connecting the future

Call for Evidence

Fraud

Home Affairs Committee

Response from
The Payments Association
October 2023

Introduction

The Payments Association welcomes the opportunity to contribute to the Home Affairs Committee "*Call for Evidence on Fraud*".

The community's response contained in this paper reflects views expressed by our members and industry experts recommended by them. As The Payment Association's membership includes a wide range of companies from across the payments value chain, and diverse viewpoints across all job roles, this response cannot and does not claim to fully represent the views of all members.

We are grateful to the contributors to this response, which has been drafted by Riccardo Tordera, our Head of Policy & Government Relations and Robert Courtneidge, Advisor to the Board. We would also like to express our thanks to the Home Affairs Committee for their continuing openness in these discussions. We hope it advances our collective efforts to ensure that the UK's payments industry continues to be progressive, world-leading, and secure, and effective at serving the needs of everyone who pays and gets paid.

Tony Craddock
Director General
The Payments Association

As indicated in the indications to respond, we are submitting written evidence, covering all or some of the points raised by the Call for Evidence, in less than 3,000 words, preceded by a summary. We are focusing on the main issues that fraud causes to the payments industry, and the appropriacy of the government and regulator's current approach.

Summary

Financial fraud is a national emergency that should already have been resolved. We need measures that effectively prevent fraud. Our members are committed to tackling any weaknesses identified in payments that enable criminals to commit fraud or other economic crime and launder the proceeds. Nonetheless, we notice that some of the measures that are being considered to prevent fraud in payments such as the PSR's "APP scam" approach do not bring every player to table. We believe that it is essential that we work alongside 'big tech' and merchants to solve fraud with state-of-the-art data-sharing solutions. Simply mandating that financial services companies reimburse victims does not solve the problem of fraud; rather, it encourages more first party fraud. More generally, the emergence of new types of technology, such as artificial intelligence, is being used to prevent or commit fraud. Such technological change necessitates the analysis of pros and cons and the impact on the industry. Money programmability could also help eradicate fraud in some areas such as government payouts and is worth of consideration as a potential longer term solution.

Response

At the time of writing, The Payments Association is trying to engage with policy and lawmakers to highlight how the proposed PSR mandatory reimbursement to solve authorised push payment (APP) scam that should come into force at some point in 2024 is unlikely to resolve the problem of fraud, but may rather trigger unintended consequences that will negatively affect the industry's growth in the UK and will increase first party fraud.

Our industry working group, *Project Financial Crime,* has recently outlined how the payments industry should move forward in order to solve the problem of fraud. As outlined in our trade association most update policy document, The Payments Manifesto, we believe that the payments industry should:

1.1. Champion engagement with other parts of the ecosystem involved with APP fraud, including social media giants where most APP fraud originates, and merchants where they are part of the payments journey.

1.2. Encourage 'big tech' companies to support Stop Scams UK and shoulder their share of the burden of fraud by collaborating with the payments industry and law enforcement agencies.

1.3. Encourage institutions to set up a central means of sharing data on fraudsters and their victims or to contribute to a proven, secure and well-run database to share financial crime data to identify criminals and help to prevent fraud.

1.4. Work with organisations such as UK Finance and Pay.UK to: a) arrange appropriate access to data sharing initiatives; b) resolve any legal challenges associated with data

sharing; and c) change perceptions of the chances that legal data sharing will result in fines.

1.5. Promote the development and adoption of a data passport, or an equivalent digital identity framework, for both consumers and SMEs. Such a framework will be interoperable with EU electronic identification (EIDAS) and trust services regulation while minimising the chances that financially excluded consumers suffer.

1.6. Highlight concerns on several aspects of the Payments Systems Regulator's (PSR) proposals to reduce Authorised Push Payments fraud, including:

1.6.1. The ongoing 'moral hazard' of consumers not taking as much care with payments due to awareness that nearly 100% of them are reimbursed from APP scams;

1.6.2. The risks that the proposed 50/50 liability split for APP scams will lead to unintended consequences, including reduced competition from smaller companies and the reduced availability of accounts for those who are financially excluded;

1.6.3. The risk that, in to avoid incurring the additional costs of reimbursing fraud losses, account providers start to: a) de-bank customers, i.e. close their accounts; b) adjust the rules on the volume, value and velocity of receiving payments from certain types of individuals, based on their enhanced risk profile; and c) increase the due diligence levels for opening accounts with potentially riskier or more costly customers.

1.7. Promote the use of: a) effective compliance tools and techniques using the latest technology; and b) artificial intelligence to onboard customers safely, identify and track fraudsters effectively and spot money mules more easily.

1.8. Support the upgrading of Companies House so that it is fit for the purpose of identifying criminals committing fraud or laundering money.

1.9. Encourage regulators to support risk-based approaches to payments, allowing friction to be added by the industry to those few payment transactions deemed to be at high risk of being a scam, while ensuring a seamless real-time payments experience wherever possible for the majority.

Deep dive on APP Fraud Prevention

Fraud accounts for over 40% of all reported crime committed in England and Wales, with Authorised Push Payment (APP) fraud and scams significantly increasing in recent years. APP fraud arises when a victim is tricked into making a payment to an account controlled by a criminal. According to UK Finance's Fraud Report 2022, losses due to APP fraud amounted to GBP£485.2m, split between personal (£408.2m) and non-personal or business (£77m).

In response to the ever-growing levels of consumer harm due to APP scams, the PSR deployed a policy agenda to prompt a step change in the culture of payments firms to improve fraud prevention, as well as to protect users. Tackling fraud (including reimbursing more victims of fraud) is one of Government's (Home Office) priority strategies, aiming to reduce fraud by 10% on 2019 levels by December 2024.

On 7 June 2023 the PSR published a policy statement creating a new reimbursement requirement for APP fraud. It will apply to all types of APP fraud where payment orders are executed over the Faster Payment System subsequent to fraud or dishonesty. Mandatory

reimbursement requirements will apply to all Payment Service Providers (PSPs) sending and receiving payments over Faster Payments, irrespective of whether they are direct Faster Payments participants or indirect PSPs connecting to Faster Payments via an indirect access provider.

Sending PSPs will have to reimburse the victim of an APP fraud. Sending PSPs will then seek contribution for the costs of reimbursement from the Receiving PSP, with a default 50:50 split between the two parties.

In order to implement this policy, the PSR will use three legal instruments, on two of which it has consulted recently:

1. The PSR will direct Pay.UK to incorporate the new reimbursement requirement into the Faster Payments rules.

2. The PSR will require all Faster Payments participants (including indirect participants) to comply with the relevant rules and to provide specified compliance data to Pay.UK.

3. The PSR will direct Pay.UK to create an effective compliance monitoring regime to ensure that all in-scope PSPs (including indirect PSPs) are following these reimbursement requirements. Pay.UK will then provide compliance data to the PSR and this will inform any enforcement the PSR may take and allow the PSR to assess the effectiveness of the policy.

Whilst the PSR has specifically sought views on only two of the three legal instruments (items 1 and 3 above), they also welcomed views on the overall package of these legal instruments. There will be a further consultation on item 2 above later in October 2023. This is because by October the PSR expects Pay.UK to have drafted the reimbursement requirement rules which will enable the PSPs to view the draft rules alongside the consultation directed at compliance of PSPs with these rules.

The consultation closed on 25 August 2023, and the PSR intends to finalise and publish findings and intentions on all three legal instruments in December 2023.

What is going well?

The initiative has generated positive efforts by receiving PSPs to enhance their mule account detection capabilities, The initiative has also brought into discussion the fundamental role of firms occupying an upstream position in the APP scam chain (e.g. telcos and social media platforms). However, significantly greater focus on these adjacent players in the payments value chain, and inclusion in regulatory responses, is required. Working with adjacent industries, regulatory initiatives towards banning cold calling for the purposes of offering financial services are perceived as a positive building block of a realistic and multi-pronged response to the APP fraud problem.

What is going less well?

There are continuous high financial losses through APP scams and fraud. There is also lack of progress towards allocating liability to firms occupying an upstream position within the APP scam value chain (e.g. telcos and social media platforms). Bank data suggests that up to 87% of scams originate on tech platforms such as social media, however these platforms are not yet subject to fraud regulations or data sharing requirements. Scams originating from stolen identities on Facebook and other Meta platforms are a major issue.

In addition there are different views across the industry in response to the 50-50 reimbursement model. For existing participants of the CRM fraud scheme, this is a smaller investment/change than PSPs or smaller banks. However, this represents a significant new cost burden for many industry participants, especially smaller non-bank firms, with some across the industry suggesting this cost burden may lead to the demise of free in-credit consumer banking in the UK.

Some members are also concerned that the CRM experience shows that account opening by scammers is driven by the prospect of reimbursement.

We have other concerns, too. A 50-50 reimbursement model will potentially have a restrictive impact for new entrants due to reimbursement costs. There is a lengthy roadmap for Confirmation of Payee ubiquity across bank and non-bank PSPs. Delays in NPA delivery is detrimental to unlocking ISO 20022 benefits on fraud detection. And finally, ongoing consultations are causing a drain on resources and further deferring implementation.

What should be done differently going forward?
The following measures will significantly reduce APP fraud without detrimental impact on market participants and exacerbating the route cause of fraud:

- Prevention is better than reimbursement. As we develop new payment methods, building in preventative mechanisms should be a priority to avoid the current APP scam situation.
- Greater prosecution of criminals is required as a disincentive that counterbalances the potential moral hazard of reimbursing all APP victims.
- Upstream players (e.g. Telco providers, big tech platforms) should be brought to the table through regulatory, reimbursement, data sharing or industry engagement levers. For example, obliging social media platforms to become a merchant of record would be a useful step. And there is potential to wrap these outcomes into broader regulatory frameworks beyond financial services (such as policies to reduce online harm).
- A greater understanding of the typology and originating behaviour of fraud / scam use cases will be important to develop the correct response to current APP scam volumes and ensure frameworks for the future are designed effectively.
- There is a need to align data sharing requirements and infrastructures across the various fraud mitigation initiatives underway in the ecosystem already today (e.g. Pay.UK reporting, JROC reporting and PSR reporting). We must ensure that the establishment of data sharing frameworks are not just reporting tools, but a shared infrastructure with predictive analytics, similarly to the EBA or Monetary Authority of Singapore frameworks.
- Implementation of ISO 20022 enriched data sets will enhance detection options.
- A Financial Passport or a Single Proxy Lookup in the UK would help to reduce scams, as it has already in other jurisdictions such as India and Denmark.

Usage of fraud and the role of technology

Research by our members has reviewed how offenders are committing fraud and how the cross-cutting nature of fraud impacts the victims of the fraud. Most of the figures and analysis in our response below is drawn from our member Sumsub's Identity Fraud Report 2022. Key points to note include:

- From 2021 to 2022 the world has witnessed a 40% growth in payment fraud and the level of fraud in the UK has been steadily increasing too.
- In 2022, a UK passport was found to be one of the easiest documents to use for fraud purposes, accounting for 1.7% of all frauds, alongside the Ukrainian ID card,

and only topped in the global rankings by the Nigerian driver's licence, the Bangladeshi ID card, the Pakistani ID Card and the Nigerian ID Card.

- The top 3 fraud trends in 2022 include:
  1. **Deepfake usage:** fraudsters have developed more advanced deepfake technology, and the software required to create a deep fake is increasingly available on the internet. Depending on the input data, some deepfakes are incredibly hard to distinguish from reality, and only sophisticated anti-fraud algorithms can detect them reliably.
  2. **Complex fraud patterns:** since fraud technology is advancing rapidly, pattern recognition is becoming a must-have in order to catch fraudsters early. For instance, behavioural analysis can indicate if a person spends too much time (or too little) on the check. This can be a possible red flag.
  3. **Advanced forgery:** fraudsters no longer rely on obvious fraud attempts such as the use of printed images, document photos plastered on top of the original, phone screens, etc. Now, just about every attempt at bypassing verification is made with the help of carefully crafted deepfakes and fabricated IDs that require robust anti-fraud technology to detect.

Regarding the demographics of fraud, the research revealed that:

- The majority of forged documents relate to men (71.9% in 2021 while documents relating to females were 28.1%). This gender gap has grown even wider in 2022, with 79% of all forged documents relating to men.
- Fraudulent documents generally claim to be for people under 30 years old. The most common ages are 20, 21, and 22. This dynamic remains unchanged in 2022.

It is assumed that fintech, payments, crypto, and gambling platforms are most affected by deepfake fraud compared to other industries. This is because the vast majority of customers are onboarded online without face-to-face communication. However, strong onboarding is not enough to counteract fraud. The research revealed that 70% of fraud incidents occur post user onboarding, meaning that measures such as "ongoing monitoring" are crucial.

Other key data points include:

- 3.6% of all e-commerce revenue in 2022 was stolen by fraudsters.
- In 2022 the e-sports industry topped the fraud charts with a 2.9% share of total fraud cases, displacing the "payments" industry, which in 2021 was the leader with 1.3% of fraud cases amongst its verifications.
- The E-commerce and Banking industries saw the greatest growth in fraud from 2021 to 2022. E-commerce saw a rise from 0.1% to 1.3%, while for banking the increase was from 0.6% to 1.4%.

The most popular fraud schemes in 2022 were:

- **Multi-accounting:** this type of fraud is very common in the gambling and betting industries. Fraudsters attempt to register more accounts than permitted to perform welcome bonus abuse, arbitrage betting, and other fraudulent activity. Multi-accounting is preventable with liveness checks.
- **Account takeover:** gaining access to another person's account is still very common. By augmenting two factor authentication with a liveness check, participants can help to ensure complete protection at no expense to the user experience.

- **Biometric spoofing:** To fool biometric fraud prevention systems criminals use life-like masks, deepfakes and other advanced methods so that only the most sophisticated verification platforms can stop them.
- **Chargeback fraud:** fraudsters use stolen cards to issue illegitimate chargebacks by raising fake disputes with the bank. Bank card verification can prevent this from happening by thoroughly checking that a card belongs to the user.

Overall, complex fraud schemes include both identity theft and use of stolen bank cards. Transaction monitoring and assessing high-risk cases prior to payment authorization is the only reliable way to prevent illegal chargebacks and money laundering.

Our members also observe how the emergence of new types of technology, such as artificial intelligence, is being used both to prevent and to commit fraud. These are described below.

A Using AI and ML to prevent fraud

Technologies such as AI and Machine Learning can help to fight fraud and money laundering. We quote again our member's research which has scrutinised the impact of AI and machine learning to our industry. AI and Machine Learning can be used to combat money laundering in the following ways:

1. **Identity verification at onboarding**: machine learning algorithms can assist in verifying client identities by analysing various data points, including personal information, biometrics, and behavioural patterns.
2. **Document verification:** machine learning models can be trained to analyse documents, such as passports, driver licences and IDs. These systems can extract necessary information from documents, compare it to reference data, and detect potential inconsistencies. They can also flag forged or altered documents.
3. **Machine learning in transaction monitoring:** machine learning systems can process large amounts of transaction data and detect behavioural anomalies and suspicious activities in financial transactions, customer profiles, and historical patterns.
4. **Fraud and money laundering detection:** by analysing historical fraud patterns and continuously monitoring transactions in real-time, machine learning models can identify and flag potentially fraudulent activities.
5. **Ongoing monitoring:** machine learning algorithms can also be used to continuously monitor customer behaviour patterns based on historical data. These algorithms can learn what constitutes normal behaviour for each customer, such as typical transaction amounts, frequency, geographic locations, and other factors.

AI and Machine Learning can also be used to combat fraud:

1. **Detection of deepfakes**: there are main two detection methods:
   a) **Detection of artefacts not present in authentic media:** deepfakes often contain certain visual or audio artefacts that are not present in authentic media. Machine learning algorithms can be trained to detect these artefacts by analysing specific features of digital content, such as inconsistencies in facial expressions, unnatural eye movements, or distortions in sound waves.
   b) **Detection of deepfake generation techniques:** machine learning algorithms can identify traces left by specific deepfake generation techniques. These models can learn to recognize the unique characteristics introduced during the deepfake generation process.

2. **Behavioural fraud detection**: machine learning algorithms can be applied in the following ways:
    a) **Profile-based analysis and anomaly detection:** machine learning algorithms can create profiles based on historical data and customer behaviour, and can remember patterns of normal behaviour for individuals and groups. Trained on historical data, these models can flag suspicious transactions, user activities, and other behavioural deviations. This way, multiple fraud types can be detected, including account takeovers or identity theft.
    b) **Ongoing learning:** machine learning models can continuously learn and adapt from new data, allowing them to stay up to date with evolving fraud techniques.
3. **Document forgery detection:** machine learning can help with document forgery detection in the following ways:
    a) **Understanding document features:** machine learning models can extract relevant features from documents that are indicative of forgery, including texture, font, signatures, stamps, watermarks, etc.
    b) **Verification of signatures:** machine learning techniques can be applied to verify signatures, comparing a signature on a document with a reference signature. These algorithms can analyse stroke patterns, pressure, and thus recognize unique features of genuine signatures differentiating them from forged signatures.
    c) **Detection of forgery in digital documents:** machine learning models can analyse metadata, digital signatures, or compression artefacts and detect traces of manipulation. These algorithms can also check the textual content of digital documents to identify inconsistencies, plagiarism, or content alterations which indicate forgery.

B How AI and ML is used to facilitate fraud

AI and ML is used by criminals to facilitate fraud, especially through the growing use of deepfakes. The deepfake fraud landscape presents the following trends:

1. The number of deepfakes detected in Q1 2023 was 10% greater than in the whole of 2022.
2. The UK ranked second globally in deepfake fraud in 2022. While Spain leads the ranking with 49.7% of global deepfake cases, the UK came second with 9.3% and well ahead of the United States in third place with 4.2%.
3. In Q1 2023 the situation is set to remain similar: most deepfakes came from the UK and Spain, with 11.8% and 11.2% of global deepfake fraud respectively,

Such tendencies indicate that governments and regulators must keep up to date, recognising this fast-growing threat and addressing it comprehensively and responsibly.

Programmable money

Finally, digital currencies (stablecoins and CBDCs), and in particular the concept of money programmability can be deployed to prevent fraud, in relation to some specific usage for government payout. Development is capabilities is at an early stage, but the smart use of digital money by governments could eradicate the risk of financial disbursements to fraudulent claimants, avoiding situations such as the c£16m supposedly lost to fraud and errors in Covid-19 pandemic loan schemes.

About The Payments Association

The Payments Association helps members navigate a complex regulatory environment and facilitate profitable business partnerships.

Our purpose is to empower the most influential community in payments, where the connections, collaboration and learning shape an industry that works for all.

We operate as an independent representative for the industry and its interests, and drive collaboration within the payments sector in order to bring about meaningful change and innovation. We work closely with industry stakeholders such as the Bank of England, the FCA, HM Treasury, the Payment Systems Regulator, Pay.UK, UK Finance and Innovate Finance.

Through our comprehensive programme of activities for members and with guidance from an independent Advisory Board of leading payments CEOs, we facilitate the connections and build the bridges that join the ecosystem together and make it stronger.

These activities include a programme of monthly digital and face-to-face events including Financial Crime 360, our annual conference PAY360 and the PAY360 Awards dinner, CEO round tables and training activities.

We run seven stakeholder working groups: Inclusion, Regulator, Financial Crime, Cross-Border, Digital Currencies, ESG and Open Banking. The volunteers within these groups represent the collective view of The Payments Association members at industry-critical moments and work together to drive innovation in these areas.

We also conduct exclusive industry research which is made available to our members through our Insights knowledge base. These include monthly whitepapers, insightful interviews and tips from the industry's most successful CEOs. We also undertake policy development and government relations activities aiming at informing and influencing important stakeholders to enable a prosperous, impactful and secure payments ecosystem.

See www.thepaymentsassociation.org for more information.

Contact malik.smith@thepaymentsassociation.org for assistance.