

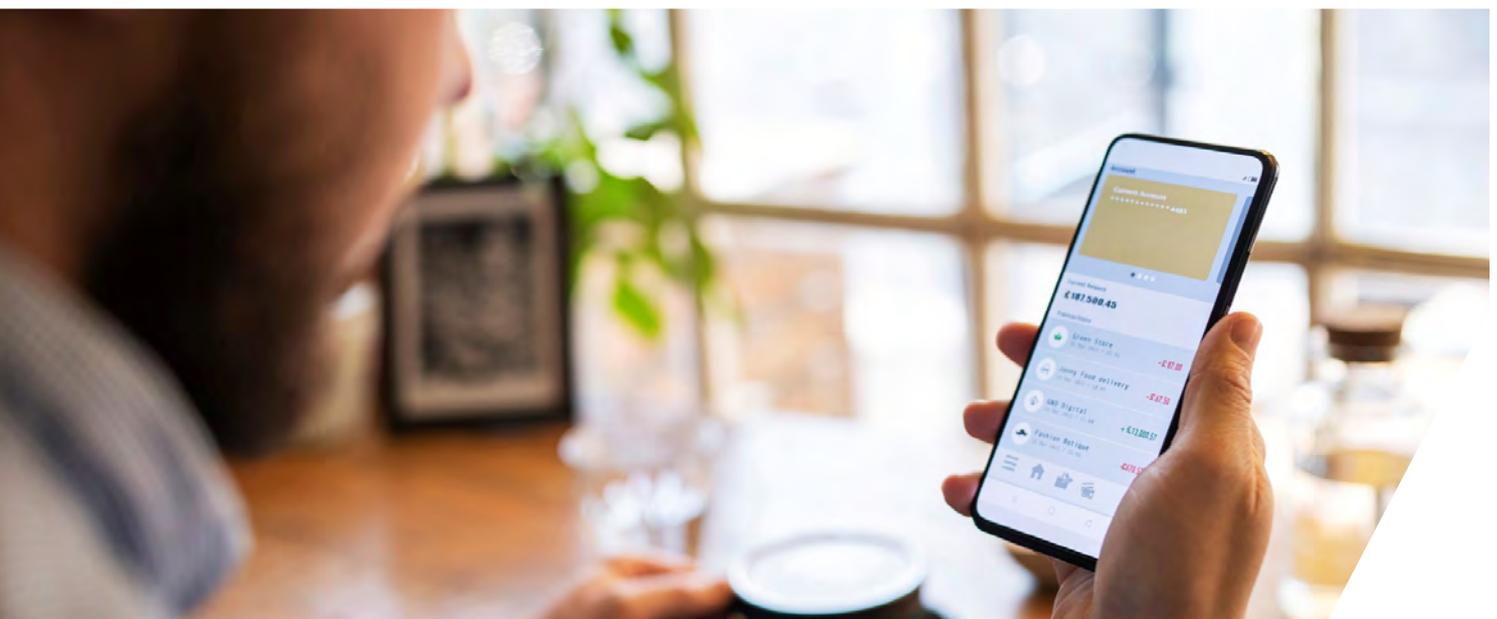
# Authorised push payment (APP) fraud performance report

October 2023



# Contents

Introduction	3
What are the current challenges with APP fraud reporting?	4
Key takeaways	5
Scope of the data	6
<b>Metric A:</b> Percentage of reported APP fraud losses refunded by value	7
<b>Metric A:</b> Percentage of reported APP fraud losses refunded by volume	8
<b>Metric B:</b> Value of APP fraud sent per £ million of transactions	9
<b>Metric B:</b> Volume of APP fraud sent per million transactions	10
<b>Metric C:</b> Value of APP fraud received per £ million of transactions – Non-directed PSPs	11
<b>Metric C:</b> Value of APP fraud received per £ million of transactions – Directed PSPs	12
<b>Metric C:</b> Volume of APP fraud received per million transactions – Non-directed PSPs	13
<b>Metric C:</b> Volume of APP fraud received per million transactions – Directed PSPs	14
What are we doing to drive better performance and improve outcomes for consumers?	15
Summary of performance	16
Total fraud	17
Technical annex	18
Glossary	19
Entity legal names	20



# Introduction

**Authorised push payment (APP) fraud happens when a fraudster tricks someone into sending a payment to an account outside of their control. There are more incidents of fraud than any other crime type in the UK, with APP fraud accounting for 40% of fraud losses in 2022.**

We are publishing 2022 data which shows how well the 14 largest banking groups<sup>1</sup> in the UK have performed with:

- ▶ the reimbursement of victims (pages 7 and 8)
- ▶ the level of APP fraud sent (pages 9 and 10)
- ▶ the level of APP fraud received (pages 11 to 14)

This is the most comprehensive data published to date, covering 95% of Faster Payments in the UK by value and volume. However, because there are many other payment firms in addition to the 14 largest, this report also shows the data for nine other smaller firms that were identified as being in the top 20 highest receivers of fraud (pages 11 and 13). These firms represent a disproportionately high level of fraud received for their size.



**Our ambition is to incentivise the entire payments ecosystem to make greater strides in preventing fraud and improving outcomes for victims.** There is more that individual payment service providers (PSPs) and the industry as a whole can do, and we would like to see significant improvements presented in the data in subsequent reports.

However, we have not sought to set targets or determine what good performance looks like in this report. This is because it is the first publication of this data, and when our reimbursement requirements come into force next year (2024) we expect to see significant shifts in levels of reimbursement. It is likely we will see changes in levels of reported fraud as consumer awareness of reimbursement requirements increases. We will continue this journey by publishing performance data on an ongoing annual basis.

The fight against APP fraud is a long-term effort. We are encouraged that firms are introducing measures to improve performance, but more needs to be done. We expect more proactive and open dialogue between PSPs to tackle fraud in real time, such as sharing better quality data to assess the risk of payments to potential fraudsters' accounts, intervening where necessary, and acting quickly to recover victims' funds where possible. Our reimbursement requirement will create further incentives on firms to prevent APP fraud, which is already prompting positive change in the industry. We have seen increased efforts by firms to tighten up controls and share more data than ever before, and we expect this to continue.

<sup>1</sup> Some banking groups include multiple PSP brands.

# What are the current challenges with APP fraud reporting?



## Communicating at the time of the fraud

The introduction of a reimbursement requirement in 2024 will see sending and receiving firms jointly liable for reimbursing victims of APP fraud in nearly all cases.

For this to happen, sending and receiving firms must communicate at the time of the fraud. Each firm holds key information relating to the transaction and it is critical they work together. In doing so, firms will be able to take action on related payments, such as stopping payments and recovering victims' funds where possible.



## Agreeing the scope of APP fraud

Firms currently assess claims differently. Through our data-collection process we identified inconsistent approaches between PSPs on in-scope cases, meaning cases accepted by one firm were rejected by others. In particular:

- ▶ **Me-to-me transactions:** Where a payment is made from a victim to an account in their name but the victim is understood to have been under the control of the fraudster.
- ▶ **Seller disputes:** Where a customer purchases a good or service which they never receive or does not match the description, which a number of PSPs have argued is very difficult to distinguish from a genuine purchase scam.
- ▶ **Payments made to a crypto exchange:** Where a scam may occur, but it may not be clear when the victim lost control of the funds to the fraudster.

Having a consistent approach is critical, as is a common understanding of which payments are in scope. In individual cases, it is important to identify where the loss of control occurred. The reimbursement requirement will drive more consistency in approach by creating the need for firms to communicate early on in the process.



# Key takeaways

**There are currently inconsistent outcomes for customers who report APP fraud to their PSP.**

A wide range of approaches are currently adopted in assessing an APP claim. These range from automatic reimbursement, to partial reimbursement with the customer bearing part of the cost, to only very narrow circumstances when a claim is considered.

Part of this variation is driven by differences in membership of the Contingent Reimbursement Model (CRM) code. This is a voluntary code that sets guidelines on how firms reimburse victims of APP fraud. While most of the firms who are CRM code members have higher rates of reimbursement to victims, some members performed poorly. Rates of sending fraud largely remain flat across the largest PSP groups.

We expect this variation to reduce with the introduction of the reimbursement measures in 2024. We will track the industry's performance and we will continue to work closely with the industry to ensure improvements are delivered.

**Receiving fraud data shows a high degree of variation and highlights weak controls that fraudsters have exploited.**

When a fraud is committed, fraudsters need access to accounts to receive the fraudulent funds. These are the receiving accounts and can include money mules or where a fraudster has taken control of a victim's account. The data on the top 20 firms receiving fraud shows greater variation in the performance of PSPs, with newer and smaller PSPs typically having disproportionately higher rates of fraud than firms that are larger and more established. This difference in performance suggests that there is significant potential for these firms to reduce fraud through enhancements to their systems and controls.

Because of this variation, we have separated the data to show performance against comparable peers.

**Firms have started to address gaps in controls, but more needs to be done.**

This report covers firm performance in 2022. Since then, our wider work on APP fraud has already focused the industry and encouraged firms to make progress in tackling the threat of fraud. Our 2024 reimbursement requirement will significantly ramp up this progress and ensure that sending and receiving firms are held equally liable for reimbursing victims of APP fraud in nearly all cases. The equal liability split will also incentivise firms to work together in addressing any vulnerabilities in their fraud prevention systems.

# Scope of the data

**An APP fraud is when a consumer is deceived into sending a payment.**

**For example:**

- ▶ the person receiving the funds may not be who they say they are, or
- ▶ the funds may not be used for the purposes which the victim transferred the funds for

Our data considers APP fraud where the reported victim is a consumer or a small business or charity with an annual income of less than £1 million.

All cases included in the data were closed in 2022 and occurred across Faster Payments in the UK. Faster Payments allow customers to send money electronically in real time. 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.

If a customer does not agree with the decision of a firm to not reimburse a reported APP fraud, they can refer the case to the Financial Ombudsman Service (FOS). We asked firms to exclude all reimbursements that happened as a result of FOS rulings as we consider these are not a true reflection of a firm's own reimbursement policy.

Approaches to reimbursement differ depending on whether the firm is a member of the CRM code.<sup>2</sup> The code is voluntary and asks members to commit to reducing and preventing APP fraud.

Currently, PSPs' interpretation of what an APP fraud is differs in a number of areas. We have not sought to change firms' decisions on whether an historical case was an APP fraud.

This has, however, created some discrepancies between sending and receiving firms. For example, the sending firm may have recorded the case as an APP fraud and reimbursed the customer, while the receiving firm may believe the fraud to be out of scope. Where the sending and receiving firm have been unable to agree, we have relied on the data submitted by the sending firm.

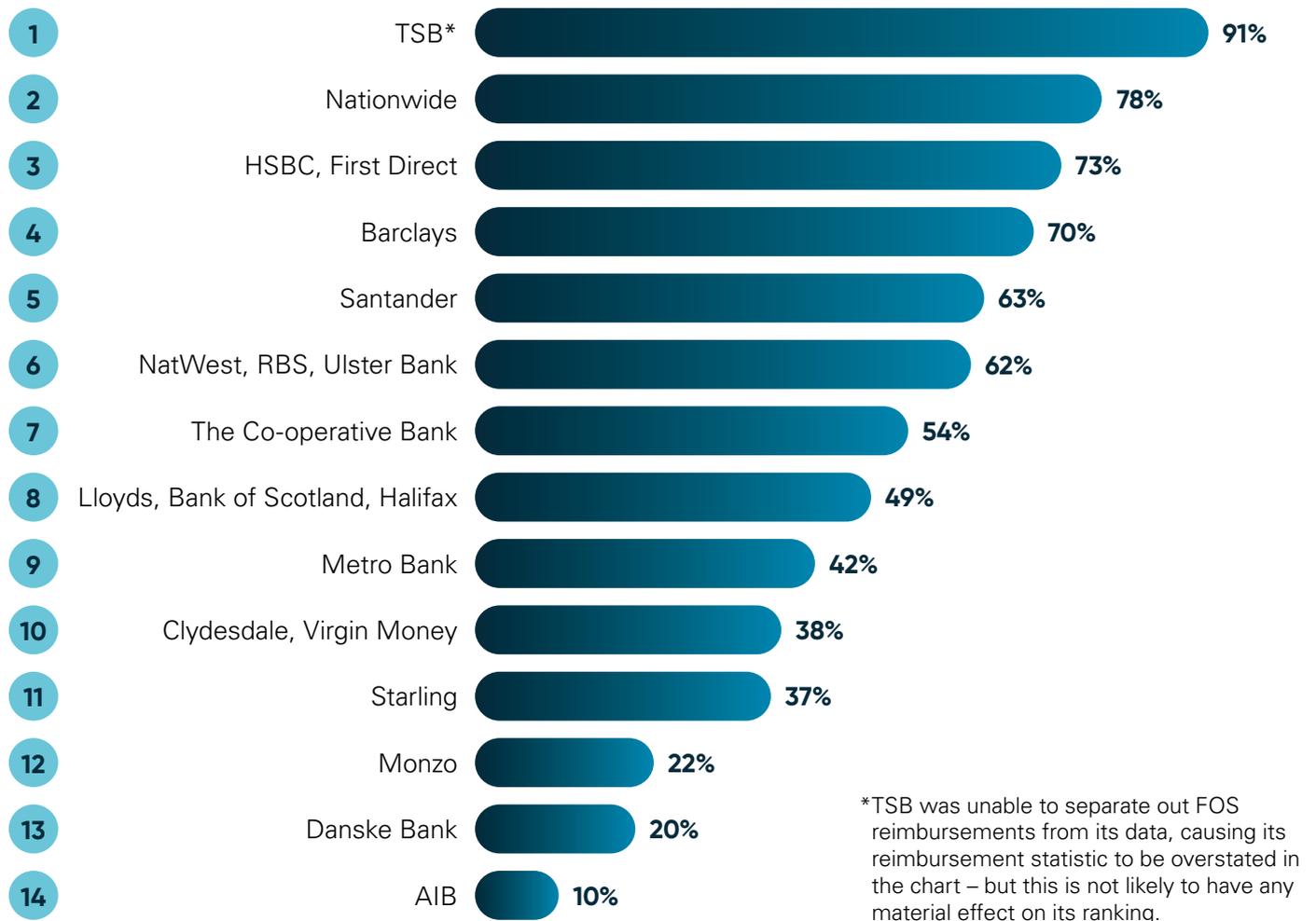
We would like to see those issues resolved at the time of the fraud rather than retrospectively. The best way for the cases to be resolved is for the sending and receiving firms to communicate at the time of the fraud.



<sup>2</sup> The Co-operative Bank, Barclays, Clydesdale/Virgin Money, HSBC, Lloyds Banking Group, Metro Bank, Nationwide, NatWest Group, Santander and Starling are the 10 members of the CRM code.

# Metric A: Percentage of reported APP fraud losses refunded by value

The chart shows the percentage of total APP fraud losses that were reimbursed to consumers by each firm in 2022. For example, TSB refunded 91% of the total value of APP fraud losses in 2022.



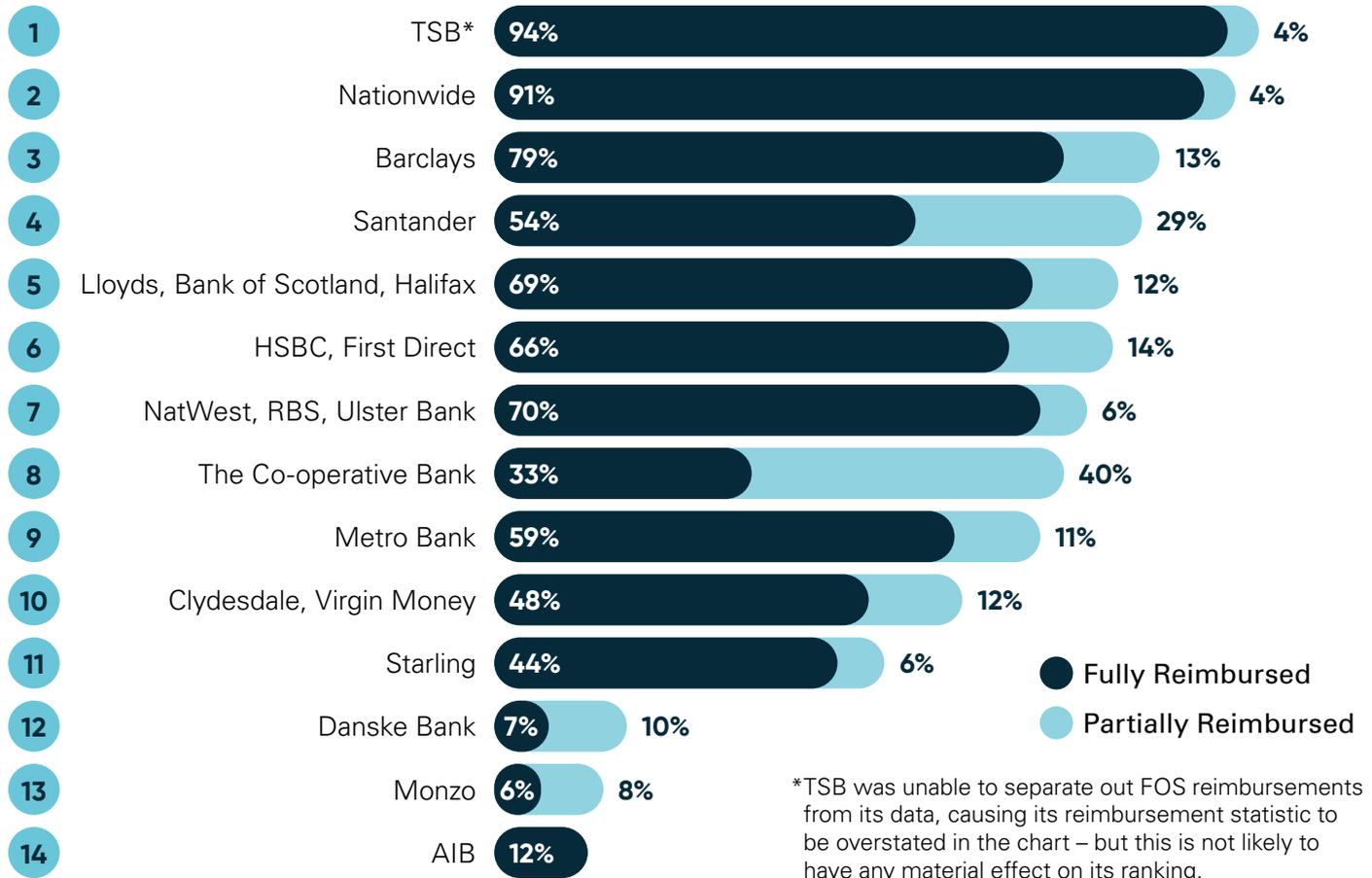
Currently PSPs are not required to reimburse victims of APP fraud.

However, in the last three years we have seen considerable progress in improving reimbursement for victims. The Contingent Reimbursement Model (CRM) code is a voluntary code launched in 2019 to establish good industry practice in preventing APP fraud and respond to its growth. As part of the Code, member PSPs reimburse victims of APP fraud. Since its introduction, we have seen positive outcomes for consumers with higher rates of reimbursement. However, it has not driven consistent outcomes, with reimbursement rates differing significantly across members.

AIB, Danske Bank, Monzo and TSB are the only four directed PSPs not in the CRM code.

# Metric A: Percentage of reported APP fraud losses refunded by volume

The chart shows the percentage of APP fraud cases that were fully and partially reimbursed by each firm. For example, Nationwide fully reimbursed 91% and partially reimbursed 4% of the APP fraud cases in 2022.



We have seen examples of industry innovation, notably from TSB and Nationwide who had the highest reimbursement levels of the major UK banks in 2022:

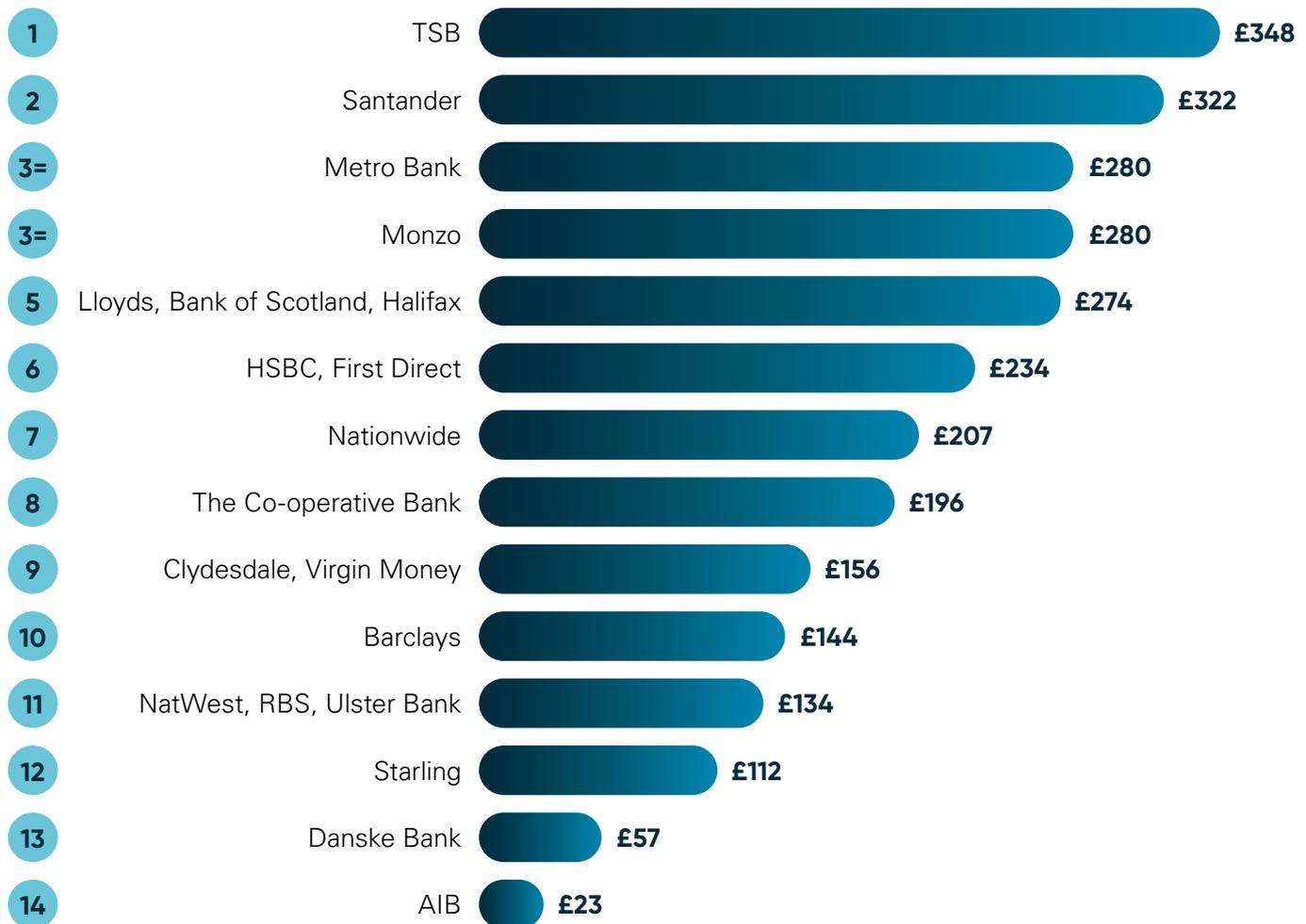
- ▶ Since 2019 TSB has offered a fraud refund guarantee. In most cases where a customer reports an APP fraud to TSB, they automatically reimburse the customer.
- ▶ Since 2021, Nationwide has provided a scam checker service. Customers can talk to Nationwide about a payment. If the service reviews a transaction that turns out to be fraudulent, Nationwide fully reimburses the customer unless the service advised them not to make the payment.

The rates of reimbursement for many firms are encouraging and it presents a positive cultural shift across the payments sector. We see different strategies and approaches by PSPs to reimbursement which could account for some having higher reimbursement rates than other PSPs. It could also account for differences in rates of cases accepted as being eligible for reimbursement and the level of responsibility borne by customers themselves (resulting in more partial payments).

We expect to see the rate of reimbursement increase with the introduction of the reimbursement requirement in 2024.

# Metric B: Value of APP fraud sent per £ million of transactions

This data shows how much money consumers at the 14 major UK banking groups lost to APP fraud for every million pounds of transactions sent. For example, for every £1 million of Santander transactions sent in 2022, £322 of that was lost to APP fraud.



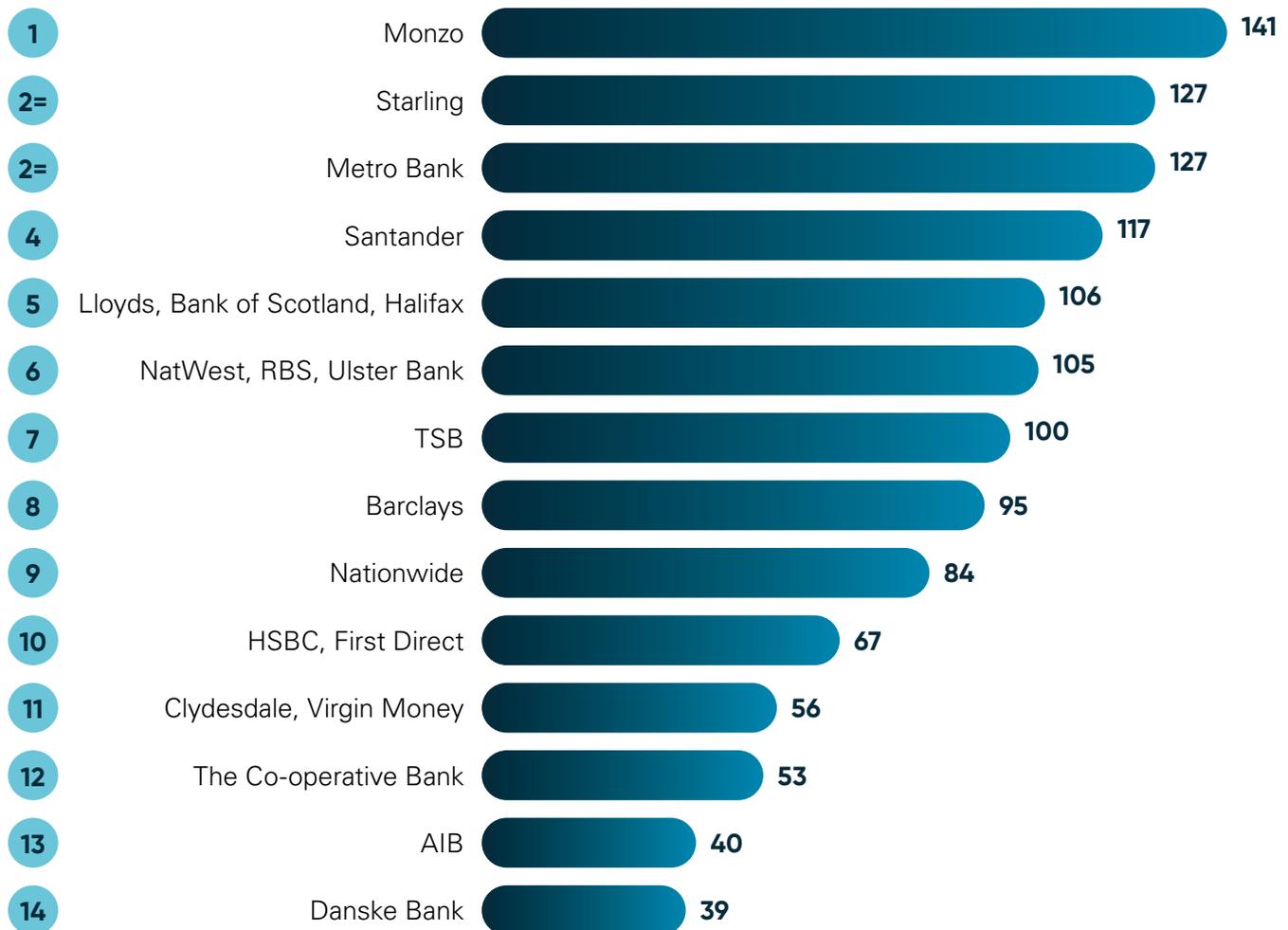
There is less variation between firms in the rate of fraud sent compared to the rate of fraud received. This suggests that directed PSPs are similarly likely to have customers that are victims of APP fraud.

The top four firms who report sending the highest rate of fraud – TSB, Santander, Metro and Monzo all perform similarly. The size of the firm does not appear to be a driver of performance with small and large firms distributed evenly. Neither does membership in the CRM code with both members and non-members identified as having high sending rates of APP fraud.

Differences that do exist between firms could be due to their approaches in processing and dealing with APP fraud reports as well as what they identify as being APP fraud.

# Metric B: Volume of APP fraud sent per million transactions

This data shows how many APP fraud payments were sent per million transactions at the 14 major UK banking groups. For example, for every million consumer transactions that Monzo sent in 2022, 141 were reported as APP fraud payments.



Monzo, Starling, Metro and Santander report sending the highest rates of APP fraud by volume in the industry while AIB and Danske Bank report sending the lowest.

Lloyds Group, NatWest Group, TSB and Barclays have average performance among the 14 PSPs with around 100 APP fraud cases per million transactions.

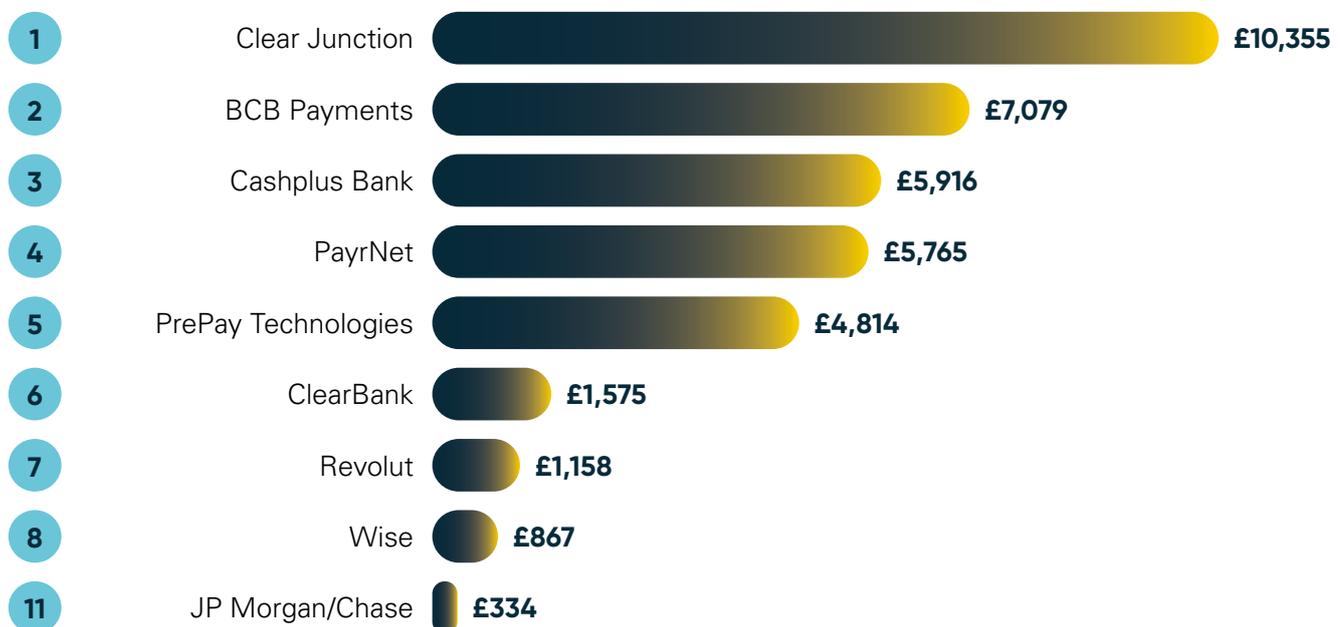
Of the 14 major UK banks, we see the highest rate being more than three times the lowest rate.

# Metric C: Value of APP fraud received per £ million of transactions

## Non-directed PSPs

This data shows which smaller banks and payment firms received the highest value of APP fraud in 2022 per million pounds of transactions. For example, for every £1 million received into consumer accounts at Clear Junction, £10,335 of it was APP fraud.

Firms in the chart were identified as being in the top 20 receivers of fraud by absolute value in the UK in 2022. Firms were then ranked from 1 to 20 on the basis of their fraud rate. A firm with rank 1 would have the highest APP fraud rate.



Non-directed PSPs are smaller banks and payment firms. They were not required to submit data to us on APP fraud due to their much smaller size compared to major UK banks.

	% share across all firms (value)	APP fraud	Faster Payments
Directed		63%	85%
Non-directed		37%	15%

In the following page we show which directed firms were identified in the top 20. We have separated the data on directed and non-directed PSPs as rates of fraud for non-directed PSPs tend to be much higher.

Tackling APP fraud is a journey. Some smaller banks and payment firms are in the much earlier stages of preventing fraud than major UK banks. The non-directed firms are not part of the CRM code which has focused members to think about how they process and deal with APP fraud. Typically fraud rates for non-directed firms in the top 20 receivers of APP fraud are much higher than those of the directed firms.

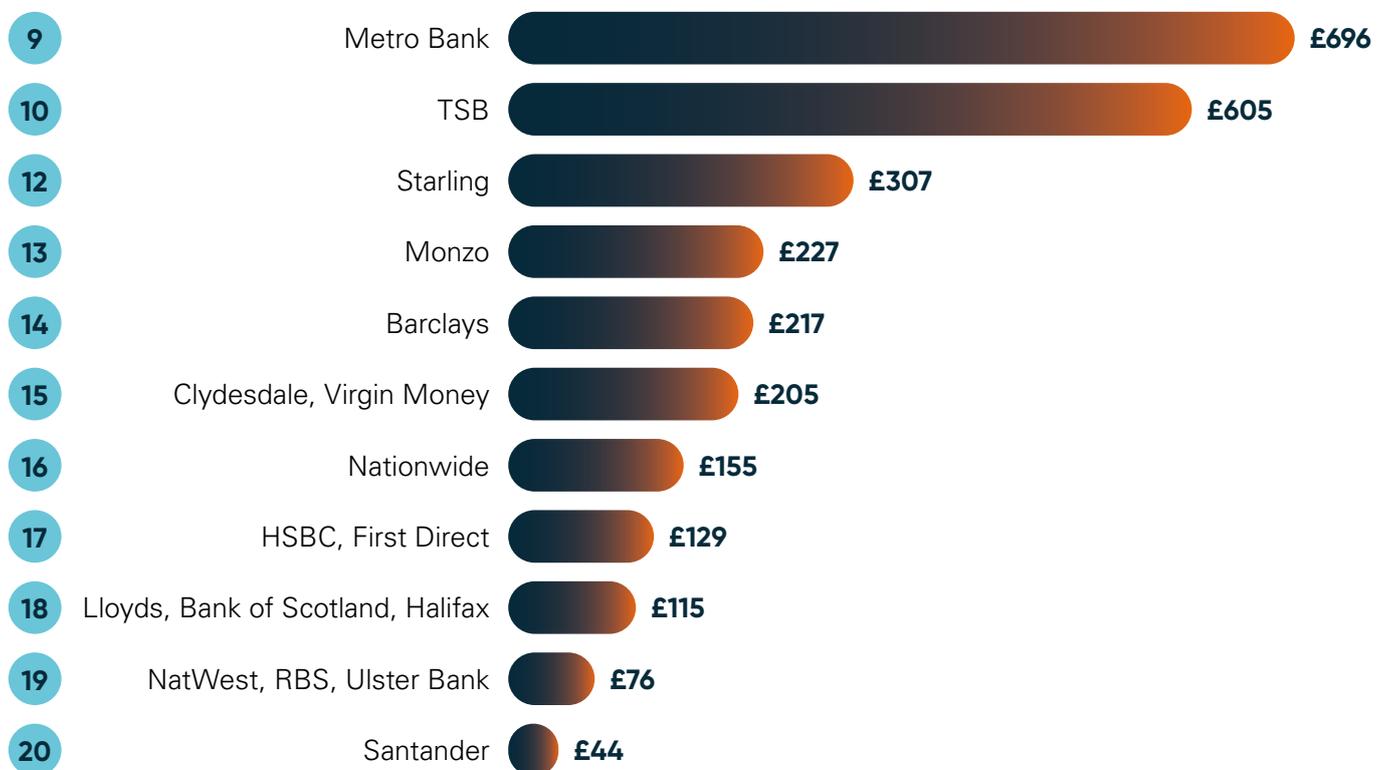
Some firms, such as ClearBank and PayrNet, provide payment accounts to customers but do not manage the customer relationship. Irrespective of whether the firms manage the customer relationships themselves or outsource this function, they retain the regulatory responsibility, and so we expect these firms to ensure their outsourced partners manage the risks of onboarding new customers, conducting identity checks and monitoring transactions effectively.

# Metric C: Value of APP fraud received per £ million of transactions

## Directed PSPs

This data shows which major UK banking groups received the highest value of APP fraud in 2022 per million pounds of transactions. For example, for every £1 million received into consumer accounts at Metro, £696 of it was APP fraud.

Firms in the chart were identified as being in the top 20 receivers of fraud by absolute value in the UK in 2022. Firms were then ranked from 1 to 20 on the basis of their fraud rate. A firm with rank 1 would have the highest APP fraud rate.



**i** AIB, Danske Bank and the Co-operative Bank are not included in this list, despite being directed PSPs. This is because they were not identified as being in the top 20 receivers of fraud.

Directed PSPs are the 14 major UK banking groups that were required to submit data on APP fraud. 11 of the 14 were identified as being in the top 20 firms receiving the highest absolute amount of APP fraud in 2022. Amongst major UK banks, there are still large variations in the amount of APP fraud received. Metro and TSB receive around twice as much APP fraud per million transactions compared to other directed PSPs.

% share across all firms (value)	APP fraud	Faster Payments
Directed	63%	85%
Non-directed	37%	15%

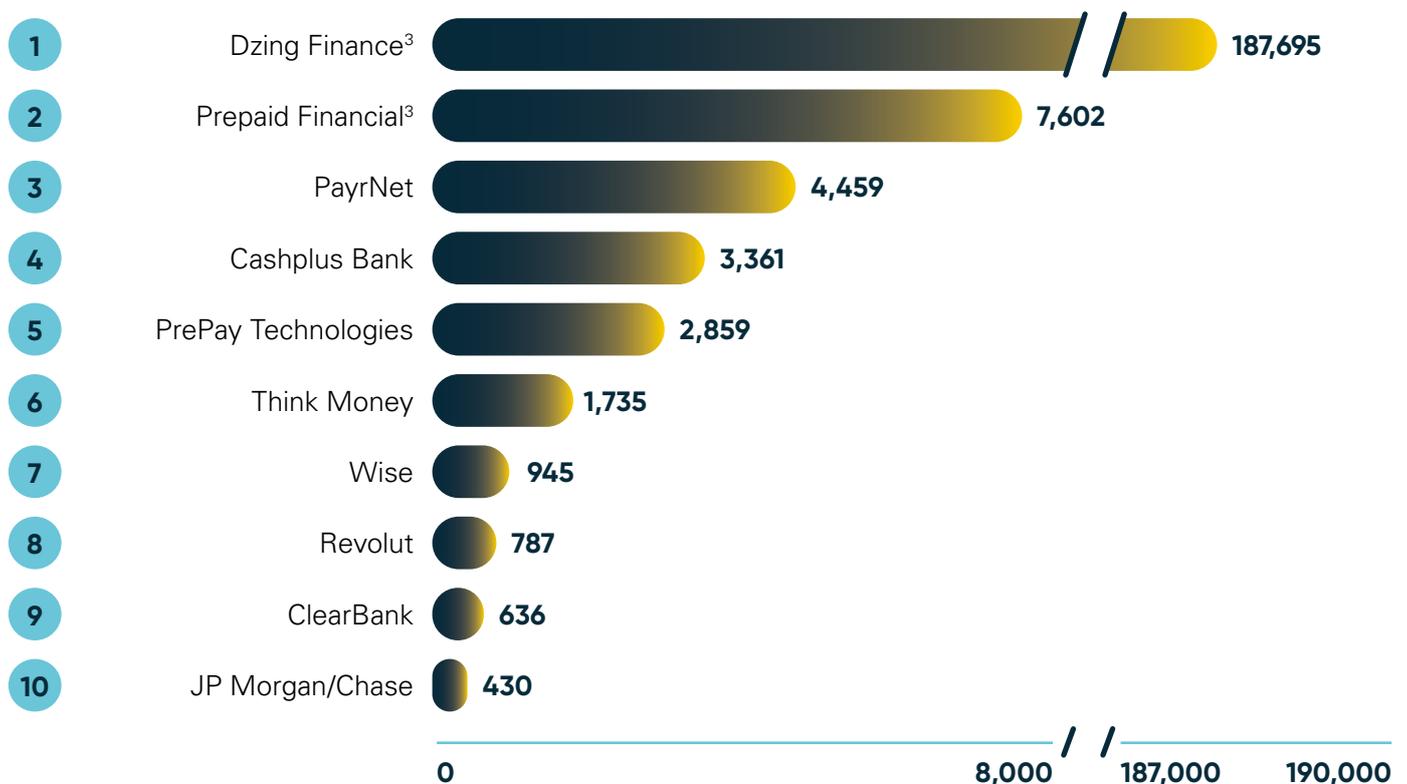
Reasons for some firms having higher rates of receiving fraud could include fewer or delayed onboarding checks, allowing the fraudster to open and close the account before they are caught, or weaknesses in inbound transaction monitoring.

# Metric C: Volume of APP fraud received per million transactions

## Non-directed PSPs

This data shows which small banks and payment firms received the highest number of APP fraud payments per million transactions. For example, for every 1 million transactions received by consumers at JP Morgan/Chase, 430 of those transactions were APP fraud payments.

Firms in the chart were identified as being in the top 20 receivers of fraud by absolute volume in the UK in 2022. Firms were then ranked from 1 to 20. A firm with rank 1 would have the highest APP fraud rate.



In 2022, Dzing Finance received the highest volume of fraud per million transactions in the UK.

Since 2022, a number of firms have taken significant steps to reduce APP fraud. This has been achieved by improving fraud controls.

Future publications of this data will show the impact these enhancements have made on reducing APP fraud.

10 non-directed PSPs were in the top 20 biggest receivers of fraud by volume in the UK.

Rates of fraud for non-directed PSPs are much higher than for directed PSPs.

	% share across all firms (volume)	APP fraud	Faster Payments
Directed		49%	94%
Non-directed		51%	6%

**i** In October 2023, the FCA published its findings on the measures that firms use to control and prevent money mule activity. The National Crime Agency defines a money mule as 'someone who lets someone else use their bank account to transfer money'.<sup>4</sup>

<sup>3</sup> Data has been extrapolated for Dzing and Prepaid Financial for comparative purposes and the actual volume is lower for both firms.

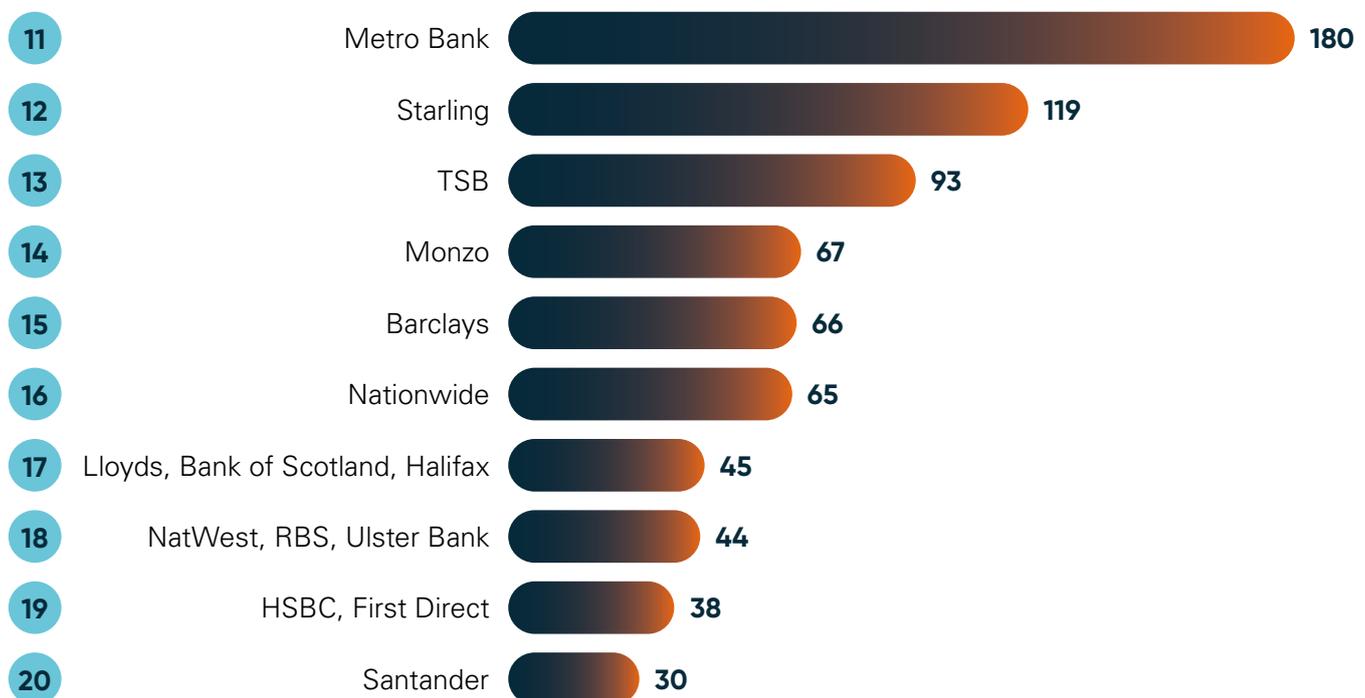
<sup>4</sup> National Crime Agency, [Money muling](#)

# Metric C: Volume of APP fraud received per million transactions

## Directed PSPs

This data shows which major UK banking groups received the highest number of APP fraud payments per million transactions. For example, for every 1 million transactions made by consumers at Starling, 119 of those transactions were APP fraud payments.

Firms in the chart were identified as being in the top 20 receivers of fraud by absolute volume in the UK in 2022. Firms were then ranked from 1 to 20. A firm with rank 1 would have the highest APP fraud rate.



AIB, Danske Bank, the Co-operative Bank and Clydesdale/Virgin Money are not included in this list despite being directed PSPs. This is because they were not identified as being in the top 20 receivers of fraud.

The chart above shows which of the 14 directed banking groups are in the top 20 list of the highest receivers of fraud in the UK. Of the directed firms, Metro and Starling received the highest volume of frauds per million transactions. However, even the highest receiving directed PSPs, Metro and Starling, received substantially fewer APP frauds per million transactions compared to the highest receiving non-directed PSPs (see previous page). The directed PSPs that received the lowest rate of APP fraud by volume were AIB, Danske Bank, the Co-operative Bank and Clydesdale/Virgin Money.

% share across all firms (volume)	APP fraud	Faster Payments
Directed	49%	94%
Non-directed	51%	6%

# What are we doing to drive better performance and improve outcomes for consumers?

## The PSR has adopted a multi-pronged approach to tackling APP fraud across payment systems



We will monitor the performance of all firms through the data that we collect. We will work with the FCA to address any poor performance through targeted action plans which will help drive better outcomes for consumers. Our regulatory partner, the FCA, has made it a business plan priority to stop an increase in APP fraud.



### We are introducing a new reimbursement requirement in 2024

This will incentivise the industry to invest further in end-to-end fraud prevention by making payment firms meet the cost of reimbursement.

This will increase customer protections so most victims of APP fraud are swiftly reimbursed, boosting confidence in the UK payments ecosystem.



### Enhanced information sharing

We tasked industry with improving intelligence-sharing between PSPs so they can improve scam prevention in real time, e.g. stopping or delaying high risk payments. We expect PSPs to implement the capability for intelligence sharing in Q1 2024.



### Confirmation of Payee (CoP)

In August 2019, we directed the six largest banking groups to implement the name checking service, CoP. In October 2022, we expanded the requirement to provide the service to include approximately 400 additional firms. CoP has helped to curtail the increase of some types of APP scams. **By October 2024, nearly all consumer payments will be covered by CoP.**



### Protection of payment systems

We want Pay.UK, as the independent payment system operator, to run Faster Payments in a way that ensures customers are protected, and fraud is prevented from entering the system. We want to give Pay.UK a stronger role to lead the development of protections for payment system users.



### Origination of APP scams data

We will consider how we can collect data which shows where APP fraud originates. We want this data to raise awareness of platforms, such as social media and telecoms firms that are at most risk of being targeted by fraudsters.

# Summary of performance

The table shows 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)
	<i>A lower number is better – i.e. a rank of 1st is the 'best'</i>		<i>A higher number is better – i.e. a rank of 14th is the 'best'</i>		<i>A higher number is better – i.e. a rank of 20th is the 'best'</i>	
<b>Directed PSPs</b>						
AIB	14	14	14	13		
The Co-operative Bank	7	8	8	12		
Danske Bank	13	12	13	14		
Barclays	4	3	10	8	14	15
Clydesdale, Virgin Money	10	10	9	11	15	
HSBC, First Direct	3	6	6	10	17	19
Lloyds, Bank of Scotland, Halifax	8	5	5	5	18	17
Metro Bank	9	9	3	3	9	11
Monzo	12	13	4	1	13	14
Nationwide	2	2	7	9	16	16
NatWest, RBS, Ulster Bank	6	7	11	6	19	18
Santander	5	4	2	4	20	20
Starling	11	11	12	2	12	12
TSB	1	1	1	7	10	13
<b>Non-directed PSPs</b>						
BCB Payments	–	–	–	–	2	
Cashplus Bank	–	–	–	–	3	4
Clear Junction	–	–	–	–	1	
ClearBank	–	–	–	–	6	9
Dzing Finance	–	–	–	–		1
JP Morgan/Chase	–	–	–	–	11	10
PayrNet	–	–	–	–	4	3
Prepaid Financial	–	–	–	–		2
PrePay Technologies	–	–	–	–	5	5
Revolut	–	–	–	–	7	8
Think Money	–	–	–	–		6
Wise	–	–	–	–	8	7

● Firm not identified in the top 20

● Data not requested by us

# Total fraud

The table shows the total volume and values of fraud sent by the 14 directed banks.

	Fraud sent		
	Total value	Total volume	Total value reimbursed
Directed PSPs	£389,022,456	385,964	£237,219,623

The table shows the total volume and values of fraud received by PSPs identified as the top 20 receivers of fraud.

	Fraud received	
	Total value	Total volume
Directed PSPs	£225,945,224	185,322
Non-directed PSPs	£93,885,883	160,213

# Technical annex

While there are discrepancies in the data between sending and receiving banks, we have looked at the materiality and found that it was such that it didn't change the rankings in any case.

## Data notes

---

### Metric A

Barclays, Lloyds and Metro included FOS cases in their reimbursed case **volumes**. We made manual adjustments to remove these from the final reimbursement statistics. These PSPs were only able to provide us with the total number of APP fraud cases that went to the FOS in 2022, not the split of which cases were partially and fully reimbursed. To subtract the FOS cases from the overall volume figures, we used the existing proportion of partial and fully reimbursed cases in the original data to make the adjustments.

TSB was unable to separate out FOS reimbursements from its total reimbursement data (for case **volume and value**). While this causes its reimbursement statistics to be overstated in the charts, it is not likely to have an impact on its Metric A rankings. Among the PSPs who submitted FOS data to us, FOS reimbursements by value were found to have a maximum of 9% additional effect on the reimbursement statistic – so it is likely that TSB would maintain its number 1 ranking even if FOS reimbursements were excluded. Similarly, FOS reimbursements by volume were found to have a maximum of 1.4% additional effect on fully reimbursed cases and 0.4% on partially reimbursed cases, making it likely that TSB would maintain its number 1 Metric A volume ranking even if FOS reimbursements were excluded from its data.

---

### Metric B

Nothing to note.

---

### Metric C

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.

As firms improve the way they capture data on APP scams for future cycles, we would expect the consistency between these metrics to improve.

Consumer Faster Payments values and volumes were used to calculate the fraud rates in Metric C. We have made adjustments to the consumer Faster Payments data in the case of some PSPs where this data was inconsistently reported by sending banks, especially where indirect PSPs were the receiving firms.

We subtracted any money recovered and returned to the victims when calculating the receiving PSP's APP fraud value rates for Metric C.

---

# Glossary

Concept	Definition
<b>authorised push payment (APP) fraud payment</b>	<p>A payment made as part of an APP fraud. The new reimbursement requirement applies to payments executed by the sending PSP, in accordance with an authorisation given by its customer, to an account controlled by a person other than the customer, where the customer has been deceived into granting that authorisation as part of an APP fraud case. This includes where:</p> <ul style="list-style-type: none"> <li>▶ the payer intends to transfer the funds to a person other than the recipient, but is deceived into transferring the funds to the recipient</li> <li>▶ the payer intends to transfer the funds to the recipient but is deceived as to the purposes for which they are transferring the funds</li> </ul>
<b>directed PSP</b>	<p>A PSP subject to this direction that submits data on:</p> <ul style="list-style-type: none"> <li>▶ APP fraud sent from its accounts</li> <li>▶ which PSPs are receiving that APP fraud</li> <li>▶ reimbursement of APP fraud losses suffered by its customers</li> </ul>
<b>Faster Payments</b>	<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. Over 90% of APP fraud losses occur over Faster Payments, based on UK Finance data.</p>
<b>indirect PSP</b>	<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 indirect.<sup>5</sup></p>
<b>payment service provider (PSP)</b>	<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>
<b>receiving PSP</b>	<p>The payment service provider that operates the ultimate account into which a payment is received. This is where the fraudster is holding their account.</p>
<b>sending PSP</b>	<p>The payment service provider that operates the account from which a payment is sent. This is where the victim of APP fraud is holding their account.</p>

<sup>5</sup> UK Finance, [Access to Payments Systems](#) (July 2023).

# Entity legal names

Firm names and brands	Legal entity/parent group
AIB	AIB Group (UK) plc
Barclays	Barclays Bank UK plc
BCB Payments	BCB Payments Limited
Cashplus Bank	Advanced Payment Solutions Limited
Clear Junction	Clear Junction Limited
ClearBank	ClearBank Limited
Clydesdale, Virgin Money	Clydesdale Bank plc/Virgin Money UK plc
The Co-operative Bank	The Co-operative Bank plc
Danske Bank	Northern Bank Limited
Dzing Finance	Dzing Finance Limited
HSBC, First Direct	HSBC UK Bank plc
JP Morgan/Chase	J.P. Morgan Europe Limited
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
PayrNet	PayrNet Limited
Prepaid Financial	Prepaid Financial Services Limited
PrePay Technologies	PrePay Technologies Limited
Revolut	Revolut Limited
Santander	Santander UK plc
Starling	Starling Bank Limited
Think Money	Think Money Limited
TSB	TSB Bank plc
Wise	Wise Payments Limited

© The Payment Systems Regulator Limited 2023

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

Telephone: 0300 456 3677  
Website: [www.psr.org.uk](http://www.psr.org.uk)