OPEN BANKING

Financial Crime within Open Banking journeys

JROC Workstream 2a - Financial Crime Data

April - September 2024 data

December 2024

The future of money | where you're in control

Contents

Executive Summary **3**

Chapter 1 – Introduction **5**

1. Background to open banking 5
2. Background to financial crime 5
3. Background to this update 6
4. Transaction risk indicators (TRIs) 6

Chapter 2 – Data Collection and learnings **7**

1. Data collection and discussions with providers 7
2. What are the headlines and trends we've observed? 8

Chapter 3 – anecdotal information from industry participants **11**

1. What are fraud typologies observed in open banking payments? 11
2. Are there any characteristic specific to open banking fraud? 13
3. What is missing to combat open banking fraud more effectively? 14
4. Looking ahead 15

Chapter 4 – Next Steps **16**

Executive Summary

This is the 2024 update on fraud seen in open banking journeys. We have asked ASPSPs in the open banking ecosystem to provide data on volumes and value of fraud that was originated using open banking. Data has been provided by a mix of five ASPSPs drawn from large banks, smaller banks and fintechs, covering 9 brands and accounting for 60% of open banking payments[1]. The data provided covers the six months from April-September 2024. From both the data and discussions with ASPSPs, we have gathered facts, trends and anecdotal insights into the fraud landscape with respect to open banking payments journeys.

This is the first time that such a rich dataset and insights on fraud have been gathered specifically relating to open banking. We thank the data providers and anticipate additional ASPSPs will want to provide data in later iterations.

Below we look at the headlines from the data and the insights given to us. In order to baseline the data, we have looked at UK Finance figures from the UK Finance Half Year Fraud Report 2024. This data does not cover exactly the same months and we have used the specific breakdowns that we think best fit the data we have compiled. This gives an illustrative comparison in terms of the trends we have observed, but caution should be given to exact use of the comparative data on a 'like-for-like' basis.

Headlines

- **Fraud volume and value trends** – open banking transactions have a significantly lower fraud rate by volume (0.021%) compared to other payment types (0.037%). However, the fraud rate by value is slightly higher (0.034% vs. 0.028%), with the average fraudulent open banking transaction (£700) more than double the industry average (£305). This reflects open banking's association with larger transactions, such as account transfers and high-value purchases.
- **APP fraud vulnerabilities** – open banking transactions exhibit higher APP fraud rates than other payment methods, both by volume (0.013% vs. 0.004%) and value (0.022% vs. 0.011%). We are told that fraudsters exploit its payments for sophisticated scams, including investment fraud and impersonation schemes, often using social engineering techniques via social media. Crypto trading/exchanges are mentioned by all five ASPSPs as being involved in fraud scams.
- **Unauthorised fraud characteristics** – unauthorised open banking fraud is significantly lower than industry fraud (0.008% vs. 0.032%). It more closely resembles 'remote banking fraud' which typically has a higher average transaction value than 'remote purchase fraud'. This is reflected by the higher fraud transaction amount of £640 compared with £214 for the broader industry.
- **Open banking fraud remains a lesser concern than for other payment methods** – several ASPSPs report an increase in fraud cases at the end of 2023. Additional measures have been put in place and fraud levels have subsequently come down. Open banking payments are still new but growing strong (+73% year-on-year): like every new payment method, open banking is likely to increasingly attract fraudsters' attention as it becomes more embedded, hence the importance of sharing data and collaborating between all ecosystem participants.
- **Open banking fraud is similar** to fraud seen in other payment methods. It is therefore important to share learnings with PISPs who may not have exposure to other payment methods.
- **Increased transaction-level information** – it would help ASPSPs to get additional information on the transaction/merchant in the same way as they do for some other payment methods. They also note that some TSPs use a single software statement for multiple merchants, preventing ASPSPs from identifying the name of the merchant/agent/customer-facing entity and implementing targeted fraud interventions. ASPSPs also mention that implementing TRIs and enhanced fraud data (EFD) across all participants would help mitigate fraud in open banking.

[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

- **Ecosystem data sharing on open banking-initiated payments** – building on this first report, OBL recommends that fraud trends continue to be monitored:
    - monthly, to detect any concerning fraud trend early;
    - that a full report is produced on a six-monthly basis, using comparisons with broader industry data;
    - data submissions are extended to additional ASPSPs to represent a higher share of the market.

  This is particularly important as open banking's growth is likely to attract fraudsters' attention as new propositions such as commercial variable recurring payments (cVRPs) enter the e-commerce space.

- **Ecosystem collaboration** – ASPSPs emphasised the importance of working together with TPPs to tackle fraud. We need to create the space for ASPSPs and TPPs to review the latest open banking fraud trends, discuss new fraud typologies, and share learnings and successful fraud prevention strategies, not only from open banking payments but from other payment rails. This will enable us to identify what we, as an industry, can consider early on, so that it isn't harder to fix at a later stage. For example, this could be a new forum specific to open banking fraud, or an addition to an existing industry forum, facilitated by OBL, UK Finance, or another industry body.

- **Payment journey** – the speed and ease of open banking payment journeys are a great benefit to open banking users, but some ASPSPs thought it limited fraud prevention efforts.

- **Customer education** – fraudsters target customers, who are then exploited. It is important that all parties help raise customers' awareness of fraud in the context of open banking payments. Customers still lack familiarity with open banking payments, the payment journey can take different forms (in-app, link, QR etc), and there is less standardisation than for other payment methods (e.g., a common name).

Next steps

In terms of next steps, ASPSPs welcomed further collaboration on trends and typologies observed in open banking. Greater awareness between ASPSPS, and importantly TPPs, could lead to better prevention of fraud. ASPSPs were happy that a forum could be established, or else pre-existing fraud groups could be used as forum for those conversations.

In addition, several ASPSPs welcomed the introduction of transaction risk indicators (TRIs) and enhanced fraud data (EFD) to share specific payment-related information in order to train models and gain a better fraud detection rate and minimise false positives. OBL supports these initiatives and would like to see them come to market and be in active use in the UK.

We note that fraud across open banking is generally quite small in nominal terms, and for some ASPSPs it is below the radar and/or data is not collected. This makes getting a complete industry picture more difficult. OBL advocates continued data collections and, where possible, data collections aligned with other industry collections such as the UK Finance half-yearly updates. This will enable like-for-like comparisons to be made, and open banking-specific issues mitigated and prevented.

Chapter 1 – Introduction

1. 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: first, it enables consumers and businesses to access and use their payment account data, second it allows the initiation of payments from consumers' payment accounts. This report on financial crime focuses on payment initiation.

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

More than 11 million people in the UK use open banking on a regular basis. There are 22 million payments initiated using open banking each month (based on OBL October 2024 data). While customers and businesses benefit from the use of open banking, fraudsters and criminals are also able to trick customers into giving their credentials away, or to use open banking products and services when perpetrating authorised push payment (APP) fraud.

2. 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 to accounts 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 is 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:

- **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 payments across Faster Payments.

3. Background to this update

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

For this report, we analysed six months' worth of 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.

We have also noted the various initiatives that ASPSPs have suggested would continue to help prevent fraud, and bring this together in a series of next steps in Chapter 4. Ultimately, OBL is keen to prevent fraud and play its part in doing so where possible.

4. Transaction risk indicators (TRIs)

Open Banking has been working with industry in developing information passed between PISPs and ASPSPs when initiating a payment. This shared information set comprises TRIs. To understand their impact, select PISPs and ASPSPs have been involved in a live pilot. This has recently concluded and we are collating the lessons learnt. Early signs are 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

1. Data collection and discussions with providers

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.

The template requests data for Fraud Payments, all open banking payments (this is used to calculate % Fraud) and a TPP Breakdown.

For the six-month period from April to September 2024, OBL received submissions covering fraud and open banking payments from five ASPSPs and ASPSP groups, and nine ASPSP brands. These data providers are used to initiate around 60% of all open banking payments (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).

While this is not the full population of ASPSPs, we take this to be a representative sample covering large banks, smaller banks and neobanks. Not every data provider is able to give a full breakdown of fraud typologies or the PISPs involved in the fraud case. For this reason, we do not report on the partial data we have on those areas.

In addition to these submissions, data from the UK Finance Half Year Fraud Report 2024 is used to compare open banking fraud with fraud from other payment methods, noting that the UK Finance data is likely to include fraud initiated using open banking across Faster Payments but that it is not split out. We have included the following UK Finance types of fraud for comparison based on the following: Remote Purchase, Remote Banking, and APP frauds.

For each of the ASPSPs that submitted data for this report, calls were arranged to gather further insights and context to the data provided. These sessions also served as an opportunity to explore views of open banking fraud more broadly. In Chapter 3 we examine additional insights that ASPSPs have provided about fraud in open banking journeys.

2. What are the headlines and trends we've observed?

Summary

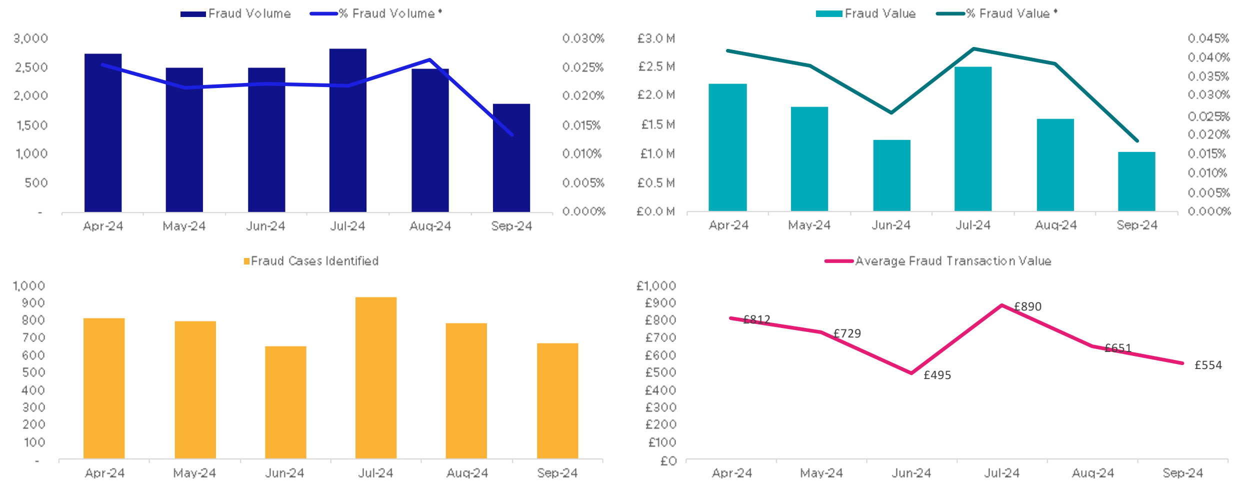
		OB Fraud Cases	OB Fraud Payment Volume	% OB Fraud Volume *	% Industry Fraud Volume (H1 24) **	OB Fraud Payment Value	% OB Fraud Value *	% Industry Fraud Value (H1 24) **	Average OB Fraud Transaction Value	Industry Average Fraud Transaction Value **
Total		**4,651**	**14,913**	**0.021%**	**0.037%**	**£10,444 k**	**0.034%**	**0.028%**	**£700**	**£305**
Fraud Type	APP	2,690	9211	0.013%	0.004%	£6,794 k	0.022%	0.011%	£738	£1,200
	Unauthorised	1,961	5702	0.008%	0.032%	£3,650 k	0.012%	0.017%	£640	£214
Customer Type	Consumer	4,594	14,776	0.022%		£10,112 k	0.038%		£684	
	Business	57	137	0.006%		£333 k	0.009%		£2,429	
Payment Type	Single	4,504	14,388	0.023%		£10,186 k	0.034%		£708	
	VRP	147	525	0.006%		£259 k	0.023%		£493	
ASPSP Authentication Channel	App	3,105	10705	0.020%		£6,805 k	0.032%		£636	
	Browser	1,036	2318	0.062%		£2,085 k	0.039%		£900	
	Unknown	510	1890	0.015%		£1,554 k	0.036%		£822	

* % Fraud is a percentage of all OB Payments supplied in tab '2 - Total OB Payments'

** % industry Fraud calculated using UK Finance and Pay.UK reported data

Aggregate findings

Charts 1-4



* "% Fraud Volume" and "% Fraud Value" are respective fraud figures divided by all open banking payments

As you can see from the charts above, fraud is relatively flat in relation to open banking payments. Some data reporters have explained that fraud has generally fallen over the past few years, and has stabilised over recent months. This reflects the work that TPPs and ASPSPs have done to educate consumers about specific new types of fraud and the preventative measures they have put in place.

Comparisons between fraud in open banking payments versus UK Finance statistics

- **Fraud volume**: fraud rates in open banking transactions are 0.021% (around 1 in every 5000 payments). UK Finance data for overarching fraud on a broadly comparable basis is around 0.037%

(around 1 in every 2500 payments) so fraud on open banking payments is lower. However, the evolving nature of fraud in open banking necessitates continued vigilance as adoption grows.

- **Fraud value**: despite lower fraud volumes, open banking fraud by value is 0.034% which is slightly higher than the UK Finance comparator at 0.028%. The average fraudulent open banking transaction amounts to £700, with an industry average of £305, highlighting the greater use of open banking in larger transactions, such as high-value purchases or transfers between accounts, in contrast to lower-value purchases common in other payment types.

Breakdowns

APP fraud

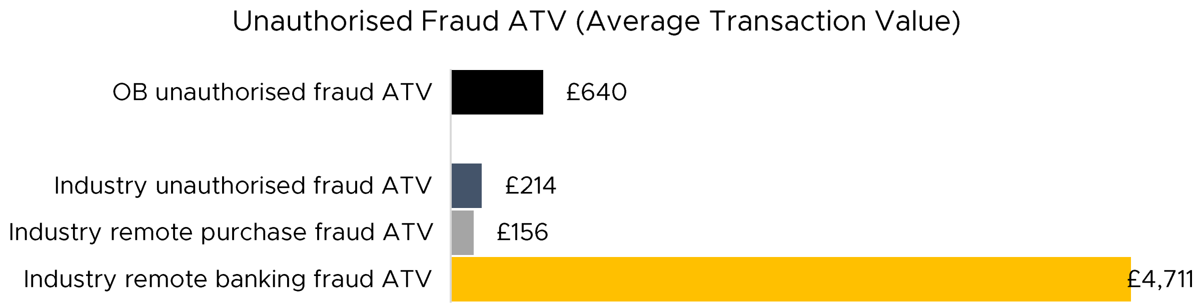
- Open banking transactions exhibit higher APP fraud rates compared to other methods, both in volume (0.013% vs. 0.004%) and value (0.022% vs. 0.011%).
  The average amount of an open banking APP fraud case (£738) is lower than the industry average (£1,200)[2]. This may be in part attributed to some APP scams being made across channels with higher limits than open banking e.g. where ASPSPs have different limits for branch and phone payments.

Unauthorised fraud

Unauthorised open banking fraud more closely resembles ‘remote banking fraud’ (high-value direct account access) than ‘remote purchase fraud’ (smaller transactions limited by merchant controls).

‘Remote purchase’ accounts for 84% of industry-wide unauthorised fraud (by volume) and we think this percentage is much lower in open banking payments. Given the limited number of e-commerce open banking use-cases, it is likely that most unauthorised open banking fraud will be similar to ‘remote banking’ fraud but will contain a small element of ‘remote purchase’ fraud.

- Industry data shows ‘remote banking’ average transaction value (ATV) is considerably higher than ‘remote purchase’ ATV (£4,711 vs £156). This is because fraudsters typically have direct access to larger funds when accessing a bank account and are not limited by merchant fraud controls.
- The ATV for unauthorised open banking fraud is higher than the industry equivalent (£640 vs £214) which supports the view that unauthorised open banking fraud contains a higher proportion of ‘remote banking’ fraud in comparison with the industry.



[2] Based on 2024 H1 total APP fraud losses of £213.7mn from 178,230 payments within the UK Finance data.

Retail and non-retail fraud

- Retail consumer payments represent the vast majority of open banking payments (97%). Therefore, the open banking retail fraud rate mirrors the overall open banking payment fraud rate (0.022% vs. 0.0021% by volume and 0.038% vs 0.034% by value).
- Although non-retail transactions make up just 3% of open banking payments, and fraud rate (by volume) is just 0.006%, fraud in this area has a big impact. The average loss per transaction is £2,429, significantly higher than for retail fraud (£684). Non-retail fraud tends to be targeted and sophisticated, involving larger fraudulent purchases and access to larger balances.

ASPSP authentication channel

Browser-authenticated open banking transactions have significantly higher fraud rates (0.062%) than app-authenticated transactions (0.020%). Browsers rely more on passwords, which are vulnerable to phishing, compared to the stronger biometric authentication used in apps:

	Fraud % Volume	ASPSP Authentication Channel			
		App	Browser	Unknown	**Grand Total**
Fraud Type	APP (Authorised Push Payment)	0.014%	0.033%	0.003%	**0.013%**
	Unauthorised payment	0.006%	0.029%	0.011%	**0.008%**
	Grand Total	**0.020%**	**0.062%**	**0.015%**	**0.021%**

While fraud rates by volume are higher in browsers, APP fraud where the user authenticates via the ASPSP's app accounts for a greater share of fraud by value (0.024%), emphasising the need for robust in-app security measures:

	Fraud % Value	ASPSP Authentication Channel			
		App	Browser	Unknown	**Grand Total**
Fraud Type	APP (Authorised Push Payment)	0.024%	0.020%	0.017%	**0.022%**
	Unauthorised payment	0.009%	0.019%	0.019%	**0.012%**
	Grand Total	**0.032%**	**0.039%**	**0.036%**	**0.034%**

Social media is a frequent enabler of APP fraud, with fraudsters for instance promoting fake investment opportunities to lure victims.

TPP & use case insights

- OBL only received useable TPP-level data from two ASPSPs. This is not sufficient to ensure this data is representative of the entire market and to derive any reliable insights. Receiving TPP-level data from a higher number of participants would allow to identify and address a potential concentration of fraud risk on certain TPPs.

Chapter 3 – anecdotal information from industry participants

1. What are fraud typologies observed in open banking payments?

Overall, there appears to be more fraud on the higher value APP scams, although we note some investment scams start with higher frequency transactions to gain a status and/or unlock benefits. ASPSPs broadly see open banking being used where it is an easier payment journey than alternatives, be that a banking app, online, or an alternative payment method. In this section, we look at the main types of APP and Unauthorised fraud.

APP fraud

ASPSPs did not find a significant difference between APP fraud perpetrated directly through their banking apps and across Faster Payments versus those initiated within an open banking journey. However, as noted in the data, the value of APP fraud in open banking is higher on average. This could be related to the types of scams that are considered as more prevalent.

Most common APP fraud typologies

- **Investment scams** – where fraudsters convince customers to move money to fake investment platforms, often through social media channels. These scams commonly involve high-pressure tactics and crypto or fake investment opportunities. Fraudsters may coax customers to send their own money to invest and get it back with a return or to ‘unlock higher commissions’. These frauds can be bundled with job opportunity scams, where victims are thought to be employed to undertake activities such as high volumes of low-value transactions. This escalates into the use of their own funds for a number of higher value investment-type cases, often crypto, generating high fraud losses.
- **Impersonation fraud** – where fraudsters impersonate legitimate organisations (e.g., financial advisers, bank representatives) to convince customers to make transfers. As with online/mobile banking fraud, most cases involve social engineering techniques like phishing, smishing, and even fake job offers. Some common frauds are safe harbour scams where victims think their accounts have been hacked and move money to a safe account which is set up by the scammers or is in their control.

Other types of APP fraud observed by ASPSPs

- **Advance fee frauds** – where customers are told they can recover past investments (e.g., lottery wins, old investments) but need to pay upfront fees to unlock the process.
- **Multi-hop / multi-step fraud** – where customers move money to accounts they have opened and which they believe are legitimate. They then either purchase crypto which they provide to a fraudster in exchange for the promise to sell the crypto for high yields, or for return with additional funds. In some cases, the fraudsters have control of the destination account (which seems legitimate and is in the customer’s name), then move the funds into crypto and into their possession.
- **E-commerce and dubious merchants** – as with other payment methods, e-commerce fraud continues to be a concern, with some fraudulent merchants targeting open banking users.

Unauthorised fraud

Unauthorised fraud refers to cases where the victim is not present, nor making the payment later found to be fraudulent. Typically, this would be account take-over frauds but other frauds are reported by ASPSPs:

- **Device theft or loss** – fraudsters use stolen or lost devices to access banking or money apps and make fraudulent payments, often before the customer can report the theft. SIM swap attacks were also mentioned, where fraudsters gain control over the victim's phone number and use it for fraudulent purposes.
- **Social engineering and credentials theft** – fraudsters use social engineering to steal credentials, gain access to accounts, and/or trick customers into giving up personal information that leads them to be able to access accounts.

Frauds related to specific TPPs or merchants

OBL did not receive useable TPP-level data from enough ASPSPs to derive any reliable insights on TPP-specific fraud. However, several ASPSPs highlighted emerging fraud in certain sectors such as money services, crypto exchanges, and travel agents, with these platforms used to launder money or buy valuable items. Crypto trading/exchanges came up in all our discussions with ASPSPs as being involved in some fraud scams.

Also, some ASPSPs reported a significant proportion of fraud cases linked to specific merchants. Although this should be taken with caution due to the very low volumes, this highlights the need for monitoring fraud at the TPP level, for a dialogue on fraud topics between ASPSPs and TPPs, and for targeted strategies to address merchant-related risks.

2. Are there any characteristic specific to open banking fraud?

There appears to be limited information as to why a fraudster may use an open banking journey but common themes emerged from our discussions with ASPSPs:

- **Less transaction details** – ASPSPs reported that the data shared during open banking transactions is not as rich as with traditional payment methods like debit cards. For example, there is less information about the recipient's identity and transaction details, especially for e-commerce transactions, which makes it more challenging to detect fraud. One ASPSP highlighted the challenge of not having access to merchant names, which hampers its ability to pinpoint high-risk merchants or sectors efficiently, detect fraud early, and take preventative action. Some TPPs/TSPs use a single software statement for multiple merchants, making it impossible to identify the name of the merchant and to use this information for fraud detection tools. Note: software statements are an integral part of open banking journeys. The TPPs provide information which the ASPSPs rely on and which also helps them understand who the agents/merchants/customer-facing-entities are.
- **Frictionless payment journeys** – some ASPSPs stated that fraudsters prefer low-resistance routes. Open banking journeys offer convenience and speed, the appeal for many consumers and businesses, but some ASPSPs feel that the open banking customer experience guidelines (CEGs) do not offer enough guidance for banks to stop a fraudulent payment.
- **Customer awareness** – open banking payments are still relatively new. Customers are well familiar with using a PIN for a POS card transaction and the 3D Secure process for an online card transaction, which are standard processes. However, there is still a lack of customer awareness about open banking payments and their different forms (e.g., link via email or text, getting a QR code). This can make it easier for customers to be deceived. One ASPSP also highlights that the customer remains the weakest link in OB fraud prevention.
- **Limited information exchange between parties** – there is often a lack of communication between TPPs and ASPSPs once the money has left the customer's account. This limits the ability for PISPs and sending ASPSPs to monitor transactions after they've been initiated, making it easier for fraudsters to funnel money to untraceable accounts and into crypto wallets.

Although not specific to open banking, the additional factors were also often quoted by ASPSPs:

- **Challenges with crypto and P2P payments** – payments to crypto exchanges or P2P transactions present specific vulnerabilities as there is often little transparency regarding the final beneficiary of the funds (e.g., the person owning a crypto wallet). This makes it difficult for banks to monitor the legitimacy of such transactions.

3. What is missing to combat open banking fraud more effectively?

All ASPSPs reporting fraud data to OBL already have data monitoring and fraud detection model capabilities.

However, many ASPSPs understand that data sharing and better models and tools are key to driving up detection rates. Some ASPSPs noted the difference between detection and prevention, observing that while it is possible to detect fraud, victims are frequently under the spell of a fraudster and prevention means breaking that spell. Below are the top four priorities identified by ASPSPs to help prevent OB fraud.

- **Enhanced data sharing** – there is a consensus from ASPSPs that enhanced data sharing across all participants could significantly improve the detection and prevention of fraud in open banking. Transaction risk indicators (TRIs) and other fraud detection tools such as enhanced fraud data (EFD) need to be expanded and made mandatory to ensure data parity with some other payment method:
    - TRIs are already an optional element of the OB standards and provide valuable information on the transaction.
    - EFD would provide valuable information on the recipient's account opening date and destination for the funds.

  OBL supports the view that more data sharing on a standardised and secure basis between participants in the payment journey will help to detect and prevent more fraud. An ASPSP looking for more data (including TRIs and EFD) to refine their fraud detection and intervention systems mentions that even in the case where TRIs do not directly detect fraud, they could improve subsequent fraud prevention actions by making their interventions more targeted.

- **Fraud prevention journeys** – a couple of ASPSPs said they look to improve their fraud prevention journeys by incorporating positive friction (e.g., additional verification steps) or to intervene in real-time for transactions at 'very high risk' of scam fraud. This APP scam intervention journey is to disrupt the fraudster's influence over the customer and is to be used on a targeted basis only, combined with a model-based approach to detect APP scams. Two ASPSPs suggest revisiting the customer experience guidelines (CEGs), balancing friction and security.

- **Ecosystem collaboration** – engagement between ASPSPs and TPPs varies significantly, with some ASPSPs actively working with TPPs to combat fraud while others don't. ASPSPs also note that there is currently no forum to specifically discuss open banking fraud, share insights and best practices between ASPSPs and with TPPs.

4. Looking ahead

All ASPSPs agreed that the volume of open banking fraud is still limited and within risk appetite, largely due to the immaturity of the channel. As such, it is not at the top of their financial crime agenda compared to other payment methods. However, as open banking matures and adoption grows, several ASPSPs expect to see open banking payments attracting more attention from fraudsters and the volume of fraud to increase, especially if prevention measures are not actively strengthened. For this reason, open banking fraud remains a key priority for them. Here are some elements that ASPSPs pay particular attention to, with a clear focus on fraud prevention.

- **Open banking's sustained growth** – like with any new payment method or new channel, open banking payments are likely to attract fraudsters' attention increasingly as they continue to become more embedded. As OB adoption grows, it is crucial to monitor the potential migration of fraud from traditional payment methods, such as debit cards, to open banking channels, and adapting prevention strategies. Customer awareness will also be key as more customers with a limited understanding of open banking will start using single immediate payments or VRPs, making them more susceptible to scams.
- **Emerging fraud risks** – most ASPSPs highlighted that new payment innovations like cVRPs and e-wallets present exciting opportunities for growth but also introduce new fraud risks that must be carefully managed, as fraudsters typically target less mature payment methods. New propositions should therefore be closely monitored. Fraud risks are also expected to rise as more merchants adopt open banking payments. Proactively addressing potential vulnerabilities in evolving systems is critical to staying ahead of fraud. For many ASPSPs and TPPs, VRPs are new or still in development. Sharing insights and best practices from those with experience in implementing VRPs will accelerate learning and enhance fraud prevention strategies across the industry.
- **Merchant-focused monitoring** – some ASPSPs indicate that fraud volumes are currently too low to warrant specific merchant-focused monitoring, but this is likely to become required as volumes increase. They emphasise the importance of monitoring new participants early, particularly merchants, who may inadvertently introduce risks.
- **Authorised fraud is a key concern** – social engineering remains a significant tactic for fraudsters, with many ASPSPs observing higher levels of authorised fraud, across payment methods, including cards.
- **Evolving TRIs** – there is a need to refine TRIs to address emerging threats. For instance, building specific indicators around investment scams could provide a valuable tool for combating this type of fraud. This development should be discussed and coordinated at an industry level.
- **Proactive fraud mitigation strategies** – ASPSPs emphasise the importance of incorporating robust fraud controls during the development phase of new products like VRP, rather than addressing vulnerabilities post-launch. ASPSPs also highlight the need to anticipate how fraudsters might exploit open banking journeys, to put proactive measures in place, to adapt to new threats, regularly evolving fraud detection measures such as monitoring money flows and introducing adaptive rules.

Chapter 4 – Next Steps

Based on our analysis of the fraud data and our interviews with ASPSPs, we propose the ecosystem focuses on six priorities.

1. **Open banking-specific fraud reporting** – this first report on six months of data from five submitting ASPSPs constitutes a strong base to build from. Fraud trends should be analysed continuously and over a longer period. We recommend that this effort is:

    a. continued, with monthly high-level reporting to detect any concerning fraud trend early, and a six-monthly full report comparing to broader industry data.

    b. extended to additional ASPSPs in order to represent a higher share of the market and as diverse a set of use cases and customer segments as possible.

    c. Enhanced with TPP-level data – OBL did not receive sufficient TPP-level data to draw any reliable conclusion in this report. Going forward, collecting TPP-level data from a higher number of participants would allow to identify and address a potential concentration of fraud risk on certain TPPs, merchants, or use cases.

    This is particularly important as the expansion of open banking is likely to attract fraudsters' attention and as new propositions like cVRPs enter the e-commerce space.

    On a separate note, changes were made to the Payment Services Regulations from 30 October 2024 allowing ASPSPs to delay payments for up to four days if they have a reasonable suspicion of fraud. It will be important to track to what extent this changes how ASPSPs manage fraud and its impact on fraud volumes.

2. **Increased transaction-level information, including TRIs and EFD** – helping ASPSPs get additional information on the transaction/merchant in the same way as for other payment methods will be critical in the fight against fraud. Implementing TRIs and Enhanced Fraud Data across all participants would help mitigate fraud in open banking.

3. **Ecosystem collaboration** – ASPSPs emphasised the importance of working together with TPPs to tackle fraud. We need to create the space for ASPSPs and TPPs to review the latest open banking fraud trends, discuss new fraud typologies, flag potential scams, share learnings and successful fraud prevention strategies, not only from open banking payments but also from other payment rails. This could take the form of a new forum specific to open banking fraud or an addition to an existing industry forum, facilitated by OBL, UK Finance, or another industry body.

    OBL will organise a round table on open banking fraud at the beginning of 2025 to review the findings of this report as well as facilitate a discussion on next steps.

4. **Single software statements** used for multiple merchants/agents/customer-facing entities – based on feedback received, it looks like some TPPs are not capturing all the required information correctly in the software statements, preventing ASPSPs from identifying the party interacting on behalf of the TPP and implementing targeted fraud interventions. We recommend this to be evaluated under the Standards maintenance work and provide remedies in terms of updating the Standards either via guidance or any updates to resolve the issues. The OBL Standards team is currently planning to discuss upcoming potential changes to the Standards with the regulators.

5. **Payment journey** – following the shift from the CRM Code to the APP reimbursement rules, OBL intends to review the new regulations and ensure consistent guidance on fraud warnings within the Standards subject to this being Standards maintenance under the Order.

6. **Customer education** – it is important that all parties help raise customers' awareness of fraud in the context of open banking payments, especially as more customers start using open banking payments and new propositions such as cVRP are introduced in the market.

OPEN BANKING

www.openbanking.org.uk