OPEN BANKING
The Standard for Open Innovation™

Financial Crime within Open Banking Journeys

OBL Report Covering Data from March 2024 to September 2025

Authors:
Christian Delesalle OBL Head of Participant Support
Nick Davey OBL Head of Strategy
Data: Anton Joachim OBL Data Scientist

December 2025

CONTENTS

Executive summary	3
Chapter 1 – Introduction	4
Chapter 2 – Data Collection and learnings	6
Chapter 3 – Anecdotal information from APSPs	12
Appendix 1 – Data request published by OBL in 2023	14
Appendix 2 – Comparative Payments Industry Data	15

Financial Crime within Open Banking Journeys – 2025 Update

Executive summary

This report provides the updated analysis of financial crime within Open Banking (OB) journeys, now covering data from March 2024 to September 2025. It builds on the findings from our December 2024 report and updates our analysis based on the recent trends observed in fraudulent activity. It is based on data provided voluntarily by Account Servicing Payment Service Providers (ASPSPs) covering 9 brands and accounting for over 60% of open banking payments[1]. We thank the data providers and are in talks with other ASPSPs to start collecting an even broader data set in 2026.

Key Insights

- Where industry data is available for comparison (January–June 2025), OB-initiated payment fraud continues to be low and lower than industry average, both in volumes (**0.013%** vs. **0.045%**) and in value (**0.020%** vs. **0.027%**). This low incidence underscores the effectiveness of current controls and the resilience of the OB ecosystem.
- Compared to our December 2024 report, OB-initiated payment fraud has decreased in volume (from **0.021%** to **0.013%**), while industry fraud increased (from **0.037%** to 0**.045%**). The trend is similar in value: decrease in OB fraud (from **0.034%** to **0.020%**) whereas the industry benchmark has remained relatively stable (from **0.028%** to **0.027%**).
- After a decrease in September 2024, OB fraud levels remained stable between September 2024 and May 2025, but have shown a slight increase over the last four months. There is no industry data available for comparison yet, but anecdotal evidence from the market and payment providers suggests that fraud is likely to be rising across other payment methods as well. Pay.UK data corroborates a rise in fraud cases during July (the latest data available for Faster Payments), reinforcing the need for continued monitoring. This indicates that the uptick is likely part of a wider industry phenomenon rather than an OB-specific issue – but we will need industry data to become available to confirm this.
- This recent increase appears primarily driven by Authorised Push Payment (APP) fraud typologies and it is worth noting that it is not observed by all ASPSPs, with some providers reporting that the latest trend is within normal tolerances, and overall fraud levels remain well-managed.
- The majority of OB fraud (74%) is attributed to APP fraud, which is a challenge across the entire payments industry. The average value of OB fraud transactions is higher than the industry average, reflecting the nature of OB use cases (e.g., account transfers, savings deposits).
- The emerging trend underscores the importance of adaptive fraud detection strategies and industry collaboration to mitigate risks.

[1] Note: the full market is defined here as open banking payments made with a payment account at a CMA9 ASPSP, or at a non-CMA9 ASPSP submitting data for this workstream

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. This report focusses on financial crime within Open Banking payment initiation journeys.

Open banking is an overlay system where payments can be initiated through internal transfer and over UK payment systems such as Bacs, CHAPS and Faster Payments. However, the majority of payments are made across Faster Payments. Payment initiation service providers (PISPs) are able to provide innovative, quick and low friction payment solutions to businesses and consumers using open banking technology.

As of September 2025, there are over 15 million user connections[2], demonstrating the growing adoption of open banking services by UK consumers and small businesses. There are 30 million payments 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.

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.

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

[2] Open Banking are unable to identify individuals consuming services through more than one brand. Reporting therefore represents the number of user connections with the brands providing reporting, rather than individual users.

- **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 to this update

In 2024, OBL started to collect data from ASPSPs, such as banks, and other PSPs under the Joint Regulatory Oversight Committee (JROC) workstream that looked at monitoring and preventing financial crime in open banking payment journeys.

For this report, 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 – Data Collection and learnings

Data collection and Analytics

In 2023, OBL issued the ASPSP Data Dictionary and Data Submission template to collect information from ASPSPs on the level of fraud in open banking journeys. We anticipated the first submissions on a voluntary basis in Q1 2024.

Submissions received for the period March 2024 to September 2025 cover five ASPSP Groups and nine ASPSP brands. Respondents are a combination of ASPSPs in the CMA9[3] 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 is not the full population of ASPSPs, we take this to be a representative sample covering large banks, smaller banks, and neobanks.

In addition to these submissions, data from the UK Finance Half Year Fraud Report 2025 is used to compare open banking fraud data with comparable information published for other payment methods. The comparisons are illustrative of the broad trends but we caveat that the comparisons are not completely like for like, for example the UK Finance data is likely to include fraud initiated using open banking across Faster Payments.

When comparing UK Finance Fraud data with open banking data, we have tried to ensure we are comparing the right underlying typologies. We have included the following UK Finance types of fraud for comparison: Remote Purchase, Remote Banking, and APP frauds.

We have spoken bilaterally to a set of ASPSPs to gather further insights and context to 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?

Key findings

1. Comparing OB fraud with UK Finance industry data (January-June 2025)

OB fraud for the period H1 2025 has been aggregated, analysed and compared to industry data from the same period – at the time of writing, the latest UK Finance industry data covers January-June 2025. Industry data includes APP fraud, remote banking and remote purchase fraud.

[3] The CMA9 refers to the nine largest banks and building societies in the UK, identified by the Competition and Markets Authority (CMA) as part of its Open Banking initiative.

Diagram 1: Fraud originated using Open Banking payment initiation & comparison with industry data, January 2025 – June 2025

	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	**4,243**	**13,968**	**0.013%**	**0.045%**	**£9,881,442**	**0.020%**	**0.027%**	**£707**	**£259**
Fraud Type:									
APP Fraud	3,102	10,322	0.009%	0.005%	£7,504,603	0.016%	0.011%	£727	£978
Unauthorised Fraud	1,141	3,646	0.003%	0.040%	£2,376,839	0.005%	0.016%	£652	£169
Customer Type:									
Business	61	110	0.004%		£196,288	0.004%		£1,784	
Consumer	4,182	13,858	0.013%		£9,685,154	0.023%		£699	
Payment Type:									
Single	4,065	13,391	0.014%		£9,651,028	0.021%		£721	
VRP	178	577	0.004%		£230,414	0.015%		£399	
ASPSP Authentication Type:									
App	3,060	10,330	0.013%		£6,871,333	0.023%		£665	
Browser	505	1,483	0.027%		£1,203,157	0.015%		£811	
Unknown	678	2,155	0.008%		£1,806,952	0.018%		£838	

Volume

Open Banking (OB)-initiated payment fraud remains lower than the industry average, at **0.013%** vs **0.045%**. The OB fraud percentage has declined vs the previous 6-month period (Jul–Dec 2024) from **0.017%** to **0.013%** for H1 2025. In contrast, industry fraud percentage has risen since FY 2024 (previous UK Finance report available), increasing from **0.035%** to the current level (**0.045%**).

Value

OB fraud is also lower than the industry comparator in value terms, at **0.020%** compared to **0.027%**. Again, this shows a reduction from the previous 6 months whereas the industry figure remains stable vs 2024 full year.

Average Fraud Value

The average value of OB fraud transactions stands at **£707**, which is higher than the industry average at **£259**. This reflects that some OB use cases are associated with higher-value use cases such as account transfers and savings deposits, and higher cost purchases. Industry-wide fraud includes a significant proportion of low-value online card transactions, the equivalent of which we are not aware of in Open Banking, explaining some of the disparity in average fraud values.

Breakdown

Fraud Type: Among OB-initiated payments, APP fraud accounts for the majority of fraud payments (74%).

APP Fraud:

- By volume: OB APP fraud is higher than the industry comparator (**0.009%** vs **0.005%**).
- By value: OB APP fraud is also higher than the industry comparator (**0.016%** vs **0.011%**).

Unauthorised Fraud

- Overall, OB unauthorised fraud is significantly lower than the industry average (**0.003%** vs **0.040%** by volume; **0.005%** vs **0.016%** by value).
    - Higher than industry remote banking unauthorised fraud (volume: **0.003%** vs **0.001%**; value: **0.005%** vs **0.004%**).
    - Lower than industry remote purchase unauthorised fraud (volume: **0.003%** vs **0.039%**; value: **0.005%** vs **0.012%**).
- OB average unauthorised fraud transaction value is **£652**, lower than the industry remote banking figure, **£1,694**, but higher than the industry remote purchase figure, **£130**.

Note: OB unauthorised fraud cannot be split into remote banking vs remote purchase due to shared payment rails. In the wider industry, remote purchase represents 98% of unauthorised fraud by volume and 75% by value, which is likely much lower for OB payments.

Retail and Non-Retail fraud

- Retail payments make up 97% of OB transactions, so retail fraud rates align closely with overall OB rates by volume (**0.013%**) and are slightly higher by value (**0.023%** vs **0.020%**).
- Non-retail payments (3%) show very low fraud rates (**0.004%** by volume and value), but the average fraud transaction value is high (**£1,784**), reflecting larger transaction sizes.

Payment Type

- Single Payments make up the majority of OB payments (88% in volume and 97% in value) and show higher fraud rates than Variable Recurring Payments (VRPs):
    - By volume: **0.014%** vs **0.004%**
    - By value: **0.021%** vs **0.015%**
- Average Transaction Value: Single payment fraud averages **£721**, compared to **£399** for VRP fraud.

ASPSP Authentication Type

- Payments authenticated via the ASPSP app represent the largest share of OB payments by volume (72%). The proportion of fraud from app-authenticated payments is comparable (74%).
- Looking at fraud, overall app-authenticated transactions have lower fraud rates in volumes than browser-authenticated (**0.013%** vs **0.027%**). However, in value, app-authenticated transactions show higher fraud rates than browser (**0.023%** vs **0.015%**), almost entirely driven by APP fraud (**0.019%** of the **0.023%**). One possible explanation on the higher prevalence of APP fraud here is that since most social media activity occurs on mobile devices and social media is a key channel for fraud scams, this could explain the higher incidence.
- Details by authentication method:

Fraud Volume %:

Fraud Category	App	Browser	Unknown	Total
APP Fraud	0.010 %	0.022 %	0.003 %	**0.009 %**
Unauthorised Fraud	0.002 %	0.005 %	0.006 %	**0.003 %**
Total	**0.013 %**	**0.027 %**	**0.008 %**	**0.013 %**

Fraud Value %:

Fraud Category	App	Browser	Unknown	Total
APP Fraud	0.019 %	0.010 %	0.008 %	**0.016 %**
Unauthorised Fraud	0.003 %	0.005 %	0.010 %	**0.005 %**
Total	**0.023 %**	**0.015 %**	**0.018 %**	**0.020 %**

- Average Fraud Value: Browser-authenticated fraud has a higher average transaction value (**£811** vs **£665** for app-authenticated), supporting the hypothesis that larger transactions are more common on desktop/laptop.

2. OB fraud Trends – March 2024 – September 2025

In addition to the above H1 2025 analysis and comparison to industry data, a longer trend analysis has been applied to data from March 2024 to September 2025.

Our earlier report analysed data up to September 2024. Since then, trend data shows that fraud remained relatively stable for the period September 2024-May2025. However, there has been a slight increase over the last 4 months. This recent trend appears to be driven more by APP fraud typologies, particularly using smart phone apps.

We do not have any comparator data for the last few months as fraud has risen, so we are unable to say whether this trend is solely an OB phenomenon or is representative of a wider increase in fraud. Anecdotally, fraud across OB tracks fraud being more widely perpetrated on other payment systems and channels, so we expect that this is a leading indicator on what is happening more generally and not specific to open banking. Pay.UK also indicated they have observed an increase in fraud cases in Faster Payments for July, their latest available data. It is also not the case that all ASPSPs are seeing a significant increase, with some ASPSPs saying this is within the tolerances seen previously.

Volume

Overall volumes of OB fraud transactions remained stable between September 2024 and May 2025. Since May 2025 there has been an upward trend, rising from **0.010%** to **0.023%** by September 2025.

Value

In Diagram 2, you can see a similar pattern in fraud value, with lower levels of fraud seen until May 2025, and an increase from June to September. The proportion rose from **0.02%** in May 2025 to **0.06%** in September 2025.

Fraud Type

Unauthorised Fraud has remained relatively stable throughout the period, with trends being largely driven by changes in APP fraud – while APP fraud has seen an upward trend in recent months, volumes of unauthorised fraud have remained stable.

Retail vs Non-Retail

Retail fraud trends closely mirror overall fraud patterns, reflecting the dominance of retail payments within OB transactions. Non-retail fraud has remained relatively stable over the period, so changes have been driven by retail fraud trends.

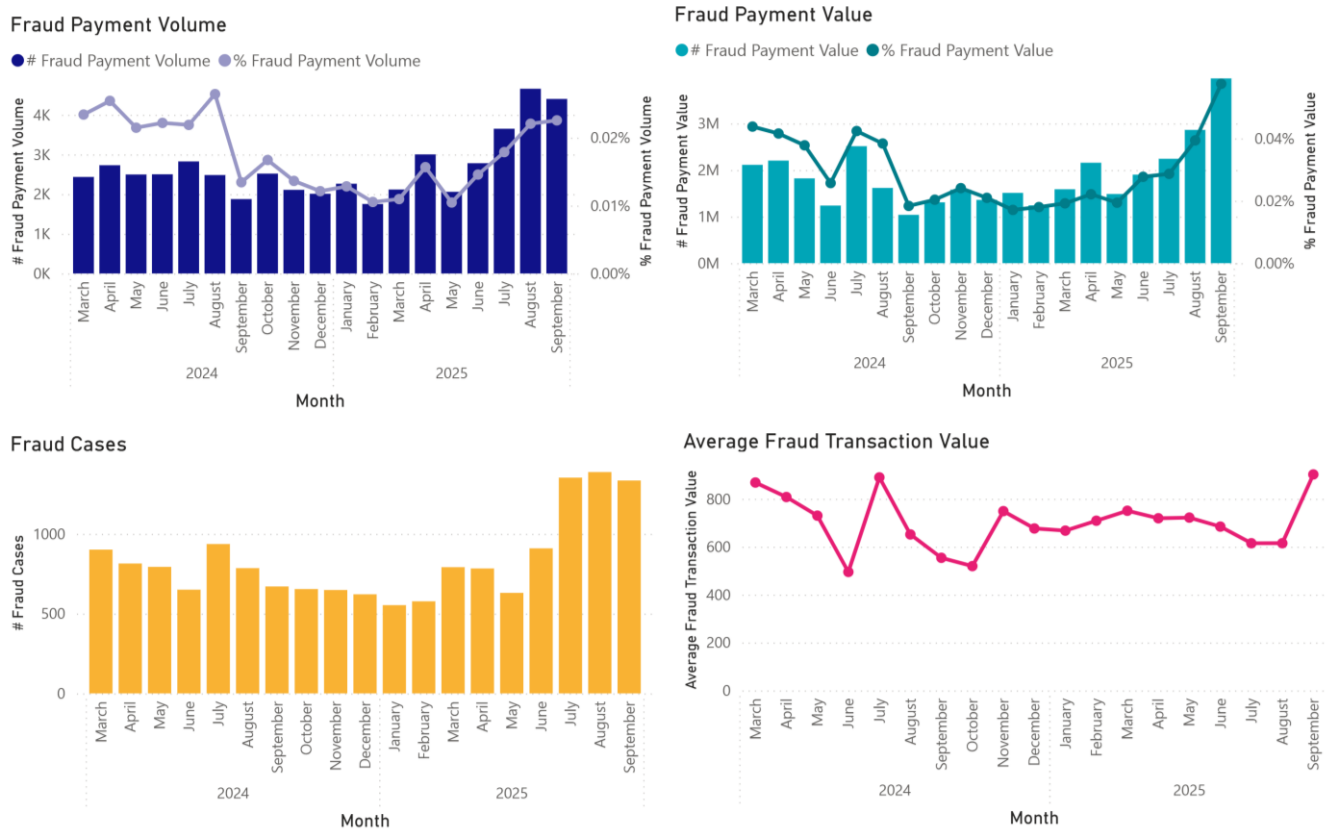
ASPSP Authentication Channel

Browser based fraud has remained relatively stable, with the recent increase in fraud trends being largely driven through fraud involving App authentication.

Payment Type

Fraud involving single payments has grown in recent months, while VRP-related fraud has remained steady without a comparable rise.

Diagram 2: 18-month trend of OB Fraud data



In summary

Open Banking continues to demonstrate trends that have shown resilience against fraud, with fraud rates lower than alternative payments systems and products. The higher average transaction values associated with Open Banking use cases – such as account-to-account transfers and savings movements – explains the slightly more elevated fraud rates by value. This reflects the nature of OB as a channel for higher-value financial activity, in contrast to the industry average which includes a significant proportion of low-value purchases.

Notably, APP fraud makes up most of OB fraud, whereas broader industry data shows a heavier concentration of unauthorised fraud, particularly remote purchase fraud. This distinction underscores the

need for targeted fraud prevention strategies that reflect the unique risk profile of Open Banking transactions.

From H1 2024 to H1 2025, the wider payments industry saw an increase in fraud rate from **0.037%** to **0.045%**. Although a like-for-like comparison is not possible (OBL only started to collect fraud data as of March 24), OB fraud saw a decrease between Mar-June 2024 and H1 2025 (**0.023%** vs. **0.013%**), in volume. OB fraud also saw a decrease in value over the same period (from **0.037%** to **0.020%**) while industry fraud remained stable (**0.028%** to **0.027%**). As noted above, OB fraud has since seen an increase. This needs to be further investigated with the industry to understand the underlying drivers and to ensure that fraud controls evolve in step with the growing adoption of Open Banking.

Chapter 3 – Anecdotal information from APSPs

Discussions with providers and other sources of information

- ASPSPs vary in the fraud trends they are seeing individually, with some ASPSPs suggesting that fraud on OB journeys was much higher in 2023 (pre-dating the data we have collected and published) and overall fraud having fallen, and only recently seeing small increases. Other ASPSPs have a much more volatile profile of fraud where we can see significant swings month on month; and others have very small and benign level of fraud. There is no one size fits all.
- Most ASPSPs have told us they do not see a significant difference between fraud initiated through Open Banking and other channels. They note that the typologies and specific fraud attributes appear relevant to OB and non-OB initiated payments. Therefore, trends appear similar, noting that OB frauds have a generally higher transaction amount.
- The fraud most prevalent across open banking is split between APP frauds such as investment scams and social engineering/impersonation scams and unauthorised fraud such as account access also via social engineering, SIM swap and handset theft related fraud.
- Fighting fraud is a continuous activity, and therefore the reduction in fraud over the majority of the period is not specifically attributed to a particular change in strategy or a new investment in fraud prevention, but rather ongoing vigilance. The changes in reimbursement rules in Faster Payments while, over the same time horizon as lower levels of fraud, anecdotally has not led to a specific change by ASPSPs and is not seen as driving trends. ASPSPs have been continually refining detection and prevention techniques.
- Some ASPSPs have alerted us to the easy availability of AI to fraudsters and the continued use of AI by fraudsters to convince APP fraud victims to make payments to them; this can be through using AI models to improve the quality of English spoken; provide accents; provide detail and enhance scripts to make them sound more plausible; hyper-personalisation to identify targets through deepfakes to trick victims into thinking they are talking to friends, family members, or senior staff within organisations. It also allows automation at scale with AI bots able to be used for larger scale phishing and social engineering campaigns, driving the 'barrier to entry' down for fraudsters.

While not related to Open Banking specifically, Experian has reported that 35% of UK businesses were targeted by AI-related fraud in Q1 20254. Experian also reported that UK businesses are themselves investing more in fraud prevention strategies, some of which will trickle down to consumers and individuals which could itself drive greater prevention of fraud at source before getting to the point where the victim is logging in to online banking or making a payment.

In terms of unauthorised fraud, CIFAs based information shows that SIM-swap fraud has increased significantly[5] whereas in our 2024 report we were alerted to phone theft as a significant driver of unauthorised fraud. SIM-swap fraud is where fraudsters convince mobile providers to port a victim's phone number to a new SIM card they control and then intercept SMS messages such as one-time passwords or codes allowing access to accounts. The Fraudster doesn't need to have the physical phone in hand. Previously we had been informed that a lot of growth in unauthorised fraud was based on stealing the physical device and cracking the security which enabled access to apps that allowed the fraudster to move money from the victim.

[4] See: https://www.experianplc.com/newsroom/press-releases/2025/new-report-from-experian-reveals-surge-in-ai-driven-fraud-

[5] See: https://www.cifas.org.uk/newsroom/fraudscape-2025-record-fraud-levels

Some ASPSPs suggested that open banking Account Information Service Provider (AISP) models and Confirmation of Payee provided the ability for victims to check that the accounts they were sending money to were legitimate. This has led to a greater prevalence of fraudsters recruiting money mules via social media and job adverts. Money Mules have legitimate looking accounts and give a false sense of confidence to the victim, who is then defrauded. In some cases, the money mule thinks they are being employed and unaware they are being used as a money mule.

Overall ASPSPs continue to look at different and evolving ways to prevent fraud. ASPSPs we spoke to would appreciate more information and data that would enable better profiling of payments. From an Open Banking aspect, a number of ASPSPs mentioned implementing TRIs which have yet to be uniformly rolled out by PISPs. Noting that the new commercial Variable Recurring Payment (cVRP) proposals were looking to establish a requirement for cVRPs to require TRIs. ASPSPs also noted industry initiatives such as enhanced data sharing between APSPs.

Appendix 1 – Data request published by OBL in 2023

- Original ASPSP data request fields:

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 – Comparative Payments Industry Data

UK Finance – Half Year Fraud Report 2025

- Page 11 – Remote purchase fraud – includes cases and gross losses where the card was not present at the point of purchase.
- Page 16 – Remote banking fraud – includes mobile, internet, and telephone banking-initiated cases and gross losses.
- Page 26 – APP: Payment Type – Faster Payments (includes APP fraud across Faster Payments - payment volumes and gross value.
- Data limitations:
    - Not all institutions provide fraud data reporting to UKF therefore total volume is likely to be understated.

H1 2025:

	Remote Purchase	Remote Banking	APP Fraud*	Total
Cases	1,655,122	41,746	213,525	1,910,393
Gross Loss	£215.4mn	£70.7mn	£208.9mn	£495.0mn

* Number of cases is not available for Faster Payments; we use payment volumes instead.

Pay.UK Monthly Payment Statistics 1990-September '25

- Faster Payments – Single Immediate Payments volume & value. (Jan '25 – Jun '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).

2025, in 000's – FPS SIPs

Jan	Feb	Mar	Apr	May	Jun	Total
370,368	349,807	393,635	385,149	386,453	400,445	2,285,857

2025, in £mns – FPS SIPs

Jan	Feb	Mar	Apr	May	Jun	Total

280,295	252,171	294,944	293,631	272,827	276,080	1,669,948

UK Finance – Card Spending Update June 2025

- Page 5 – Card Activity – includes total online payment volume & value. (Jan '25 – Jun '25)

Data limitations:

- Includes data for non-UK issued cards.

2025

	Jan	Feb	Mar	Apr	May	Jun	Total
Volume (000s)	326,000	303,000	346,000	329,000	336,000	323,000	1,963,000
Value (£mns)	28,387	23,994	27,532	27,217	26,038	24,535	157,703

Christian Delesalle
OBL Head of Participant Support
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 16 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