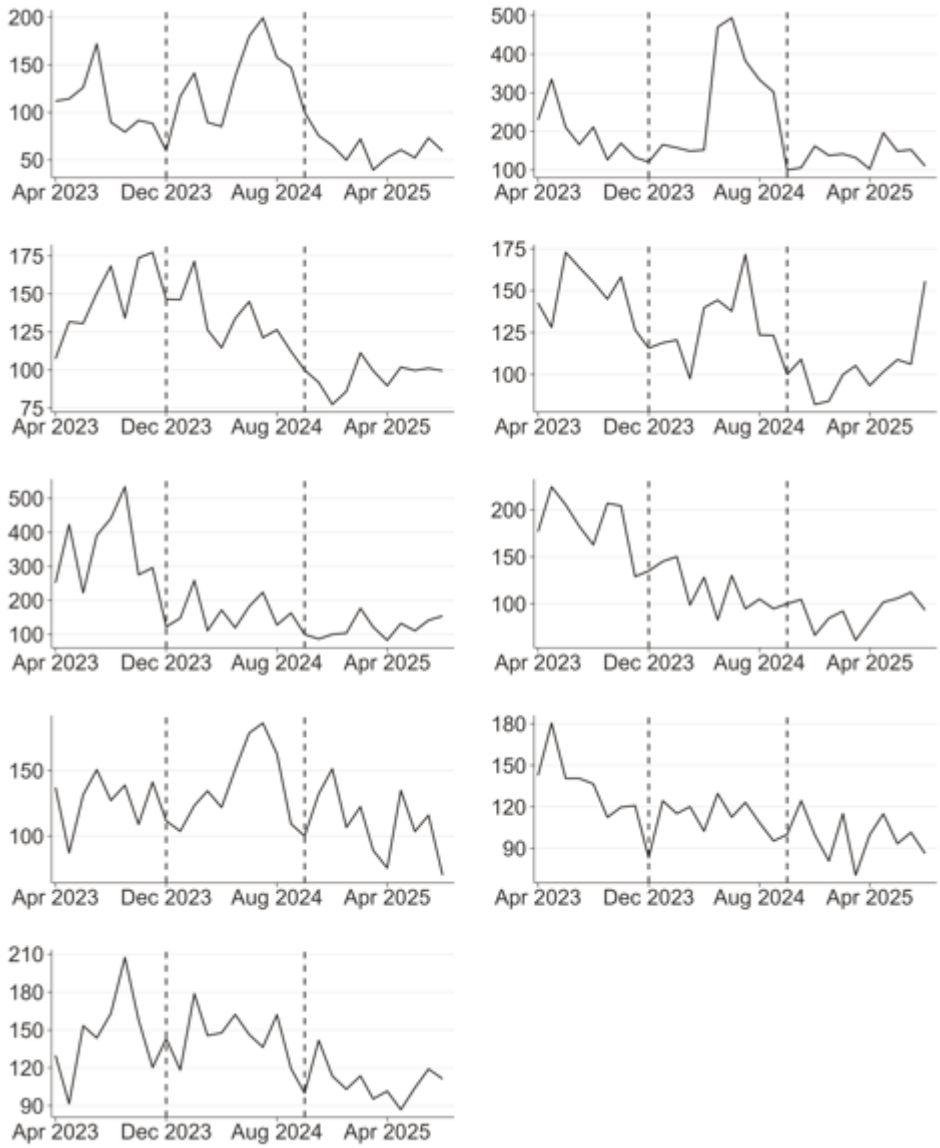
B.1 Inbound fraud

Most CRM and non-CRM firms experienced a reduction in inbound APP fraud rates after the reimbursement requirement was introduced. This is consistent with the policy increasing receiving PSPs' financial exposure to reimbursable APP fraud losses and therefore strengthening incentives to identify and prevent mule activity and other inbound APP fraud risks.

In particular:

- 9 out of 11 CRM firms experienced a decrease in inbound fraud value rates;
- all 8 non-CRM firms experienced a decrease in inbound fraud value rates;
- 4 out of 11 CRM firms experienced a decrease in inbound fraud volume rates; and
- 7 out of 8 non-CRM firms experienced a decrease in inbound fraud volume rates.

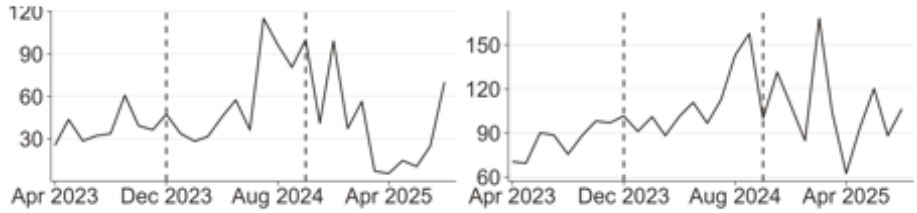
Figure 53 Inbound value of APP fraud has decreased for 9 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud value over FPS as a percentage of inbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

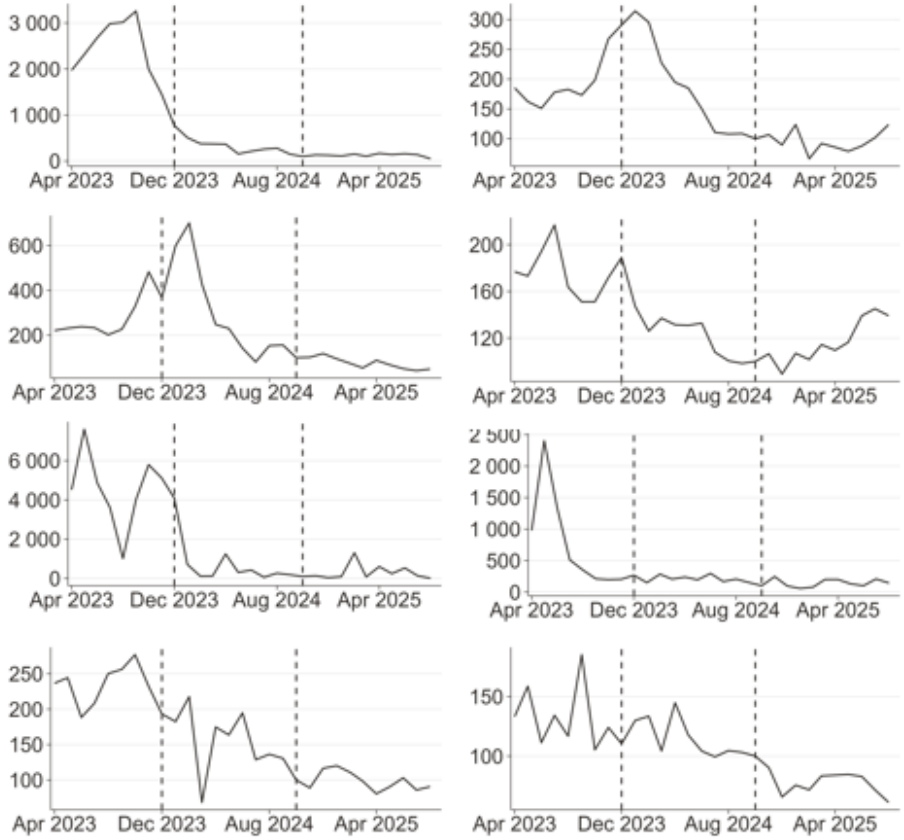
Figure 54 Inbound value of APP fraud trend was ambiguous for 2 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud value over FPS as a percentage of inbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

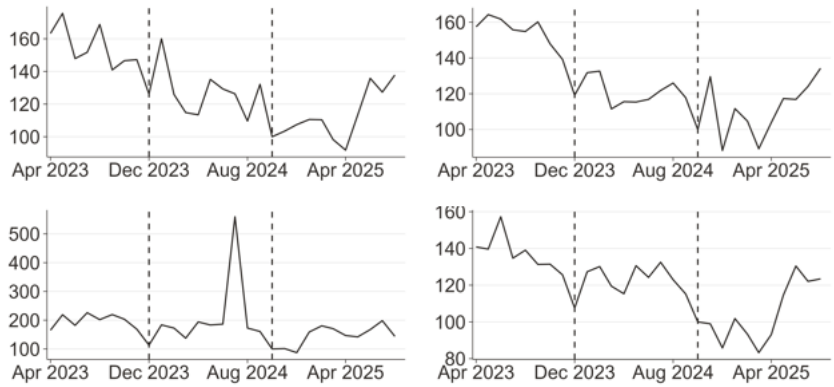
Figure 55 Inbound value of APP fraud has decreased for all 8 non-CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud value over FPS as a percentage of inbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

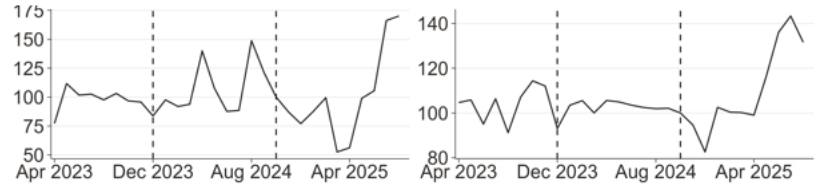
Figure 56 Inbound volume of APP fraud has decreased for 4 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud volume over FPS as a percentage of inbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

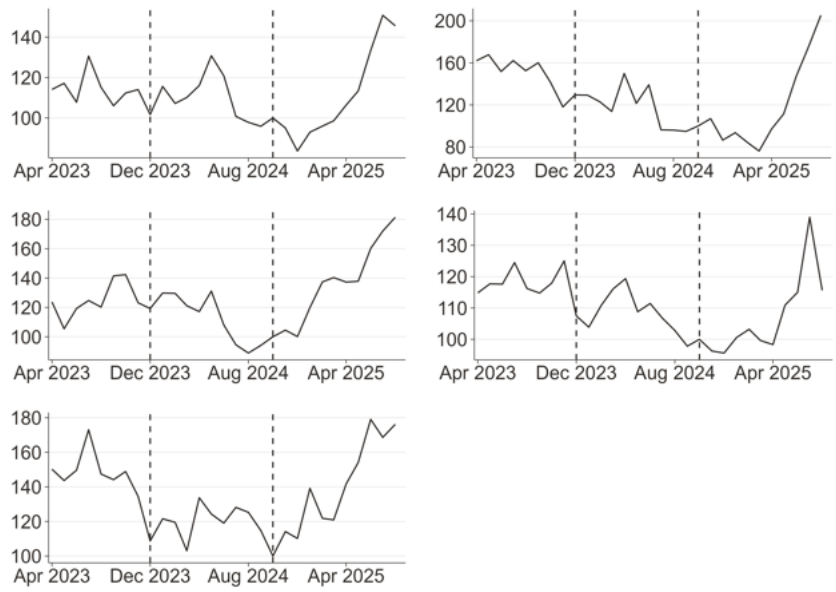
Figure 57 Inbound volume of APP fraud has increased for 2 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud volume over FPS as a percentage of inbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

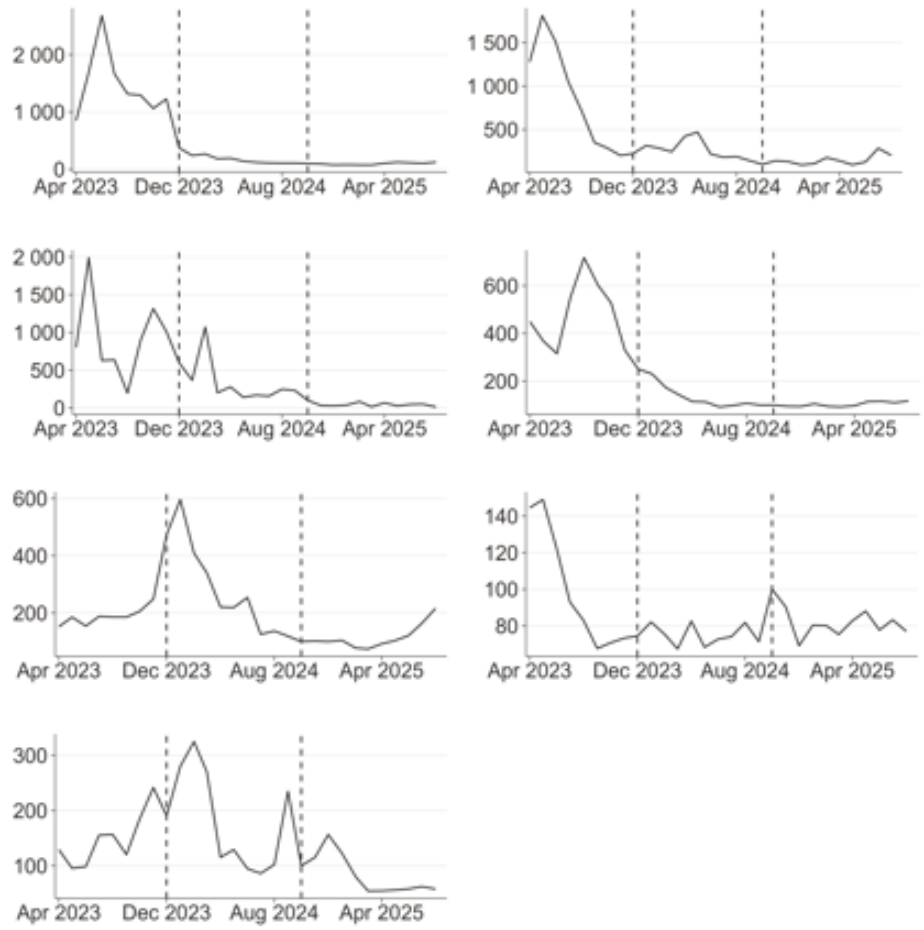
Figure 58 Inbound volume of APP fraud trend was ambiguous for 5 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud volume over FPS as a percentage of inbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

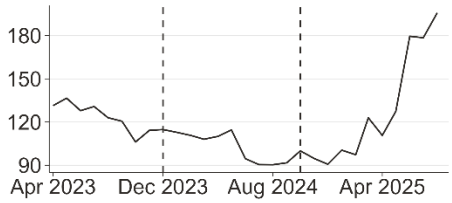
Figure 59 Inbound volume of APP fraud has decreased for 7 non-CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud volume over FPS as a percentage of inbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

Figure 60 Inbound volume of APP fraud has increased for 1 non-CRM firm



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows inbound APP fraud volume over FPS as a percentage of inbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

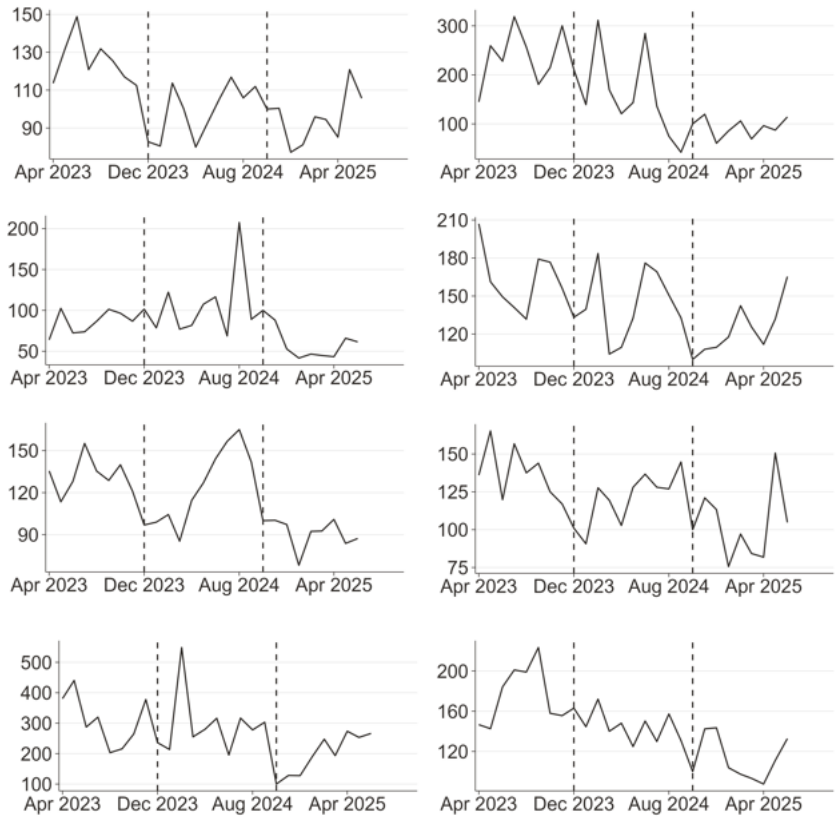
B.2 Outbound fraud

Most CRM and non-CRM firms also experienced a reduction in outbound APP fraud rates after the reimbursement requirement was introduced. This suggests that sending-side controls also strengthened over the period, including customer warnings, transaction monitoring, payment interventions and other measures intended to prevent customers from sending money to fraudsters.

In particular:

- 8 out of 11 CRM firms experienced a decrease in outbound fraud value rates;
- 5 out of 8 non-CRM firms experienced a decrease in outbound fraud value rates;
- 8 out of 11 CRM firms experienced a decrease in outbound fraud volume rates; and
- 5 out of 8 non-CRM firms experienced a decrease in outbound fraud volume rates.

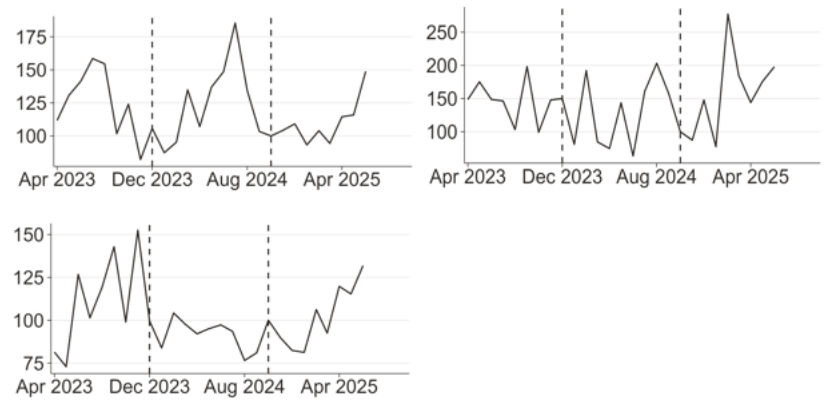
Figure 61 Outbound value of APP fraud has decreased for 8 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud value over FPS as a percentage of outbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

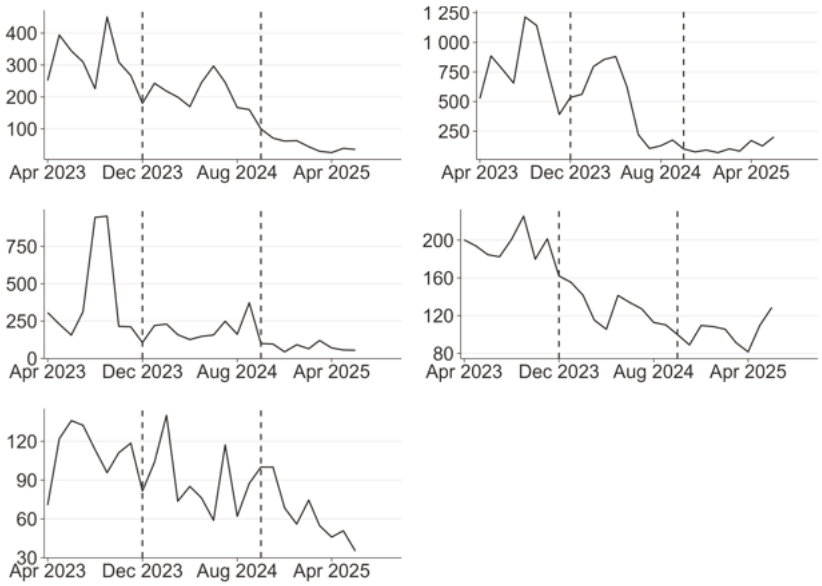
Figure 62 Outbound value of APP fraud trend was ambiguous for 3 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud value over FPS as a percentage of outbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

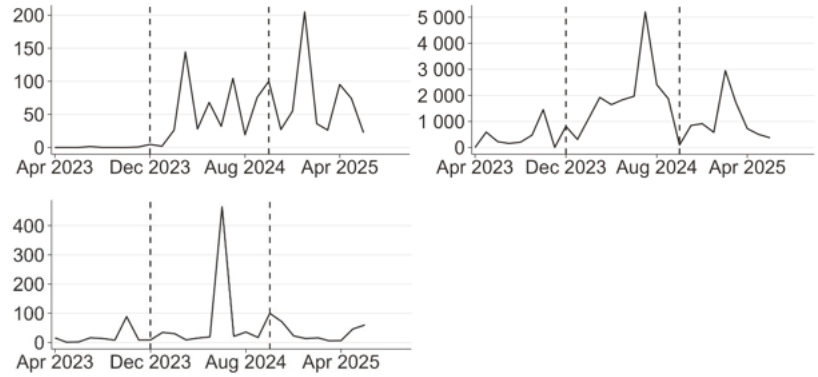
Figure 63 Outbound value of APP fraud has decreased for 5 non-CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud value over FPS as a percentage of outbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

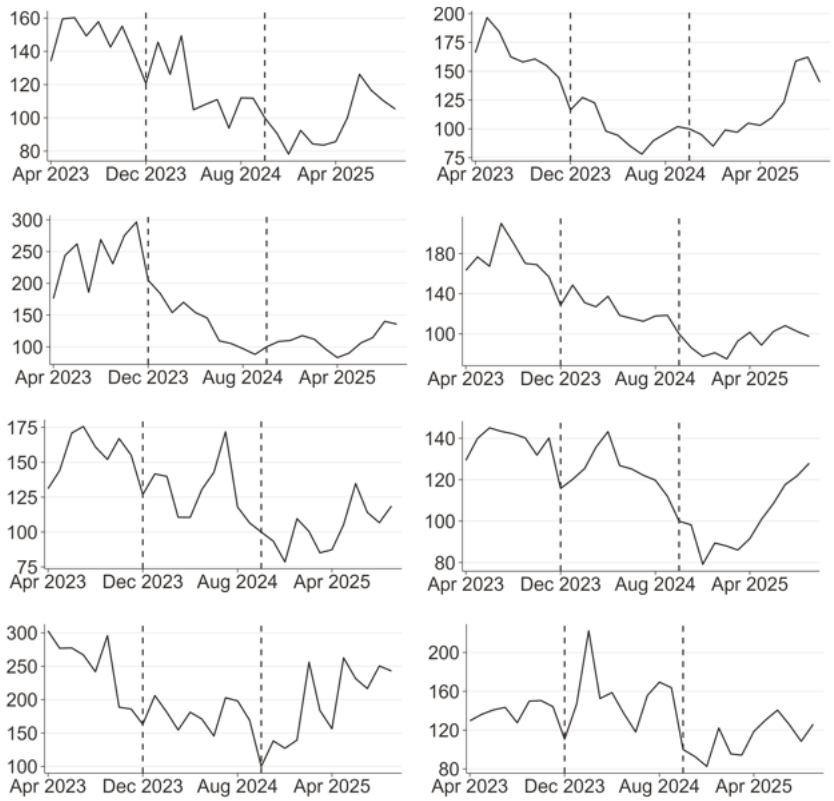
Figure 64 Outbound value of APP fraud has increased for 3 non-CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud value over FPS as a percentage of outbound FPS transaction value. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

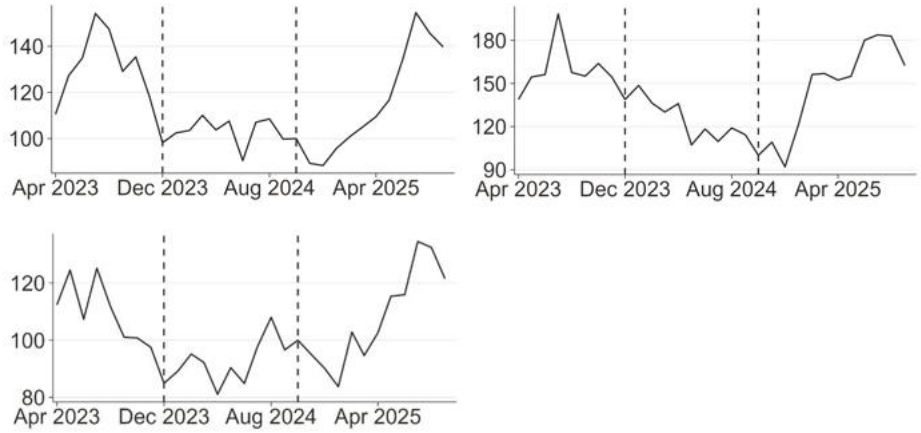
Figure 65 Outbound volume of APP fraud has decreased for 8 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud volume over FPS as a percentage of outbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

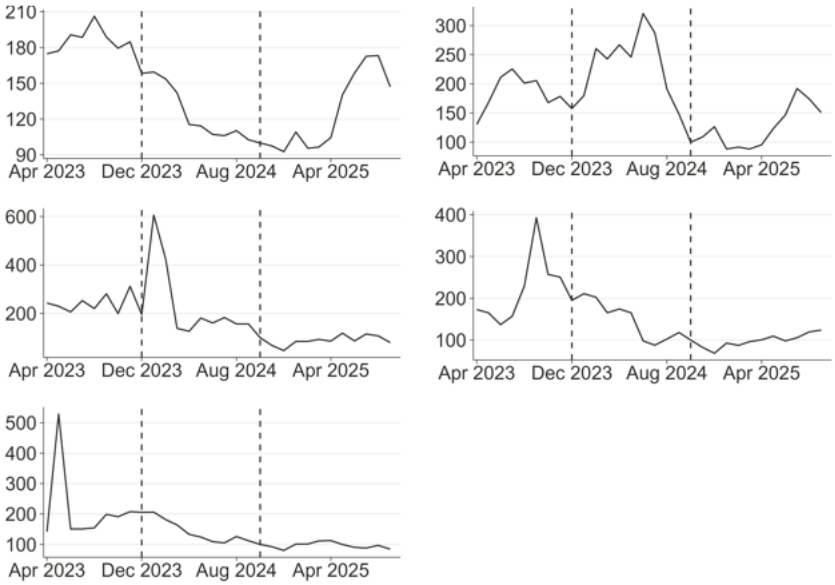
Figure 66 Outbound volume of APP fraud trend was ambiguous for 4 CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud volume over FPS as a percentage of outbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

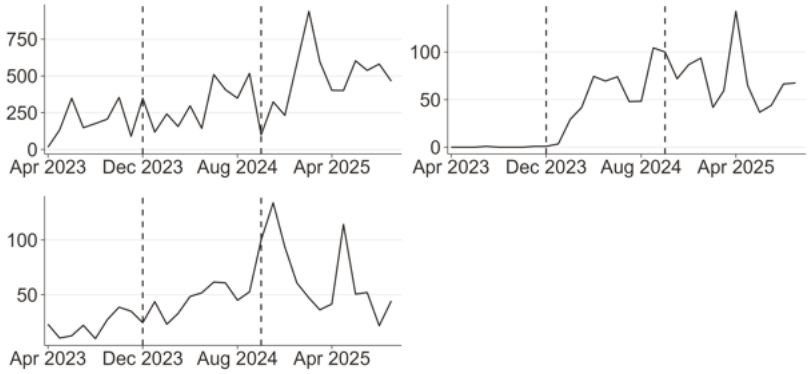
Figure 67 Outbound volume of APP fraud has decreased for 5 non-CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud volume over FPS as a percentage of outbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*

Figure 68 Outbound volume of APP fraud increased for 3 non-CRM firms



Source: *Frontier analysis of industry evaluation data*

Note: *For each PSP, the series shows outbound APP fraud volume over FPS as a percentage of outbound FPS transaction volume. The series is indexed to 100 in October 2024, when the reimbursement requirement came into force.*