OPEN BANKING
The Standard for Open Innovation™

Open Banking Payments Fraud Monitor

Monitoring fraud trends within Open Banking payments covering data from March 2024 to March 2026

Authors:
Christian Delesalle OBL Head of Customer Success
Nick Davey OBL Head of Strategy
Data: Anton Joachim OBL Data Scientist

June 2026 Edition

CONTENTS

Foreword from the CEO	3
Executive Summary	4
Chapter 1 – Introduction	5
Chapter 2 – Comparison to Payments Industry Data	7
Chapter 3 – Latest OB Fraud Trends and Learnings	8
Chapter 4 – Anecdotal information from ASPSPs	13
Appendix 1 – OBL Data Submission Template	16
Appendix 2 – Industry data sources	17

Open Banking Payments Fraud Monitor – June 2026 Edition

Foreword from the CEO

Fraud is not a victimless crime. Behind every case is a person, family or business dealing with financial loss, disruption and the very real emotional toll that fraud can take. Across the UK, millions of people are affected by fraud every year. Preventing it is a shared responsibility and a collective goal for our industry.

With this in mind, I am pleased to introduce the first edition of the Open Banking Payments Fraud Monitor, Open Banking Limited's (OBL) twice-yearly assessment of fraud within Open Banking payment journeys.

This publication builds on our Financial Crime in Open Banking Journeys reports, published in December 2024[1] and December 2025[2]. It reflects our continued commitment to providing transparent, consistent and evidence-based insight that supports the safe and trusted growth of Open Banking payments within the wider payments landscape.

The Monitor draws on data from account providers representing more than 60% of Open Banking payment volumes. It provides a consistent view of fraud trends and helps us understand how those risks are evolving as adoption continues to grow. It also compares our fraud rates with wider UK payments industry benchmarks, providing important context for discussions taking place across the financial services sector.

This edition offers reasons for both confidence and caution. Open Banking continues to compare favourably with wider payment channels, reflecting the benefits of strong standards, security and collaboration across the industry. Yet the picture is far from static. Authorised Push Payment fraud remains a significant challenge and the tactics that criminals use continues to evolve, becoming more sophisticated, more convincing and harder to detect. Fraudsters adapt quickly. Our response must be just as determined.

Every fraud statistic represents a real incident that affected someone. While the numbers help us measure the scale and direction of the challenge, they also remind us that fraud remains a very human problem.

By sharing insight, learning from trends and working together across the industry, we can strengthen protections, support more effective fraud prevention and reinforce the trust that underpins Open Banking payments.

At OBL, we set the standard for open innovation. Trust is fundamental to that mission. By working together to tackle fraud, we can help ensure Open Banking continues to grow in a way that is safe, secure and beneficial for consumers and businesses alike.

Henk Van Hulle
Chief Executive Officer
Open Banking Limited

[1] OBL publishes JROC report: Financial Crime within Open Banking journeys - Open Banking
[2] Financial Crime Report - December 2025

Open Banking Payments Fraud Monitor – June 2026 Edition

Executive summary

The Open Banking Payments Fraud Monitor builds on OBL's Financial Crime in Open Banking Journeys publications, first published in December 2024 and followed by a second edition in December 2025. Covering data from March 2024 to March 2026 it combines quantitative analysis from ASPSPs, representing over 60% of payments initiated using Open Banking, with qualitative feedback from providers. We show how fraud in Open Banking compares with the wider industry, how recent fraud patterns are evolving, and where firms are seeing emerging risks and opportunities to strengthen prevention.

Key Findings

1. OB fraud vs. industry (Full Year 2025): OB fraud remains lower than the wider industry by volume, with around 1 in 6,000 OB payments fraudulent compared to around 1 in 2,500 payments for the wider industry (0.017% vs. 0.043%). Fraudulent payments are higher by value between OB initiated and wider industry (0.035% vs. 0.026%), with a higher fraudulent average transaction value (£785 vs. £266). We anticipate this is explained by OB being used more often for higher-value payment journeys, including account transfers and investment-related payments, rather than significant lower-value purchases seen in broader industry data.

2. Latest OB fraud trends (Q1 2026): Fraud volume rose to 0.024% (around 1 in 4,200) in Q1 2026, up from both the previous quarter and the same period last year, marking a return to earlier levels after the low seen in Q1 2025. APP fraud still accounts for more than two thirds of reported cases and remains the main driver of overall risk. Business fraud rates remain materially below consumer rates, VRPs continue to show lower fraud than single immediate payments, and app journeys continue to show lower fraud than browser-authenticated journeys, although app fraud is growing faster. Fraud by value eased slightly in Q1 2026 but remained above prior-year levels, while average losses per case fell to £676, indicating more frequent but lower-value cases in the latest quarter.

3. What firms are seeing on the ground: Anecdotal feedback suggests fraud is evolving in sophistication rather than changing fundamentally. ASPSPs report that social engineering remains the main driver of OB fraud, with investment scams, impersonation scams, smishing, phishing, newer pay-by-link and fake refund scams featuring in recent cases. They report that growth in fraud is broadly tracking growth in OB payment volumes (which is increasing year-on-year), but also highlighted how newer payment journeys, merchants new to Open Banking, and use of business accounts on the recipient leg of fraud use can create new vulnerabilities. Newer scam sophistication increasingly blurs the line between authorised and unauthorised fraud, where it is unclear at the point that the victim loses control of their accounts or their funds. At the same time detection and prevention continues, some banks are beginning to see benefits from more targeted detection and richer data-sharing, supporting the case for broader use of tools such as Transaction Risk Indicators (TRIs).

Chapter 1 – Introduction

Background to Open Banking

Open Banking is a simple, secure way to help you move, manage and make more of your money. It facilitates two different types of activity: it enables consumers and businesses to access and use their payment account data, and it allows the initiation of payments from consumers' payment accounts.

For payments; Open Banking is an overlay system where payments are initiated using Payment Initiation Service Providers (PISPs) and payers accounts over UK payment systems such as Bacs, CHAPS and Faster Payments. The majority of payments are made across Faster Payments. PISPs are able to provide innovative, quick and low friction payment solutions to businesses and consumers using Open Banking technology.

We anticipate at least 1 in 5 UK residents use Open Banking on a regular basis. There are over 18 million user connections, demonstrating the growing adoption of Open Banking services by UK consumers and small businesses. There are currently over 40 million payments[3] initiated using Open Banking each month. While customers and businesses benefit from the use of Open Banking, fraudsters and criminals are also able to manipulate customers into giving their credentials away, or to use Open Banking products and services when perpetrating authorised push payment (APP) fraud.

This edition of the Monitor focusses on financial crime within Open Banking payment initiation journeys.

Background to financial crime

Financial crime is usually split between authorised fraud and unauthorised fraud. Authorised fraud is where a victim is tricked into sending money to fraudsters who then move the money. Unauthorised fraud is where a criminal gains access to a consumer's account and moves money from it, typically to an account in their control.

Unauthorised fraud

Unauthorised fraud occurs when criminals are able to gain access to a victim's account online or via a banking app. This may be a password, code or other form of identification that a criminal has access to. Some Open Banking PISP propositions may benefit fraudsters because they are aimed at making payments easier and quicker than alternatives, so fraudsters can use passwords or other login arrangements to quickly move money from a victim's account.

Unauthorised fraud is also seen in debit and credit cards, where cards are stolen, or the electronic card details are scammed, and the cards and/or card information are used to make purchases which the victim didn't authorise.

Authorised push payment fraud (APP fraud)

Authorised fraud occurs when a victim is tricked into making one, or many, payments to fraudsters typically by way of some form of malicious deception.

[3] Open Banking Payments Monthly Performance Update

There is a wide range of APP frauds. Below is a non-exhaustive list of different types:

- **Purchase scams** – victims paying for goods with e-commerce merchants or marketplaces, where the goods do not exist.
- **Impersonation scams** – where a fraudster impersonates a bank or public authority to pretend to the victim that their savings are at risk. This results in the victim being persuaded to move the money to a 'safe account', under the fraudster's control.
- **Romance scams** – fraudsters posing as genuine individuals on dating websites, then conning victims out of their money.
- **Investment scams** – fake investment websites or investment brokers which persuade victims to make what they believe is a genuine investment, only to find out their money was never invested.

APP fraud is most prevalent in Faster Payments transactions, compared with other payment methods. Open Banking is one way of initiating Faster Payments.

Background and methodology

In 2024, OBL started to collect data from ASPSPs, such as banks, and other PSPs on the basis of monitoring and helping to prevent financial crime in Open Banking payment journeys.

For this edition of the Monitor, we analysed fraud data provided by a range of ASPSPs including some of the big six GB banking groups, fintech ASPSPs and other smaller providers. We look at the messages and trends from the data in Chapter 2 and look at information gathered from speaking to ASPSPs in Chapter 3.

We have found that Open Banking fraud is also split between authorised and unauthorised typologies, with some overlaps between the two. Some ASPSPs have seen a higher prevalence of unauthorised fraud compared to APP fraud, and others vice versa. We explore these trends in more detail below.

We thank all the companies that provided data, and those that have spoken to us about fraud. We note that the Open Banking ecosystem is unified in the interests of preventing fraud, and the effects of fraud on individuals, society and the UK's economic health.

Transaction risk indicators (TRIs)

OBL has been working with industry in developing information passed between PISPs and ASPSPs when initiating a payment. This shared information set is referred to as Transaction Risk Indicators (TRIs), which are a block of data fields that PISPs can populate to indicate key information to the ASPSP such as the nature and purpose of the transaction, whether the PISP has a contract with the merchant, and the relationship between the PISP and the merchant. To understand their impact, select PISPs and ASPSPs have been involved in a live pilot. This has now concluded, and findings indicate that TRIs would be an effective tool in identifying fraudulent payments originated through Open Banking, but also importantly minimising false positives e.g., payments that may appear to be suspect but are, in fact, genuine.

OBL agrees that the best way to combat fraud within payment journeys is the better exchange and use of data and tools that more accurately spot fraud. TRIs are one such data delivery element that can help in the fight against fraud.

Chapter 2 – Comparison to Payments Industry Data

	Volume				Value				
OB Fraud Category	OB Fraud Cases	OB Fraud Payment Volume	% OB Fraud - Volume	% Industry Fraud - Volume	OB Fraud Value	% OB Fraud - Value	% Industry Fraud - Value	Average OB Fraud Transaction Value	Average Industry Fraud Transaction Value
Total	**12,787**	**42,142**	**0.017%**	**0.043%**	**£33,081,727**	**0.035%**	**0.026%**	**£785**	**£266**
Fraud Type:									
APP Fraud	9,550	30,594	0.013%	0.006%	£27,356,101	0.029%	0.012%	£894	£948
Unauthorised Fraud	3,237	11,548	0.005%	0.037%	£5,725,625	0.006%	0.014%	£496	£163
Customer Type:									
Consumer	12,650	41,906	0.018%		£32,608,139	0.039%		£778	
Business	137	236	0.004%		£473,587	0.004%		£2,007	
Payment Type:									
Single	12,320	40,731	0.019%		£32,477,097	0.036%		£797	
VRP	467	1,411	0.005%		£604,630	0.017%		£429	
ASPSP Authentication Type:									
App	9,843	32,742	0.019%		£25,778,786	0.043%		£787	
Browser	1,335	4,305	0.037%		£3,442,210	0.023%		£800	
Unknown	1,609	5,095	0.009%		£3,860,731	0.019%		£758	

Figure 1 - Full year 2025 OB fraud compared with latest industry data for the same period

Figure 1 compares Open Banking fraud rates (by volume and value) and average transaction value (ATV) for 2025 with the latest available industry benchmarks. See the end of this section for a full list of industry data sources used in the comparison.

On a volume basis, the Open Banking fraud rate (0.017%) is below the industry comparator (0.043%). On a value basis, the Open Banking fraud rate (0.035%) is above the industry comparator (0.026%), and the average transaction value for Open Banking fraud (£785) is also higher than the industry benchmark (£266).

This difference may partly reflect variation in underlying use-case mix. Open Banking is used relatively more often for higher-value transactions, such as account transfers and investments, whereas the industry comparator may be more heavily weighted towards lower-value transactions via card.

Chapter 3 – Latest OB Fraud Trends and Learnings

Data collection and analytics background

Submissions received for the period from March 2024 to March 2026 cover six ASPSP groups and eleven ASPSP brands. Respondents are a combination of ASPSPs in the CMA9 group and non-CMA9 ASPSPs.

These data providers are used to initiate over 60% of all Open Banking payments (note: the full market is defined here as Open Banking payments made from a payment account at a CMA9 ASPSP or at a non-CMA9 ASPSP submitting data to us). While this does not represent the full population of ASPSPs, we consider it a useful and representative sample covering large banks, smaller banks and neobanks.

This chapter presents analysis of the data, including trend analysis and breakdowns. Appendix 2 also includes a comparison of full-year Open Banking fraud data against industry benchmarks for the same period.

In addition to the data collected, we have spoken to a group of ASPSPs to gather further insight and context on the data provided. These sessions also served as an opportunity to explore views on Open Banking fraud more broadly. We cover the anecdotal insights in Chapter 3.

What are the headlines and trends we've observed?

Q1 2026 Fraud Summary

	% OB Fraud - Volume			% OB Fraud - Value			Average Fraud Transaction Value		
	% OB Fraud - Volume	QoQ Change	YoY Change	% OB Fraud - Value	QoQ Change	YoY Change	OB Fraud ATV	QoQ Change	YoY Change
Overall	**0.024%**	**+0.003%**	**+0.012%**	**0.040%**	**-0.020%**	**+0.022%**	**£676**	**-£275**	**-£29**
Fraud Type:									
APP Fraud	0.017%	+0.002%	+0.009%	0.034%	-0.019%	+0.020%	£798	-£354	£46
Unauthorised Fraud	0.007%	+0.001%	+0.004%	0.006%	-0.000%	+0.002%	£362	-£20	-£215
Customer Type:									
Consumer	0.024%	+0.003%	+0.013%	0.046%	-0.021%	+0.025%	£672	-£270	-£27
Business	0.003%	-0.002%	-0.001%	0.003%	-0.005%	-0.000%	£1,816	-£1,162	£445
Payment Type:									
Single	0.026%	+0.003%	+0.014%	0.041%	-0.021%	+0.023%	£691	-£276	-£32
VRP	0.007%	+0.002%	+0.001%	0.014%	-0.007%	-0.003%	£256	-£233	-£130
ASPSP Authentication Type:									
App	0.029%	+0.004%	+0.017%	0.049%	-0.031%	+0.030%	£632	-£331	-£8
Browser	0.038%	+0.001%	+0.009%	0.031%	-0.016%	+0.016%	£1,148	-£132	£350
Unknown	0.007%	-0.001%	-0.000%	0.017%	+0.001%	-0.002%	£720	£132	-£239

QoQ (Quarter-on-Quarter) Change is the current period's measure minus the measure for the period 3 months prior. QoQ Change for Q1-2026 is the change since Q4-2025.
YoY (Year-on-Year) Change is the current period's measure minus the measure for the period 3 months prior. YoY Change for Q1-2026 is the change since Q1-2025.

Figure 2 - Q1 2026 OB Fraud Summary

Figure 2 shows a summary of fraud rates in volume and value, as well as an average transaction value for Q1 2026, together with comparisons with the previous quarter (Q4 2025) and the same period last year (Q1 2025).

Q1 Fraud Volume

- Fraud volume as a proportion of total payment volume increased marginally to 0.024% in Q1 2026, up 0.003 percentage points from the previous quarter and 0.012 percentage points year on year. This continues the upward trend observed over the past 12 months, following a historic low in Q1 2025 and indicating a return to earlier levels.

- APP fraud remains the dominant typology, accounting for more than two thirds of total reported fraud. In Q1 2026, the APP fraud rate by volume was 0.017%, compared with 0.007% for unauthorised fraud.

- By customer type, the consumer fraud rate by volume was 0.024% in Q1 2026, materially above the equivalent business rate of 0.003%. Consumer fraud rates have increased over time, whereas business fraud rates have improved; however, business transaction volumes remain comparatively low and therefore have only a limited effect on the aggregate fraud rate.

- Fraud remains higher on single immediate payments (0.026%) than on variable recurring payments (VRPs) (0.007%), with the rate on single payment fraud also increasing more quickly over time – more than doubling compared to the same period last year.

- Browser-authenticated journeys continue to exhibit a higher fraud rate than app-authenticated journeys, although fraud in app-authenticated journeys is growing more quickly, suggesting a shift in the mix of observed fraud.

Q1 Fraud Value

- Fraud rate by value stood at 0.40% in Q1 2026, down 0.020 percentage points quarter-on-quarter, but 0.022 percentage points above the level recorded in the same period a year earlier.
- Quarter-on-quarter movements in fraud value were primarily driven by APP fraud, which reduced over the quarter (from 0.054% to 0.034%) but remained above prior-year levels. Unauthorised fraud by value was comparatively stable.
- Average transaction value (ATV) for fraudulent payments dropped to £676 in Q1 2026, a reduction of £275 over the quarter. This decrease was driven mainly by smaller APP and app-authenticated fraud ATV.

Quarterly Trends

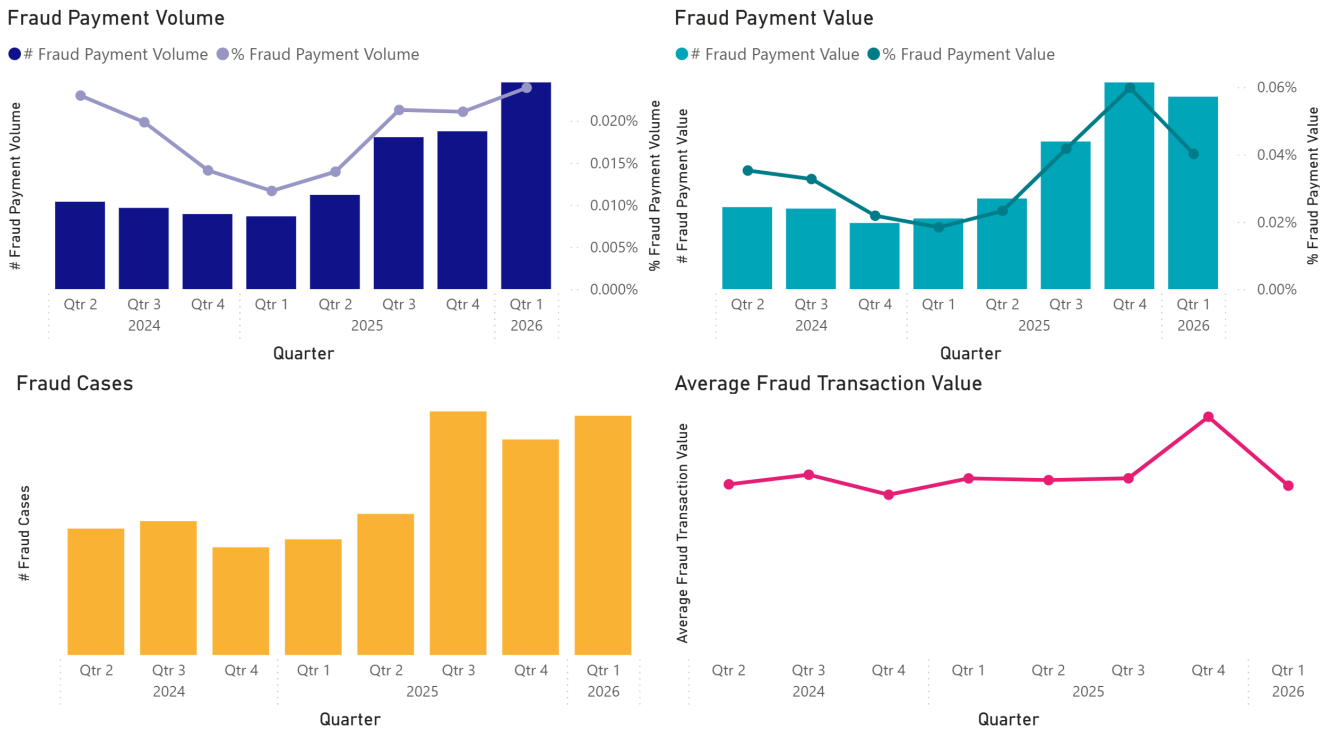

Figure 3 - Quarterly trends Q2 2024 – Q1 2026

Figure 3 shows quarterly trends in fraud volumes, values, rates and ATV. It illustrates the longer-term trends in fraud.

- Fraud rate by volume reduced from 0.023% in Q2 2024 to 0.012% in Q1 2025, but has increased to a high of 0.024% in Q1 2026.
- In the last three quarters (Q3 2025 to Q1 2026), the fraud rate by value has been the highest on record. However, fraud value decreased in Q1 2026 compared with the previous two quarters.

Monthly Trends

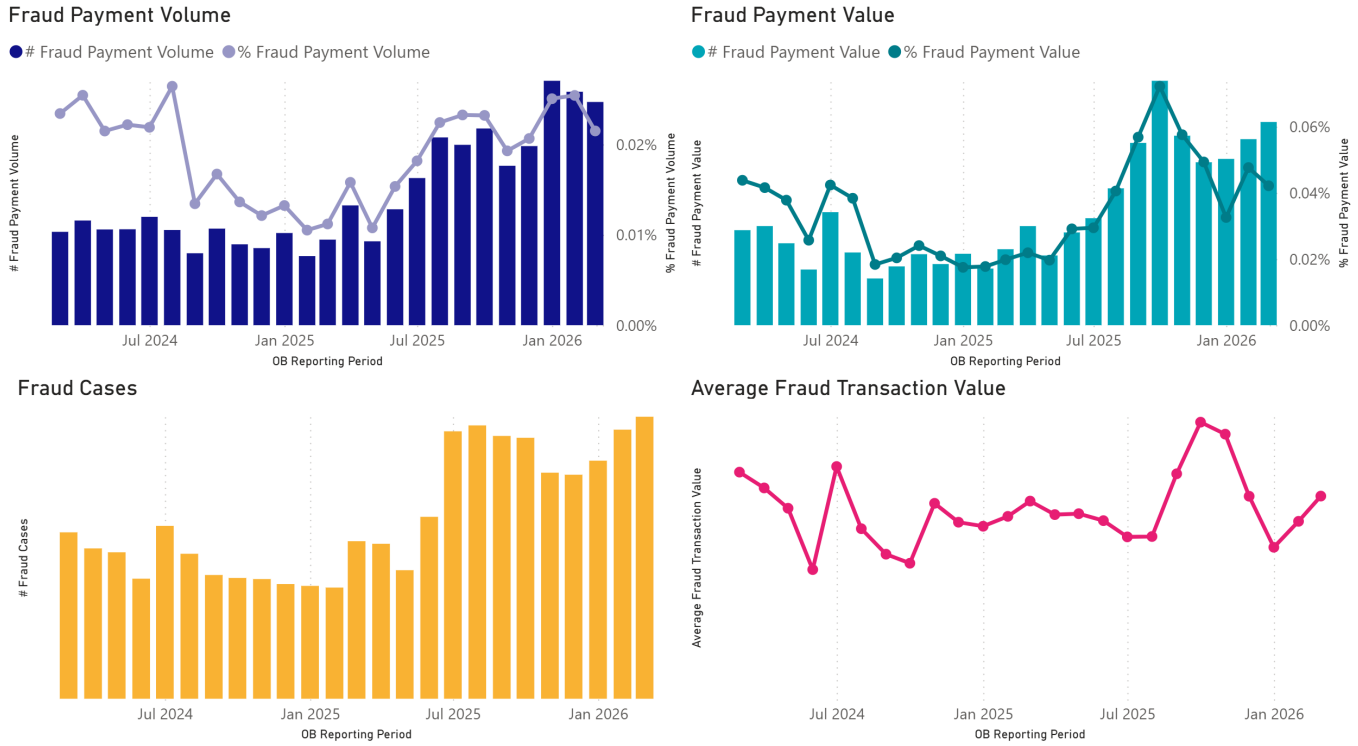

Figure 4: Monthly fraud trends March 2024 - March 2026

Figure 4 illustrates the monthly trend in fraud volumes, values, cases and ATV, providing a more granular view of fraud trends.

- Data indicates that fraud volumes were elevated during the first two months of 2026, with some moderation visible in March.
- Despite a reduction in fraud volume rates in March, fraud cases remained elevated in that month, indicating lower exposure per case on average.
- Compared to the same period last year, a slight month-on-month increase in fraud rate (by volume and value) was observed in March 2025, indicating that the March 2026 drop is unlikely to be seasonal.

By Fraud Type

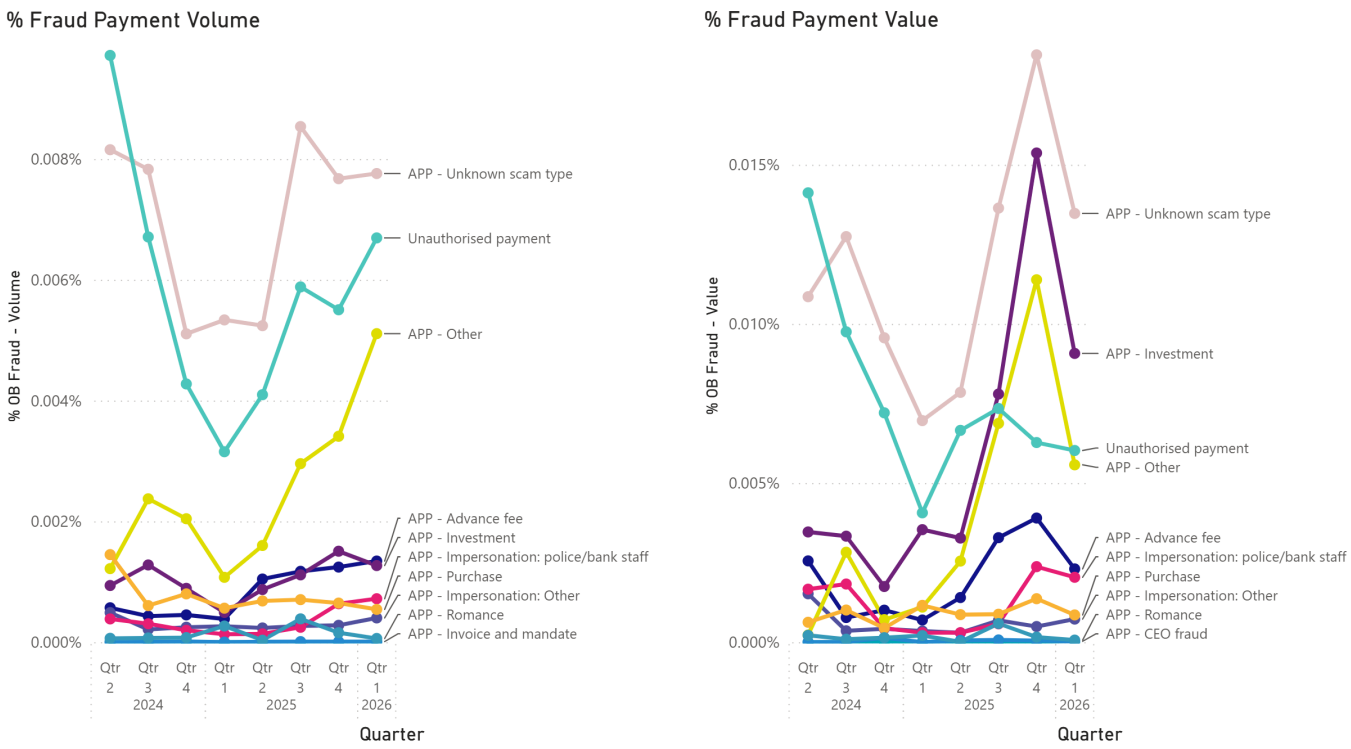

Figure 5 - Fraud type trends

Figure 5 shows fraud rates by volume and value, split by reported fraud type, including a breakdown into APP sub-categories.

- A material share of APP fraud continues to be recorded as "Unknown" or "Other", which limits the precision of typology-level analysis and suggests that the current categorisation does not yet capture the full picture.
- Among the identified APP fraud typologies, Advance Fee and Investment fraud remain the largest categories by both volume and value.
- Investment fraud is notable on a value basis, indicating substantially higher average losses per transaction than other APP categories. After a spike to 0.015% in Q4 2025, reported investment fraud value reduced to 0.009% in Q1 2026, although it remains a typology warranting continued monitoring due to its relatively high weighting.
- Unauthorised fraud rate by volume decreased from a high of 0.010% in Q2 2024 to a low of 0.003% in Q1 2025, but has since increased to 0.007% in Q1 2026. By value, the increase has been less pronounced (from 0.004% to 0.006%), indicating lower ATV on more recent cases.

Monitor summary

Overall, fraud volume has increased over the last 12 months to March 2026 marking a return to historic levels. Fraud value saw a quarter-on-quarter reduction in Q1 2026 but remained materially above the level recorded in the same period of the previous year. APP fraud remained the dominant typology, and investment fraud continued to be the largest identified APP sub-category by value, although it declined in the latest quarter.

Chapter 4 – Anecdotal information from ASPSPs

Provider observations supporting the Monitor findings

OBL receives data that provides context on the TPPs involved in initiating some fraud cases.. This information provides initial insights although only as a subset of all the information we receive. For now we consider it indicative and anecdotal; this is an area for future innovation. We have highlighted some trends that we were previously unaware of:

- There is a mix of the level of fraud initiated through TPPs, some have fraud rates materially above average, and others below. Where fraud rates are higher than average, we have not seen any patterns related to size of the TPP or known product types, for example.

- A TPP may experience elevated fraud rates with respect to one ASPSP, while remaining closer to the norm with others, suggesting that risk may be influenced by differences in customer base, control environment or reporting practices.

- The data also shows instances where fraud initiated through a TPP has generated an increase at a specific bank for a period of time before appearing to shift to a different bank . This may reflect reporting lag, or displacement effects following interventions, but further analysis is required before firm conclusions can be drawn.

Feedback from ASPSPs suggests that fraud patterns across Q4 2025 and Q1 2026 were shaped by a combination of growing payment volumes, continued social engineering activity and the adaptation of fraud typologies to newer payment journeys. When fraud is measured in terms of the number of frauds and value of fraud, ASPSPs have noted how it is important to take into consideration the significant rise on Open Banking initiated payments. For this reason, we also look at rates of fraud. However, the majority of ASPSPs have linked increases in Fraud to the overall growth in Open Banking payments.

Some firms have seen a rise in a type of phishing and impersonation scam that has been emerging more recently.

- The scam typically starts with a text or an email, although other forms of engagement with victims can also occur. The message may appear to be from a victim's bank or a relatively well-known retailer and say that the retailer or bank have noticed a transaction from the victim's account for a purchase that they think may not be you e.g. a scam. The message will say words to the effect that the original purchase was not genuine and they will refund the victim. The victim will need to click on a link and then follow some steps for the funds to be returned.
- The victim then clicks on the link to a fraudulent site, follows additional steps including giving access to their bank account - via a third-party provider - to make a payment. This may be posed as a step to check that the funds arrive.
- The fraudsters using the TPP have set up a payment from the victim's account, and the victim will be agreeing to 'receive funds' which instead initiates a payment from their account.

Across both periods, firms reported that APP and wider scam activity remained the main driver of concern, while Open Banking fraud was still a smaller share of overall attacks, but increasingly seen as an area likely to grow as usage becomes more mainstream.

Banks also highlighted the sophistication of emerging scams making it difficult to know when a fraudster had access to victim's accounts or when the money left the control of the victim. This level of sophistication has created operational challenges when classifying scam journeys, which then relates to the mechanisms under which ASPSPs then need to act, as well as in providing us the data. In some cases, it has blurred the boundary between authorised and unauthorised fraud for example.

Q4 2025: main themes highlighted by ASPSPs

ASPSPs reported that the aggregate picture in Q4 2025 was broadly consistent with what they were seeing in their own books. Social engineering continued to dominate, with APP scams remaining the main source of fraud losses. Firms specifically pointed to investment and crypto scams, alongside smishing and phishing activity, as persistent drivers. Some also noted that artificial intelligence was beginning to feature more visibly in fraud typologies, for example through deepfakes used during onboarding or celebrity impersonation in investment scam journeys.

Several banks also highlighted changes in how fraud manifests across payment journeys. These included me-to-me payments where the destination account had been opened under the victim's name while they were being coached by a fraudster, as well as an apparent increase in transactions to business beneficiaries, potentially pointing to a rise in consumer-to-business scam activity. ASPSPs further noted that fraud does not necessarily begin and end on the same payment rail: for example, a scam may originate through cards and then move through faster payments before funds are withdrawn, transferred internationally or converted into crypto. This can leave an ASPSP acting as an intermediary rather than the initiating or ultimate receiving institution.

On prevention, ASPSPs observed that Open Banking still accounted for a small portion of fraud attacks and was therefore not yet viewed as the most significant fraud channel. Banks also suggested that earlier sharing of emerging fraud intelligence with TPPs could help those firms prepare and respond more effectively. More broadly, firms saw value in richer payment profiling data, including the use of TRIs, even though these are not currently mandatory in most scenarios.

Q1 2026: latest trends and drivers

Feedback on Q1 2026 pointed to continued fraud growth, but largely in line with the underlying increase in payment volumes rather than a sharp divergence. ASPSPs highlighted the impact of growing customer activity, the emergence of new merchants and concentration around major online platforms, with some smaller firms experiencing significant growth in payments to particular merchants and a corresponding rise in fraud exposure. At the same time, some banks reported that targeted detection strategies focused on problematic TPPs and high-risk indicators were beginning to reduce both APP and unauthorised fraud rates.

ASPSPs also described continued evolution in scam typologies, including pay-by-link scams and fake refund journeys in which customers are manipulated into making payments while believing they are receiving money back. Firms noted that these cases can be difficult to classify cleanly because they sit in a grey area between authorised and unauthorised fraud, especially where social engineering exploits unfamiliar payment journeys. ASPSPs also highlighted pet scams, airline refund scams and impersonation scams, alongside broader concerns about fraudsters adapting established techniques to newer payment methods such as wallets and pay-by-bank journeys. The use of business accounts to increase payment limits and mask transaction purpose was also raised as a contributing factor in some cases.

Banks further pointed to a rise in first-party fraud, in some cases linked to scam journeys where customers unwittingly act as mules before later disputing the transaction. Banks share a strong view that Open Banking should be included fully in wider fraud data-sharing and prevention initiatives as volumes continue to grow. Previous work by the PSR and Pay.Uk looked into the viability of Enhanced Fraud Data, we understand that the approach to EFD has changed more recently. Pay.Uk is looking at the viability of a subset of information about the sending and recipient accounts being shared between the sending and receiving institutions in the transaction. This would not necessarily be dissimilar to how Confirmation of Payee operates between the sending and receiving institutions. We remain supportive of the approach to sharing information in order to detect and prevent fraud, to minimise false positives, and to avoid friction in payments where risks are low.

Overall direction across the two quarters

Taken together, anecdotal feedback from ASPSPs suggests a fraud landscape that is evolving in sophistication rather than changing direction fundamentally. Social engineering remains the dominant driver, but the channels, payment journeys and typologies involved are becoming more varied. The growth of Open Banking and digital payment use appears to be increasing exposure gradually, while also exposing gaps in warning mechanisms, classification approaches and cross-ecosystem information sharing. At the same time, some firms are beginning to report benefits from more targeted detection and richer data, indicating that more coordinated prevention measures could help contain future growth.

Appendix 1 – OBL Data Submission Template

Original ASPSP data request fields (2023):

Fraud Reporting

This return should be used to provide data on Open Banking payment frauds identified in your payment systems(s). Reporting should be based upon the reporting period in which the fraud was detected, *not* the period in which it was perpetrated.

By submitting data to Open Banking Limited ("OBL") you agree to do so under the terms of the Data Sharing Agreement, which can be found here: https://www.openbanking.org.uk/wp-content/uploads/Data-Sharing-Agreement.pdf.

Reporting Period	ASPSP Brand ID	Fraud Type	Consumer/ Business	Payment Type	ASPSP Authentication Channel	Total Fraud Cases Identified	Total Fraud Volume	Total Fraud Value
2023-10-01	9999	Unauthorised payment	Consumer	Single	App	5	6	4600
2023-10-01	9999	APP - Impersonation: police/bank staff	Consumer	Single	App	12	15	58750
2023-10-01	9999	APP - Invoice and mandate	Business	Single	Browser	3	11	28449

Total OB Payments

This return should be used to provide data on the total number of Open Banking Faster Payments (including internal transfers) initiated during each reporting period.

By submitting data to Open Banking Limited ("OBL") you agree to do so under the terms of the Data Sharing Agreement, which can be found here: https://www.openbanking.org.uk/wp-content/uploads/Data-Sharing-Agreement.pdf.

Reporting Period	ASPSP Brand ID	Consumer/ Business	Payment Type	ASPSP Authentication Channel	Total OB Payment Volume	Total OB Payment Value
2023-10-01	9999	Consumer	Single	App	662941	330144618
2023-10-01	9999	Consumer	Single	Browser	1226	35226
2023-10-01	9999	Consumer	sVRP	App	67781	52830331
2023-10-01	9999	Consumer	sVRP	Browser	474	165221
2023-10-01	9999	Business	Single	Browser	16552	15192360

TPP Volumetrics

Where available, this return should be used to provide information on Payment and Fraud data, initiated through each PISP.

By submitting data to Open Banking Limited ("OBL") you agree to do so under the terms of the Data Sharing Agreement, which can be found here: https://www.openbanking.org.uk/wp-content/uploads/Data-Sharing-Agreement.pdf.

Reporting Period	ASPSP Brand ID	TPP Brand ID	Consumer/ Business [Optional]	Payment Type [Optional]	Total OB Payment Volume	Total OB Payment Value	Total Unauthorised Payment Volume	Total Unauthorised Payment Value	Total APP Volume	Total APP Value
2023-10-01	9999	9999	Consumer	Single	11934	5776056	0	0	2	24000
2023-10-01	9999	9998	Consumer	Single	5331	1775223	0	0	8	8750
2023-10-01	9999	9998	Business	sVRP	847	204127	6	10550	0	0
2023-10-01	9999	9998			6178	1979350	6	10550	8	8750

- Detailed data dictionary and other supporting documents can be found here under the 'Financial Crime' tab: https://www.openbanking.org.uk/jroc/

Appendix 2 – Industry data sources

UK Finance Annual Fraud Report 2026

- Page 25 – Remote purchase fraud – includes cases and gross losses where the card was not present at the point of purchase.
- Page 31 – Remote banking fraud – includes mobile, internet, and telephone banking-initiated cases and gross losses.
- Page 33 – APP fraud – includes payment volumes and [gross] value, before value returned to victim.
- Data limitations:
    - Not all institutions provide fraud data reporting to UKFinance therefore total volume is likely to be understated.

Pay.uk Monthly Payment Statistics 1990-April 2026

- Faster Payments – Single Immediate Payments volume & value. (Jan '25 – Dec '25)
- Data limitations:
    - Includes data from all financial institutions therefore not a directly comparable denominator, with UKF fraud data.
    - Only reflects FPS single immediate payments, as this is the most likely payment method for APP and remote banking fraud. (Accounts for >98% of APP and remote banking fraud payments).

UK Finance – Card Spending Update December 2025

- Page 5 – Card Activity – includes total online payment volume & value. (Jan '25 – Dec '25)
- Data limitations:
    - Includes data for non-UK issues cards.

Christian Delesalle
OBL Head of Customer Success
christian.delesalle@openbanking.org.uk

Nick Davey
OBL Head of Strategy
nick.davey@openbanking.org.uk

Anton Joachim
OBL Data Scientist
anton.joachim@openbanking.org.uk

OPEN BANKING

The Standard for Open Innovation™

Open Banking Limited (OBL) - the Implementation Entity described in the CMA Order - built the UK's world-leading Open Banking Standard and industry guidelines to drive competition, innovation and transparency in UK retail banking.

There are now over 19 million active user connections - consumers and SMEs -of open banking-powered financial management apps and payment tools in the UK.

www.openbanking.org.uk
www.linkedin.com/company/openbanking