

2024 APP scam performance data – before the reimbursement requirement was implemented

February 2026



Contents

Introduction	3
Key takeaways	4
Our ongoing work on APP scams	5
Scope of the data and challenges with APP scam reporting	6
Metric A: Percentage of reported APP scams losses refunded by value	7
Metric A: Percentage of reported APP scams losses refunded by volume	8
Metric B: Value of APP scams sent per £ million of transactions	9
Metric B: Volume of APP scams sent per million transactions	10
Metric C: Value of APP scams received per £ million of transactions	11
Metric C: Value of APP scams received per £ million of transactions	12
Metric C: Volume of APP scams received per million transactions	13
Metric C: Volume of APP scams received per million transactions	14
Annexes	15
Annex 1: Summary of performance	16
Annex 2: Scam types	17
Annex 3: Technical annex	18
Annex 4: Glossary	19
Annex 5: Scam type definitions	20
Annex 6: Entity legal names	21

Introduction

This is our report on Authorised Push Payment (APP) scam performance in 2024 before the reimbursement requirement came in. It covers the start of 2024 up to 7 October 2024.¹

APP scams occur when a fraudster tricks someone into sending a payment to accounts the fraudster controls. APP scams cause serious harm to consumers and damage trust in payments. They made up just over 38% of fraud losses in 2024², making them one of the UK's most prevalent crimes.

We implemented a mandatory reimbursement requirement in October 2024 to:

- ▶ ensure victims are reimbursed (except in exceptional cases)
- ▶ split reimbursement costs 50:50 between sending and receiving firms
- ▶ provide additional protections for vulnerable customers

Early data shows the policy is delivering positive outcomes for consumers and is driving PSPs to strengthen scam prevention. This global-first approach sets a strong standard for consumer protection and industry collaboration.

In the first twelve months of our policy, reimbursement rates were high with 88% of the money lost to APP scams (in scope of the policy) returned to victims, equalling £173m.

View since 7 October 2024

- ▶ 82% of claims were closed within 5 business days meaning consumers are generally receiving timely responses
- ▶ consumers reported around 269,000 claims of which 188,000 were in scope for reimbursement
- ▶ 3% of claims were rejected due to the consumer not taking enough care over the transaction or their claim

About this report

This is the **final dataset before the reimbursement requirement** came into effect.

It covers **January to 7 October 2024¹** and includes:

- ▶ victim reimbursement performance (pages 7–8)
- ▶ APP fraud sent (pages 9–10)
- ▶ APP fraud received (pages 11–14)

Unlike previous full-year reports, this one ends early due to the policy change. Since October 2024, we've published quarterly aggregate updates, with the latest covering **Q3 2025**.

¹ The data included in this report relates to fraudulent transactions that took place over the Faster Payments system before 7 October 2024 and where the case was closed between 1 January and 31 December 2024.

² UK Finance Annual Fraud Report 2025, page 13

Key takeaways

APP scams before mandatory reimbursement (Jan – 7 Oct 2024)

The data in this report reflects performance before the reimbursement requirement. Since October 2024, firm performance has shifted significantly. As the policy embeds, we expect continued improvements in end-to-end scam prevention.

For APP scams that took place before 7 October 2024 (and where the case was closed in 2024), we observed:

Reimbursement

60% reimbursed by value and 73% by volume – meaning most victims got their money back, but not all.

Significant variation between firms: outcomes depended heavily on the customer's bank, showing inconsistent protection before the new rules.

Sending fraud

£145m lost to APP fraud in the first half of 2024 – an 18% drop compared to H1 2023.

Volume down 13% year-on-year, with 108,759 cases recorded.

Decline driven mainly by purchase scams, which fell 8% compared to H1 2023.

Receiving fraud

The fraud rate for non-directed firms by value was 41 times higher than for the largest 14 banking groups.

Non-directed PSPs received 34% of total fraud value, despite handling only 19% of consumer Faster Payments by value.

They accounted for 48% of fraudulent transactions, despite processing just 10% of consumer Faster Payments by volume.

Scams by type

Purchase scams remain dominant, with 73% of cases by volume, but only 27% by value – mostly low-value scams.

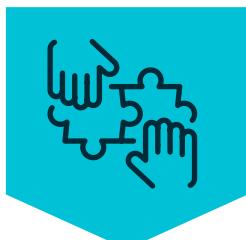
Investment scams represent 25% of value, but just 4% of cases – fewer but often high value and complex.

Our ongoing work on APP scams



Independent review of the APP scams policy

We have appointed Frontier Economics to carry out an independent evaluation of the APP fraud policies. This is in line with the commitment we made in the [Fighting authorised push payments scams: final decision policy statement](#) we published in December 2023. The independent evaluation will conclude by Q2 2026.



Working together with the FCA

We work closely with the FCA to tackle fraud and address any poor performance to ensure better outcomes for consumers. Fighting financial crime is part of the FCA's Strategy 2025 to 2030, and it has committed to driving awareness of APP scams.



Future APP scams reports

We are committed to leveraging data to enhance our work and contribute to the broader efforts within the ecosystem to mitigate fraud. We plan on consulting on proposals for APP scam data in Q1 2026 and welcome views from our stakeholders.

Scope of the data and challenges with APP scam reporting

The 14 largest banking groups in the UK³ were required to submit APP scams data.

This data includes:

- ▶ reimbursement levels
- ▶ levels of APP scams sent
- ▶ levels of APP scams received

The data covers the vast majority of Faster Payments in the UK by value and volume. As well as data about the 14 largest banks in the UK, the report also includes data about 11 smaller firms which are among the 20 highest receivers of fraud by volume and value.

As in previous years, there has been disagreement between sending and receiving firms regarding whether certain claims meet the criteria for an APP scam. Sending and receiving PSPs were encouraged to work together when investigating individual claims.

Identifying when a customer loses control is essential for assessing whether a transaction is within scope. This includes examples covered in prior reports, such as:

- ▶ me-to-me transactions: These involve a payment being sent from one account to another, where both accounts are in the same name. In these cases, an APP scam is flagged where the victim is considered to have been under the control of the scammer.
- ▶ payments to crypto exchange: where a scam may occur, but it may not be clear when the victim lost control of the funds to the fraudster or where only part of a payment journey took place over Faster Payments.

As in the first two cycles, the firms that were the highest receivers of APP scams had the opportunity to provide evidence to the sending firms and ask for the data to be amended where it does not meet the scope of a reportable APP scam.



Limitation

The data included in this report relates to fraudulent transactions that took place over the Faster Payments system **before** 7 October 2024 and where the case was closed between 1 January and 31 December 2024.

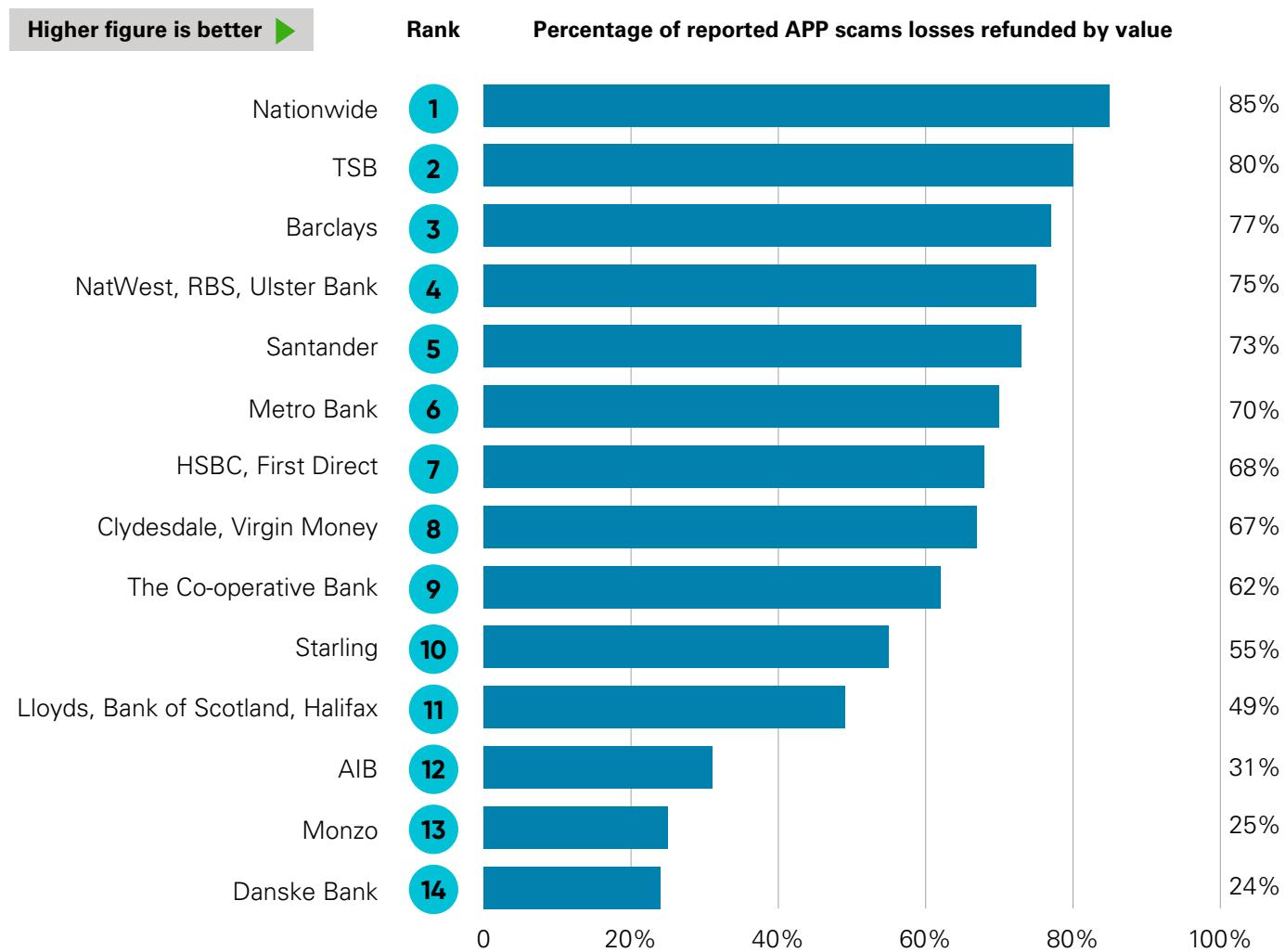
As the data does not capture cases over a full calendar year, we have not compared firm-level performance across different years.

By exception and where appropriate, we have looked at figures for the first half of 2024 and compared them to the equivalent period in 2023.

³ The 14 largest banking groups in Great Britain and Northern Ireland are listed on page 21.

Metric A: Percentage of reported APP scams losses refunded by value until 7 October 2024

The data in this chart is for the period prior to the introduction of the reimbursement requirement. It shows the percentage of APP scam losses reimbursed by the 14 largest banking groups for transactions before 7 October 2024 (cases closed in 2024). For example, Nationwide refunded 85% of the total value of money its customers lost to APP scams in 2024.



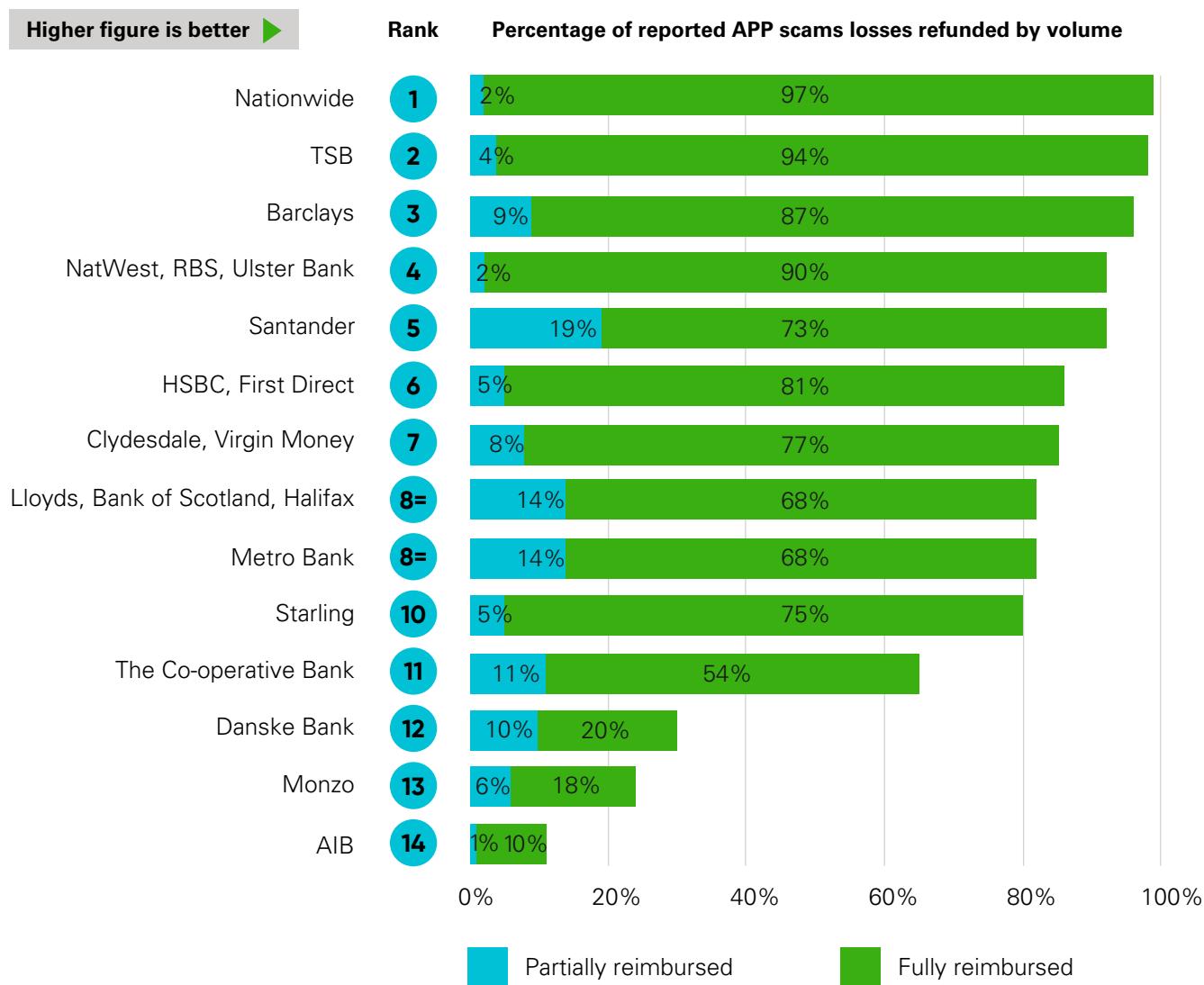
Up to 7 October 2024, of the money lost to APP scams by customers, 60% was reimbursed.

There's also a significant gap of 61 percentage points between the firms with the highest and lowest reimbursement levels. Consumer outcomes used to depend on who they bank with. Our new rules ensure fair treatment.

Our latest data on reimbursement shows that 88% of the money lost to APP scams (for in-scope cases) was returned to victims, equalling £173m

Metric A: Percentage of reported APP scams losses refunded by volume until 7 October 2024

The data in this chart is for the period prior to the introduction of the reimbursement requirement. It shows the percentage of APP scam cases that were fully and partially reimbursed by the 14 largest banking groups in the UK before 7 October (cases closed in 2024). For example, Nationwide fully reimbursed 97% and partially reimbursed 2%.

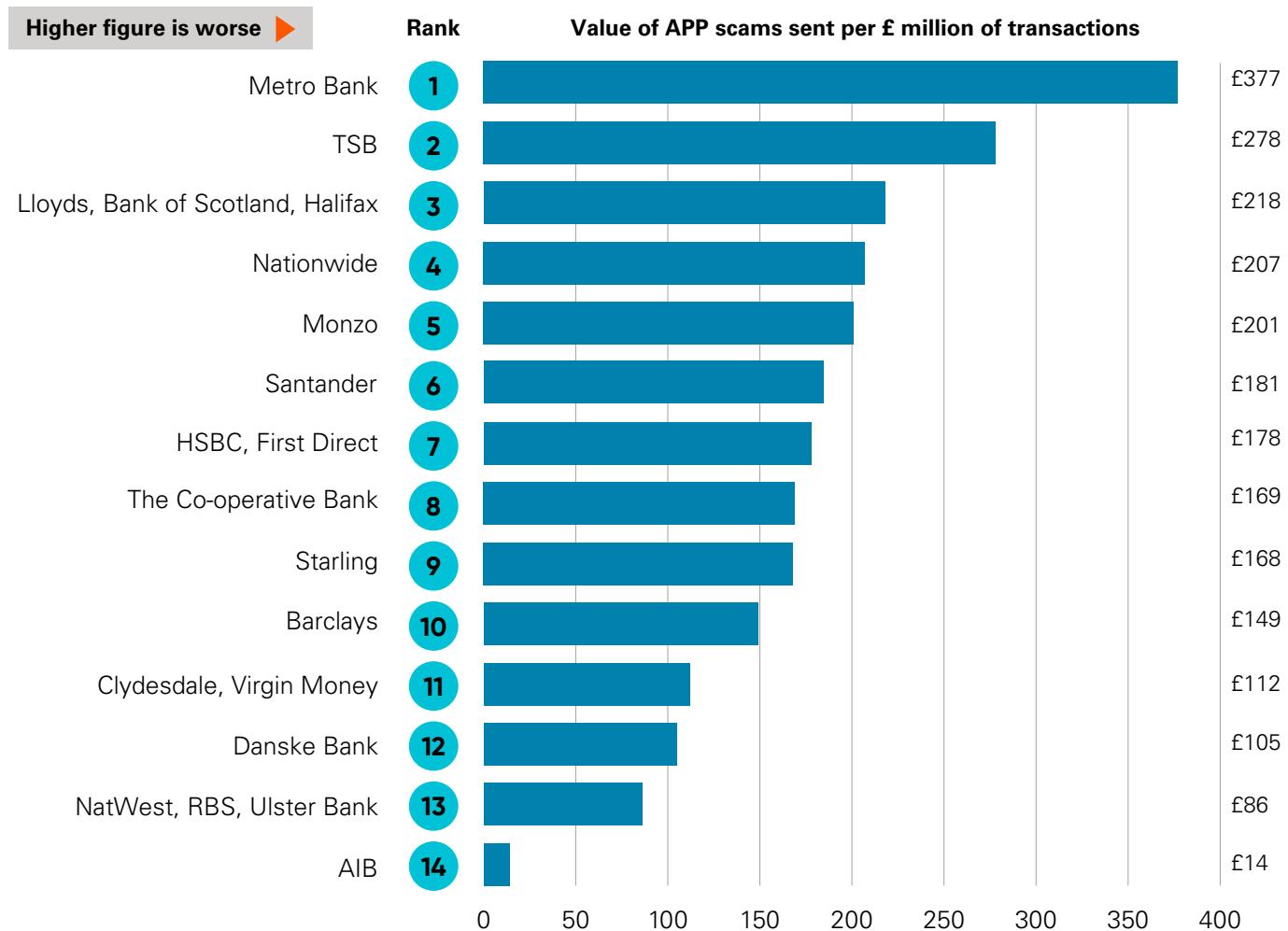


Up to 7 October 2024, 73% of reported APP scam cases were fully or partially reimbursed. We have seen a significant shift in performance since 7 October 2024.

Our latest data on reimbursement shows that 88% of the money lost to APP scams (in scope of the reimbursement requirement) was returned to victims, equalling £173m.

Metric B: Value of APP scams sent per £ million of transactions until 7 October 2024

The data in this chart is for the period prior to the introduction of the reimbursement requirement. It shows how much money customers at the 14 largest banking groups lost to APP scams for every £ million of transactions sent before 7 October 2024. For example, for every £1 million of transactions sent by customers of Metro Bank, £377 was lost to APP scams.

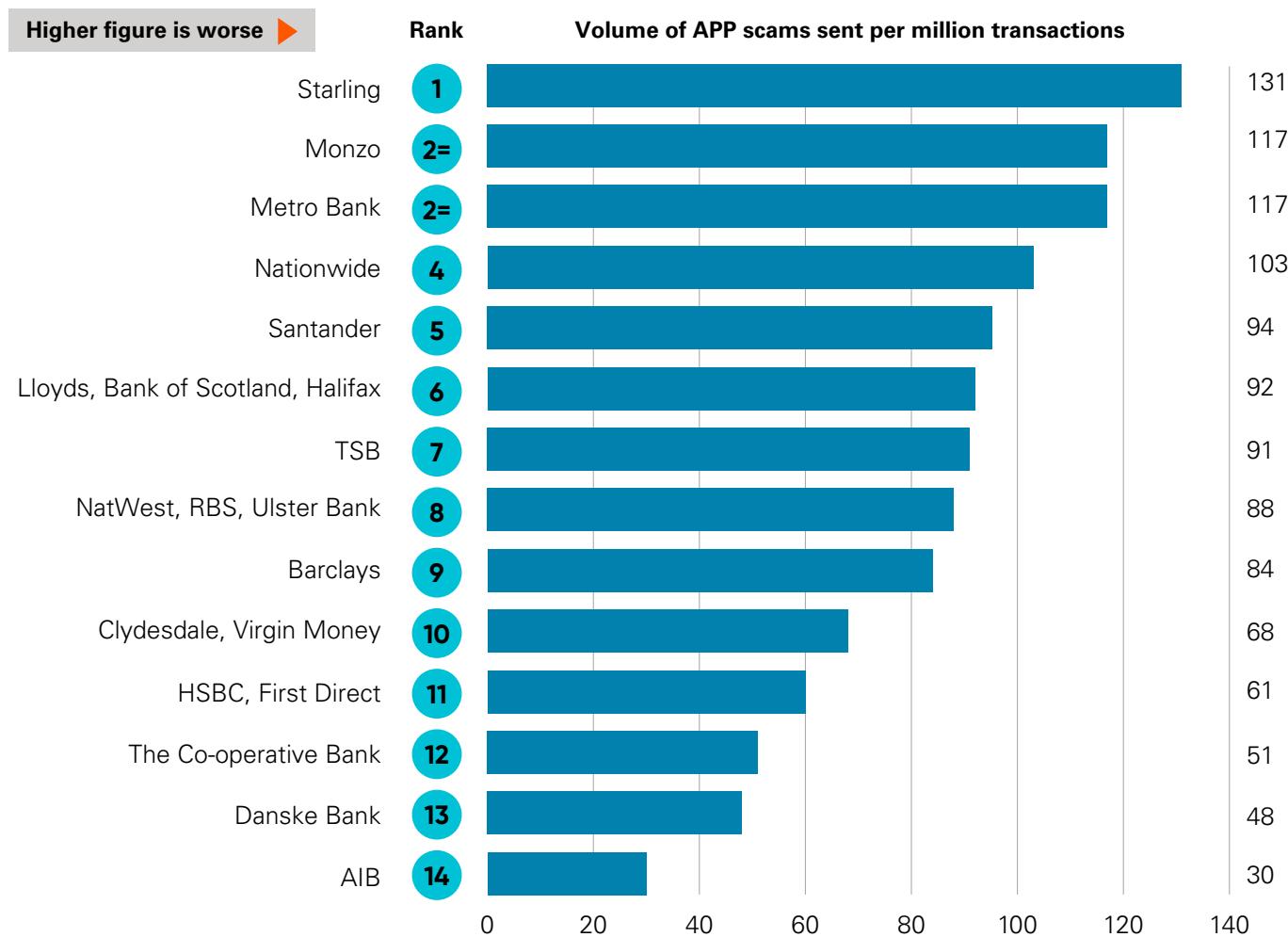


In the first half of 2024, £145 million was lost to APP scams in the UK. This is an 18% reduction compared to the equivalent period in 2023.*

* As this report only covers transactions before 7 October 2024, we cannot compare the total value of APP scams for the 14 largest UK banks with annual figures from previous years. Instead, we compare the first half of 2024 with the same period in 2023.

Metric B: Volume of APP scams sent per million transactions until 7 October 2024

The data in this chart is for the period prior to the introduction of the reimbursement requirement. It shows the number of APP scam transactions per million transactions customers of the 14 largest banking groups sent prior to 7 October 2024. For example, for every 1 million customer transactions Starling sent, 131 were reported as APP scams payments.



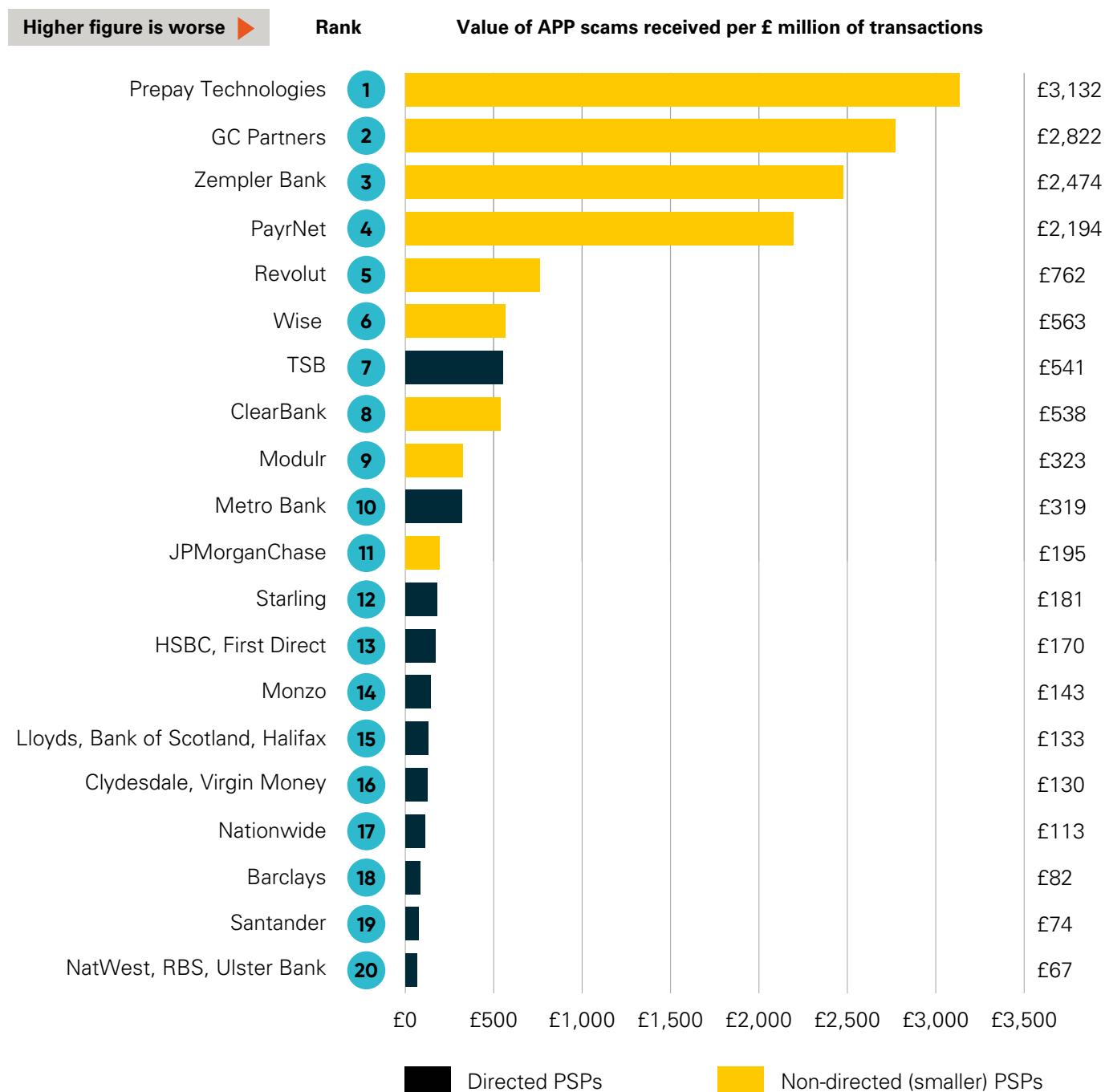
In the first half of 2024, 108,726 APP scam cases were reported in the UK. This is a 13% decrease compared to the equivalent period in 2023.*

* As this report only covers transactions before 7 October 2024, we cannot compare the total value of APP scams for the 14 largest UK banks with annual figures from previous years. Instead, we compare the first half of 2024 with the same period in 2023.

Metric C: Value of APP scams received per £ million of transactions until 7 October 2024

The data in this chart is for the period prior to the introduction of the reimbursement requirement. It shows the 20 firms which received the highest value of APP scams per £ million of transactions received prior to 7 October 2024.

For example, for every £1 million received into customer accounts at Prepay Technologies, £3,132 was APP scams.



Metric C: Value of APP scams received per £ million of transactions until 7 October 2024

As in previous reports, smaller non-directed firms continue to show significantly higher APP scam rates, compared to directed firms. Notably, the three highest non-directed firms are responsible for 15% of all APP scam losses, even though they only handle 3% of Faster Payment transactions made by consumers.

% of APP scams received by value by all directed and non-directed firms in the data*

Firm type	APP scams	Consumer Faster Payments
Directed	66%	81%
Non-directed	34%	19%

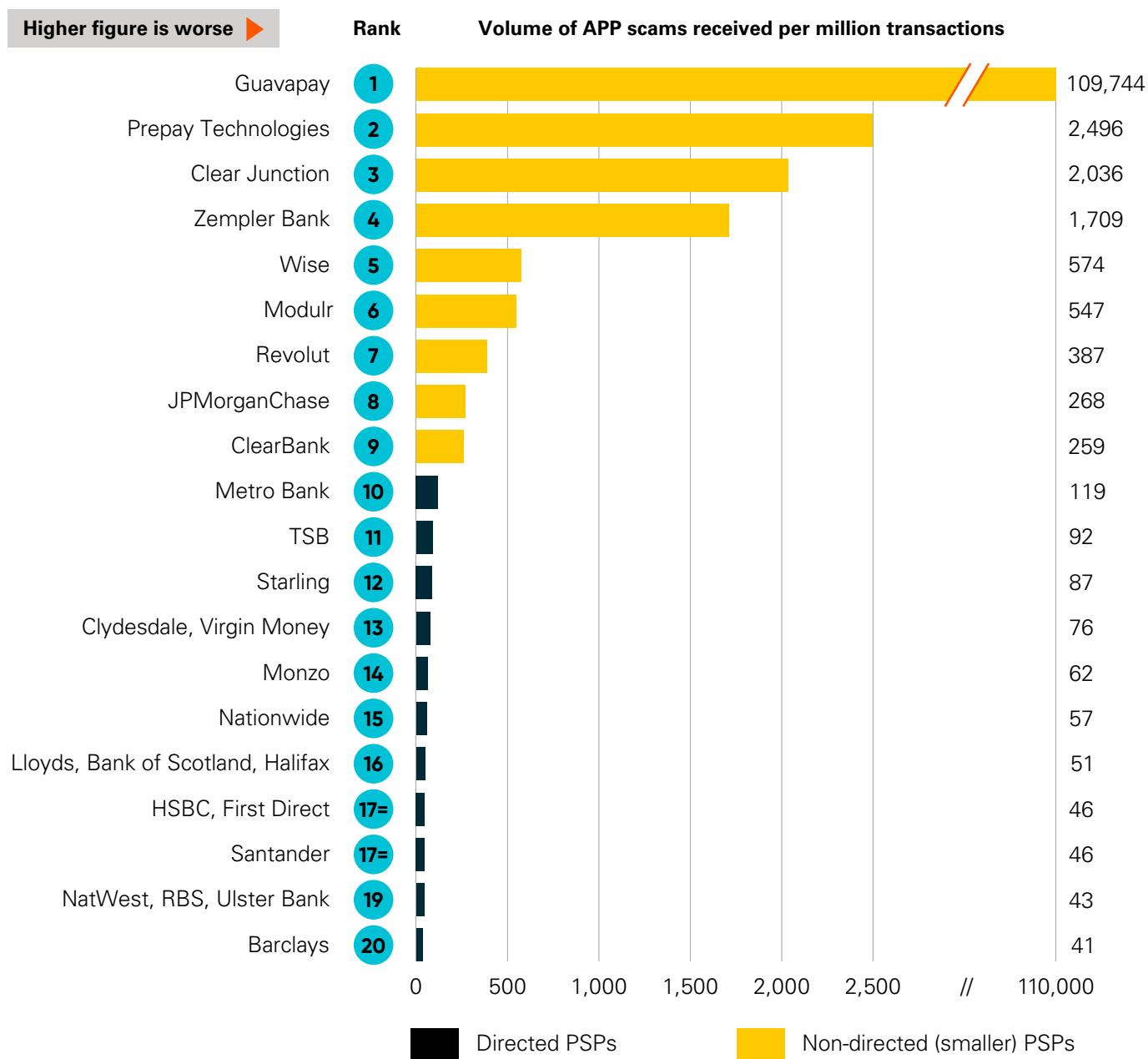


* This includes all 14 directed banks and all the non-directed firms they have sent fraudulent transactions to.

Metric C: Volume of APP scams received per million transactions until 7 October 2024

The data in this chart is for the period prior to the introduction of the reimbursement requirement. It shows the 20 firms which received the highest value of APP scams per million transactions received prior to 7 October 2024.

For example, for every 1 million transactions received by customers of Guavapay, 109,744* were APP scam payments.



* For comparison purposes, data for Guavapay has been scaled to represent fraudulent transactions per million transactions. The total number of fraudulent transactions received by Guavapay is much smaller (fewer than 10,000).

Metric C: Volume of APP scams received per million transactions until 7 October 2024

Scams received by non-directed firms account for just under half of total fraudulent transactions received, despite non-directed firms receiving only 10% of consumer Faster Payments transactions.

In 2024, Guavapay received the highest volume of APP scams per million transactions in the UK. Nearly 11% of the transactions it received were fraudulent. Guavapay is an outlier as its rate is nearly 44 times higher than the rate of the second worst-performing PSP. The FCA has imposed restrictions on Guavapay, mandating it to cease all customer onboarding and to stop issuing new e-money for existing clients.

There is a clear difference between the highest four firms receiving the most scams per million transactions and the next five firms. In fact, the fourth firm on the list gets almost three times more scams per million transactions than the fifth firm.

% of APP scams received by volume by all directed and non-directed firms in the data*

Firm type	APP scams	Consumer Faster Payments
Directed	52%	90%
Non-directed	48%	10%



* This includes all 14 directed banks and all the non-directed firms they have sent fraudulent transactions to.

Annexes

Annex 1: Summary of performance

How each firm has ranked across the metrics

	Metric A		Metric B		Metric C	
	Ranking (value)	Ranking (volume)	Ranking (value)	Ranking (volume)	Ranking (value)	Ranking (volume)
Directed PSPs						
AIB	12	14	14	14		
Barclays	3	3	10	9	18	20
Clydesdale, Virgin Money	8	7	11	10	16	13
The Co-operative Bank	9	11	8	12		
Danske Bank	14	12	12	13		
HSBC, First Direct	7	6	7	11	13	17 =
Lloyds, Bank of Scotland, Halifax	11	8 =	3	6	15	16
Metro Bank	6	8 =	1	2 =	10	10
Monzo	13	13	5	2 =	14	14
Nationwide	1	1	4	4	17	15
NatWest, RBS, Ulster Bank	4	4	13	8	20	19
Santander	5	5	6	5	19	17 =
Starling	10	10	9	1	12	12
TSB	2	2	2	7	7	11
Non-directed PSPs						
ClearBank	-	-	-	-	8	9
ClearJunction	-	-	-	-		3
GC Partners	-	-	-	-	2	
Guavapay	-	-	-	-		1
JPMorganChase	-	-	-	-	11	8
Modulr	-	-	-	-	9	6
PayrNet	-	-	-	-	4	
PrePay Technologies	-	-	-	-	1	2
Revolut	-	-	-	-	5	7
Wise	-	-	-	-	6	5
Zempler Bank	-	-	-	-	3	4



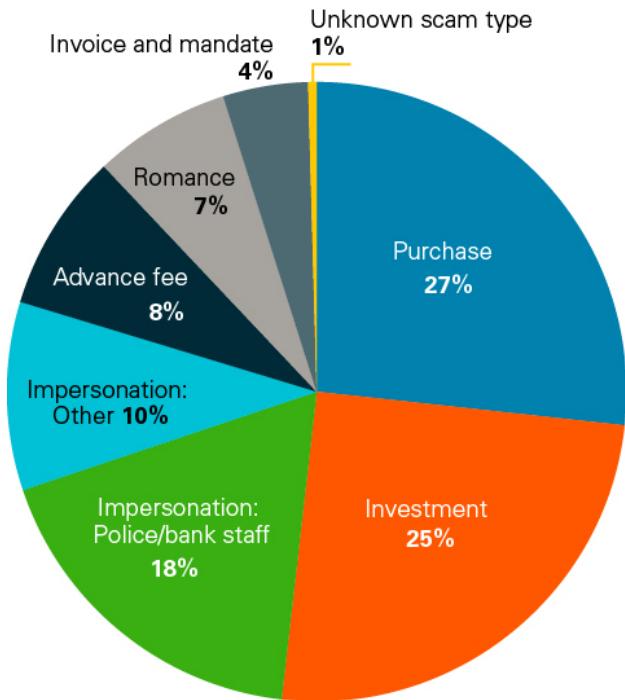
Firm not identified among the 20 firms receiving the highest levels of scams



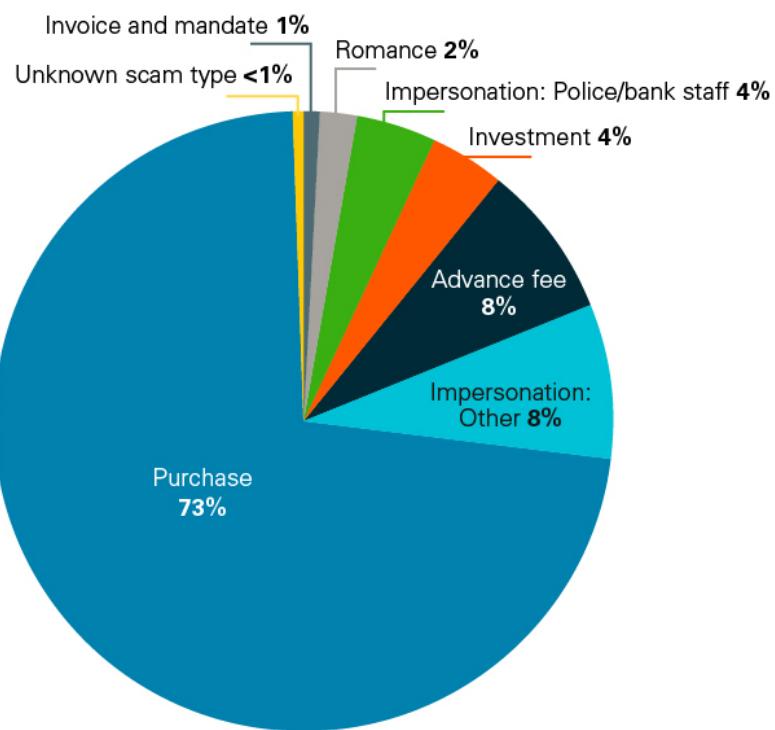
Data not requested by us

Annex 2: Scam types

APP scam types by value*



APP scam types by volume*



* CEO fraud is not shown on the pie charts as its share of value and volume of APP scams is minimal.

Annex 3: Technical annex

Data notes

Scope of the data

This report focuses on fraudulent APP scams in 2024 until the introduction of our reimbursement requirement. The data included in it relates to fraudulent transactions that took place over the Faster Payments system before 7 October 2024 and where the case was closed between 1 January and 31 December 2024.

The data included in this report shows:

- ▶ the reimbursement of victims across the 14 largest banking groups (**Metric A**)
- ▶ the level of APP scams sent from the 14 largest banking groups (**Metric B**)
- ▶ the level of APP scams received by the 20 firms receiving the highest levels of scams (**Metric C**).

Metric A

Financial Ombudsman Service reimbursements have been excluded when calculating reimbursement rates for firms.

Metric B

Any statistics related to sending APP scam losses in 2024 have been calculated excluding any recoveries made by firms, unless specified otherwise.

Metric C

We subtracted any money recovered and returned to the victims when calculating Metric C statistics for 2024.

While we would expect there to be consistency between the volume and value of APP scams sent (Metric B) and the volume and value of APP scams received (Metric C), this is not always the case, with some firms unable to identify the receiving firm in some cases.

We have made adjustments to the consumer Faster Payments in the case of some PSPs where this data was inconsistently reported by sending banks, especially where indirect PSPs were the receiving firms.

The receiving rate for the non-directed firms comes from data provided by the UK's 14 largest banks as non-directed firms are not required to submit data to us.

Annex 4: Glossary

Concept	Definition
Authorised push payment (APP) scams payment	<p>A payment made as part of an APP scam. The new reimbursement requirement applies to payments executed by the sending PSP, in accordance with an authorisation given by its customer, to an account controlled by a person other than the customer, where the customer has been deceived into granting that authorisation as part of an APP scams case. This includes where:</p> <ul style="list-style-type: none"> ▶ the payer intends to transfer the funds to a person other than the recipient, but is deceived into transferring the funds to the recipient ▶ the payer intends to transfer the funds to the recipient but is deceived as to the purposes for which they are transferring the funds
Closed case	<p>A closed APP fraud case means the directed PSP has completed an investigation of the case and made a decision on whether to reimburse the customer.</p>
Directed PSP	<p>A PSP subject to <u>Specific Direction 18</u> that submits data on:</p> <ul style="list-style-type: none"> ▶ APP scams sent from its accounts ▶ which PSPs are receiving those APP scams ▶ reimbursement of APP scams losses suffered by its customers
Faster Payments	<p>The UK electronic payment system that provides near real-time payments, as well as standing orders and forward-dated payments, operated by Pay.UK.</p>
Indirect PSP	<p>An organisation is considered to have indirect access to a payment system if it has a contractual arrangement with an indirect access provider, that is an organisation that already has direct access to that payment system. Less than 3% of FCA-regulated financial institutions are direct participants in Faster Payments, so most PSPs are indirects.*</p>
Payment service provider (PSP)	<p>A provider of payment services to customers typically through the provision of accounts. A PSP may be a bank, an e-money institution, a building society or a payment institution. In the UK, a PSP must be authorised and regulated by the FCA. PSPs may be direct PSPs or indirect PSPs, depending on whether they are able to initiate payments directly in a payment system or only via an indirect access provider.</p>
Receiving PSP	<p>The payment service provider that operates the account into which a payment is received in the UK via Faster Payments.</p>
Sending PSP	<p>The payment service provider that operates the account from which a payment is sent. This is where the victim of APP scams is holding their account.</p>

* UK Finance, Access to Payment Systems, July 2023.

Annex 5: Scam type definitions

Scam type	Definition
Advance fee	A scammer convinces a victim to pay an upfront fee for a good or service that they never receive.
CEO scam	A scammer pretends to be a CEO or other workplace figure to convince the victim (often employees of a business) to make a payment.
Impersonation	A scammer pretends to be the police, bank staff or a friend or family member to convince the victim to make a payment.
Investment	A scammer convinces a victim to make a payment into an investment that isn't real with the promise of a high return. The scammer may be pretending to be a financial advisor and using cold calling to reach out to the victim.
Invoice and mandate	A scammer sends a fake invoice to a victim to request payment for a good or service.
Purchase	A victim pays in advance for a good or service that they don't receive. The scammer may create a fake website or advertise a false product on social media.
Romance	A scammer feigns a romantic interest in the victim to win their trust and manipulate them into sending money.

You can find out more about different scam types in [UK Finance's Annual Fraud Report](#).

Annex 6: Entity legal names

Firm names and brands	Legal entity/Parent group
Directed PSPs*	
AIB	AIB Group (UK) plc
Barclays	Barclays Bank UK plc
Clydesdale, Virgin Money	Clydesdale Bank plc/Virgin Money UK plc
The Co-operative Bank	The Co-operative Bank plc
Danske Bank	Northern Bank Limited
HSBC, First Direct	HSBC UK Bank plc
Lloyds, Bank of Scotland, Halifax	Lloyds Bank plc/Bank of Scotland plc
Metro Bank	Metro Bank plc
Monzo	Monzo Bank Limited
Nationwide	Nationwide Building Society
NatWest, RBS, Ulster Bank	National Westminster Bank plc/Royal Bank of Scotland plc/ Ulster Bank Limited
Santander	Santander UK plc
Starling	Starling Bank Limited
TSB	TSB Bank plc
Non-directed PSPs**	
ClearBank	ClearBank Limited
ClearJunction	Clear Junction Limited
GC Partners	Global Currency Exchange Network Limited
Guavapay	Guavapay Limited
JPMorganChase	JP Morgan Europe Limited
Modulr	Modulr Finance Ltd
PayrNet	PayrNet Limited
PrePay Technologies	PrePay Technologies Limited
Revolut	Revolut Limited
Wise	Wise Payments Limited
Zempler Bank	Advanced Payment Solutions Limited

* The 14 largest banking groups in the UK

** Smaller companies identified as high receivers of APP scams

© The Payment Systems Regulator Limited 2026

The Payment Systems Regulator Limited
12 Endeavour Square
London, E20 1JN

Telephone: 0300 456 3677
Website: www.psr.org.uk