

6 November 2024

Dear recipient,

Help us get better insights about fraud

If you wish to discuss or write to us about our plans set out in this letter, please do so by 5pm on 4 December 2024. Please send any written comments to appscamenablers@psr.org.uk

Preventing authorised push payment (APP) fraud is a top priority for the Payment Systems Regulator (PSR). APP fraud causes immense suffering and harm to consumers and society, and damages confidence in payments.

That is why we introduced the reimbursement requirement, which requires victims of APP fraud to be reimbursed by their payment service provider when they lose out. While undoubtedly important, ensuring that scam victims are not left out of pocket is only part of the solution. We want to strike at the heart of the problem to stop fraud occurring in the first place. To do so, we need to understand more about how fraudsters contact victims and earn their trust.

For that reason, we used our formal power¹ earlier this year to require the 14 largest banking groups in Great Britain and Northern Ireland to give us data reported by victims on fraud committed in 2023. That data includes the frequency of fraudulent activity reported as being enabled via your firm's platforms or services, as well as via other providers. We intend to publish the data in a report in the week beginning 9 December 2024 and alongside this letter, we are sending you data pertaining to your performance and how it ranks relative to the other providers also identified in the data.

The story so far

The payments industry plays a vital role in fighting APP fraud, and this has been the focus of our fraud work since 2019. Key measures we have introduced include:

- **A world-leading reimbursement requirement:** This holds both sending and receiving payments firms jointly responsible for reimbursing APP fraud victims. This came into effect on 7 October 2024.
- **Publishing fraud data:** For the last two years, we have published payment firm-level data showing the highest senders and receivers of APP fraud, and how well these firms reimburse victims.

We designed these measures to incentivise payments firms to innovate to prevent APP fraud, leading to better outcomes for consumers.

¹ These include our formal information gathering power under section 81 of the Financial Services (Banking Reform) Act 2013.



When recording instances of fraud, payments firms can gather and analyse a rich dataset on the platforms and services that fraudsters use to contact victims and persuade them to make payments. We call these platforms 'fraud enablers'.

Many payments firms and industry bodies have published datasets at a sector level. They have called for other industries to act to stop attempted financial crime before consumers are exposed to harm.

We welcome initiatives between technology, telecoms, and other large online-based businesses along with the payments industry to better understand the threats and improve their collective response.

However, we consider that more systemic action is needed. Data insights can be a powerful way to encourage a greater ecosystem response to prevent APP fraud. This data tells us which private sector companies are most commonly reported as enabling contact between fraudsters and victims that results in an APP fraud payment.

Industry-wide benefits of publishing fraud enabler data

Collecting and publishing this data supports our statutory objectives to ensure that payment systems are operated and developed in a way that takes account and promotes the interests of businesses and consumers who use them; and to promote effective competition in payments.

The main benefits of publication are:

- **Raising consumer awareness:** With people increasingly reliant on online and telecoms enabled channels to communicate, shop and learn, it is important for consumers to be aware of which platforms and services fraudsters use to target them. Publicly available data can help consumers decide whether to make certain payments.
- **Raising customer vigilance:** We think the timing of publishing the 2023 data in December 2024 is important. Insights for consumers will encourage them to remain vigilant in the run-up to Christmas, when more are likely to be shopping online, creating more opportunities for fraudsters to target and take advantage of customers.
- **Providing valuable insights:** Payment firms can build risk profiles of transactions based on how their consumers use platforms and services. We expect this to encourage non-payments firms to collaborate more with payments firms to share data across industries, better target interventions, and build resilience to stop consumers from being caught out. Supporting the upstream fraud prevention in this way also complements our responsibility for the reimbursement rules.
- **Highlighting the platforms and services that are most often exploited by fraudsters:** This will help the ecosystem understand the scale and nature of the threat. Firms will see the extent of fraud originating on their platforms and have a reputational incentive to do more to prevent it. With more action being taken by a wider set of actors to prevent fraud at source, we expect fewer people will see their money fall into the hands of fraudsters.

Future plans for publishing 2024 and 2025 data

We propose to publish fraud enabler data every year. When collecting and publishing data for 2024 and 2025, we will follow the same approach we took for the 2023 data.

We benchmarked the 2023 data against existing industry data. For consistency, we used common definitions of key terms in the payments industry in our data request. However, this year we noticed variation across the industry in how some data is gathered and defined. Therefore, the payments industry needs to do more to improve data consistency. We will explain more about this as well as key definitions and our approach when we publish our December report.

In the first quarter of 2025, we will consult on plans to improve data collection, and develop consistent metrics and definitions. We expect that the first opportunity to build more consistency in the data collection will be from 2026.

How we collected data

We gathered data from the 14 largest banking groups in Great Britain and Northern Ireland for 2023. This data is collected by payments firms at the time of recording an APP fraud and is victim self-reported. The firms were asked for a breakdown of the fraud incidents into these sub-categories of push payment fraud:

- Invoice and mandate fraud
- Impersonation – police/bank staff
- Impersonation – CEO
- Impersonation – other
- Investment
- Advance fee
- Purchase
- Romance

We asked the firms to share the value and volume of APP scam incidents that occurred from 1 January 2023 to 31 December 2023 where a victim reported that an entity such as a social media platform, search service, telecoms provider, email provider, or auction/listing site enabled contact between them and a fraudster.

We defined 'an enabler' as an entity that a victim reported as either:

- a platform or service through which the fraudster made contact with the victim, or
- a website or platform where the victim saw an advertisement or profile that led to an APP scam.

Our data shows that when reporting incidents of fraud to their bank or building society, victims cannot always identify the platform that enabled contact between them and a fraudster. It has also shown that family and friends can play a role in enabling fraud, and that not all fraud is digitally enabled. We are standardising how this fraud enabler data is collected in the future, to address any data gaps, and make the data as insightful as possible about how APP fraud happens.



We plan to rank firms by the number of times they were reported by fraud victims as an enabler, using the fraud types listed above. We may also publish rankings of firms by specific sectors or sub-sector such as the most common enabler recorded among listing or auction sites, the most common among social media platforms, and so on.

Tell us what you think

If you would like to meet or share your comments on plans to publish this data, please do so by 5pm on 4 December 2024. Send written comments to appscamenablers@psr.org.uk

Yours sincerely

A handwritten signature in black ink, appearing to read 'David Geale', with a long horizontal flourish extending to the right.

David Geale
Managing Director