the payments association

The impact of APP fraud on cross-border payments

Supported by

payall

the payments association

Contents

the payments association

Foreword

This whitepaper tackles one of the messiest and most controversial consequences of near-instant cross-border payments: Authorised Push Payment (APP) fraud.

The researcher and author, Dr. Nicola Harding, is an expert criminologist and is noted for her unusual and highly valuable real-world research techniques (I won't say more, you'll need to check out her work) as well as interview subjects. For this piece, she interviewed a wide range of professionals from vastly different positions in the ecosystem and at different stages in their experiences with APP fraud. These differences are important to keep in mind – views are diverse and provide texture, more so than a unanimous way forward.

I'll continue this theme by sharing a few of my views here, and again, these are my views – not those of The Payments Association or Nicola to get you started.

Regarding banks, EMIs and other regulated entities, here are three thoughts:

- More creative, hard-hitting and fresh techniques are needed to warn customers of these scams.
- The industry should embrace new, purpose-built software to identify and prevent APP fraud as well as contribute data to a shared repository for others to access.
- When a foreign bandit opens an account or a wallet with a domestic regulated entity to access the domestic payment network and commit fraud, a large share of the financial burden should be the responsibility of the entity that gave the shady foreign entity or person access to the domestic payment network.

Regarding regulators, here are two thoughts:

- It's not practical to expect regulators from around the world to align on how to solve this problem. However, when there's evidence and reasonable suspicion of a citizen perpetrating fraud, regulators should exempt the suspect from data protection in the context of the foreign investigation so that personal and transaction details can be shared to assist in the investigation.
- When there's a pattern of fraud or suspected fraud from a particular institution, local regulators should more quickly intervene and investigate.

Regarding consumers, we can't ignore personal accountability. No matter how effective the tech, or warnings – we as humans sometimes make terrible decisions with our money – and we should be accountable if funds can't be recovered.

There you have it. Some initial thoughts to get you started on what I'm sure will be a stimulating and enlightening read.

Gary Palmer
Founder, Chairman and CEO
Payall

the payments association

Abstract

The global landscape of cross-border payments is undergoing rapid expansion, driven by several key factors. These include the globalisation of trade, the rise of e-commerce, and the digital transformation brought by fintech innovations.

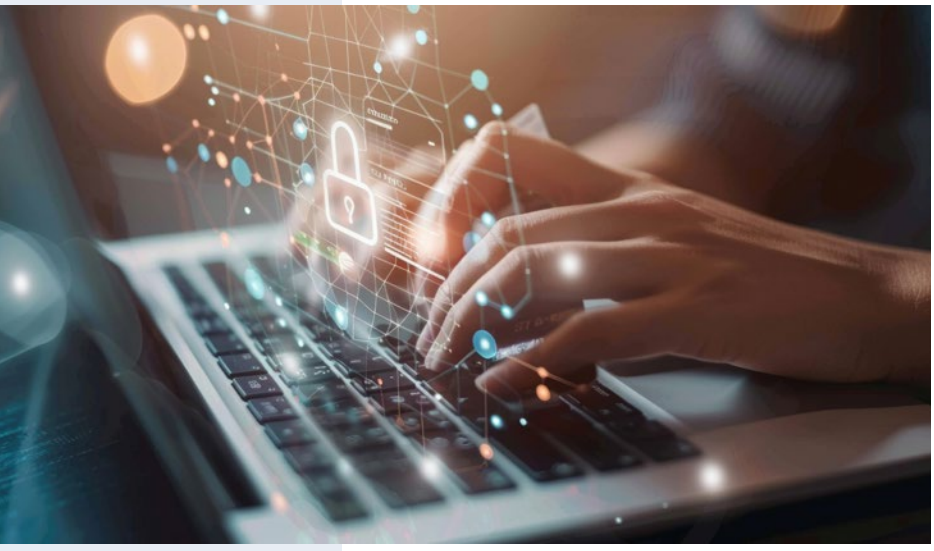
Small and medium enterprises (SMEs) now engage in international commerce more seamlessly, while consumers increasingly shop from global retailers. Digital wallets and payment platforms are simplifying transactions, and the increase in remittances due to global migration and international employment further contributes to the surge in cross-border transactions. In addition, the growing adoption of cryptocurrencies and blockchain technology, as well as the development of Central Bank Digital Currencies (CBDCs), are contributing to the cross-border payments landscape by offering faster and cheaper alternatives to traditional currency exchanges.

However, the growth in cross-border payments, particularly with over 80 countries offering real time payment schemes where payments can be initiated, cleared and settled between bank accounts within seconds, comes with heightened concerns about fraud, particularly Authorised Push Payment (APP) fraud. APP fraud, where individuals and businesses are tricked into making payments to fraudsters, is becoming more prevalent in international transactions due to the complexity, lack of standardisation, and involvement of multiple intermediaries. Fraudsters exploit global communication gaps, regulatory differences, and cybersecurity vulnerabilities to deceive victims, while the difficulty in reversing payments and recovering funds across jurisdictions further amplifies the threat.

To address these challenges, it is essential to go beyond technological solutions and learn from the personal experiences of victims and the insight of experts, gaining a deeper understanding of how criminals operate in the cross-border payment ecosystem. Fraud prevention strategies must incorporate this knowledge to identify patterns, predict fraud tactics, and educate stakeholders on the evolving risks. As cross-border payments continue to grow, the need for robust security measures, regulatory frameworks, and a thorough understanding of criminal methodologies becomes increasingly critical.

This paper consults with experts from across the payments infrastructure to explore the drivers of cross-border payment growth and addresses the emerging threat of APP fraud, offering insights into how advanced technologies, combined with experiential learning and criminal behaviour analysis, can safeguard the integrity of international transactions while supporting continued expansion.

*"Fraudsters exploit global **communication gaps, regulatory differences, and cybersecurity vulnerabilities** to deceive victims, while the difficulty in reversing payments and recovering funds across jurisdictions further amplifies the threat."*



the payments association

Executive Summary

Authorised Push Payment (APP) fraud is a global issue, yet the relationship between APP fraud and cross-border payments is under-explored.

To gain insight into the current threats linked to APP fraud and cross-border payments, we consulted with 15 industry experts from across the payments ecosystem to understand the challenges that APP fraud brings to cross-border payments and to consider the opportunities that exist now and in the near future to solve them. This paper found that:

1

Criminals are exploiting gaps

Criminals exploit the speed and anonymity of cross-border payments to commit APP fraud. This is facilitated by difficulties in tracing illicit funds across jurisdictions and the complexities of international payment systems. The UK, with its faster payment system, is a focal point for such activity.

2

Regulations are fragmented

Current regulatory efforts, while evolving, are fragmented and lack international consistency. Regulations like those from the UK's Payment Systems Regulator (PSR), which focus on domestic transactions and reimbursement, have limited applicability to cross-border payments. This highlights the need for greater international collaboration and a more comprehensive approach to combating APP fraud.

3

Social media giants must play their part

APP fraud is a broader societal issue, extending beyond financial services. Social media platforms, with their vast reach and anonymity, are often exploited for social engineering attacks. This necessitates a comprehensive response involving law enforcement, technology providers, and social media companies to address scams at their source.

4

Key challenges with cross-border APP fraud

Key challenges include the speed of transactions, the lack of global standards in fraud prevention, data sharing limitations, and the emergence of cryptocurrencies as a tool for money laundering.

- The speed at which fraudsters can move funds, often across multiple accounts and jurisdictions, makes it difficult to react and recover funds.
- The lack of consistent global standards in KYC, AML, and fraud detection allows criminals to exploit gaps in the system.
- Data privacy laws and the fragmented nature of the global financial system hinder collaboration and timely data sharing.
- Cryptocurrency, due to its anonymity and lack of comprehensive regulation, poses new challenges for tracing funds and combating fraud.

5 Opportunities to strenghten APP fraud prevention

Opportunities to combat cross-border APP fraud include leveraging technology, enhancing collaboration, and adopting a comprehensive "ecosystem" approach, as demonstrated by Australia.

- AI and machine learning can be used for real-time monitoring, faster fraud detection, and enhanced security measures – if policy gaps are closed and relevant data are used.
- Increased collaboration among financial institutions, law enforcement, regulators, and technology providers is crucial for sharing data, intelligence, and best practices.
- The Australian "ecosystem" approach, which involves a coordinated effort from various stakeholders, provides a potential model for other countries to consider. This approach emphasises prevention, early intervention, data sharing, and shared responsibility across the digital economy.

---

6 The big picture

Combatting cross-border APP fraud requires a global, collaborative approach and technological innovation. A paradigm shift is needed, moving from a reactive focus on reimbursement to a proactive approach that addresses the entire fraud lifecycle. This involves fostering a collaborative ecosystem that extends beyond financial institutions to include law enforcement, regulators, technology providers, and social media companies. Leveraging technology, such as AI, machine learning, and APIs, is crucial for real-time monitoring, fraud detection, and data sharing. Addressing the broader societal impact of APP fraud and building trust in the digital economy is equally important. A unified, global approach is essential to tackle the cross-border nature of APP fraud. This includes developing standardised data sharing protocols, harmonising regulatory frameworks, collaborating with social media platforms, and investing in advanced fraud prevention technologies. By embracing collaborative and technology-driven solutions, the global community can work towards a safer and more resilient financial ecosystem.

Introduction

In October 2022, the G20 outlined key initiatives to enhance cross-border payments[1], shaping a landscape that is becoming more efficient, secure, and inclusive. These efforts aim to address long-standing challenges in global transactions, with emerging technologies like blockchain, artificial intelligence (AI), and machine learning accelerating the transformation. These technologies offer faster, more cost-effective, and transparent alternatives to traditional payment models.

A central theme of these initiatives is interoperability — the linking of national real-time payment systems across central banks to promote seamless cross-border transfers. A growing number of countries are interconnecting their systems to facilitate instant cross-border transactions.

In 2023, India and Singapore connected their real-time payment networks[2], enabling customers of participating banks to send and receive funds instantly across borders. Similarly, in Europe, the Immediate Cross-Border Payments (IXB)[3] initiative is working to connect the European EBA Clearing RT1 system with the U.S. Clearing House (TCH) via SWIFT[4]. Meanwhile, Mastercard's Vocalink technology, which powers real-time payments in markets such as the UK, U.S., and Singapore, is advancing global interoperability in cross-border payments.

In addition to interoperability, the harmonisation of legal, regulatory, and supervisory frameworks is crucial to ensuring consistent cross-border operations between banks and non-banks. This is a real challenge, and perhaps unrealistic. However, APP fraud is a potential area for some alignment across jurisdictions.

Another key development is the growing role of Central Bank Digital Currencies (CBDCs), which provide central banks with a way to digitise national currencies for more efficient cross-border transactions. For instance, a collaboration between Israel, Norway, and Sweden (Project Icebreaker[5]) aims to make cross-border retail payments and remittances faster and more secure. Other initiatives, such as Jura[6] (exploring Euro/Swiss Franc applications) and mBridge[7] (focused on the Hong Kong Dollar and Chinese Yuan), are exploring wholesale cross-border payments. In Canada, the central bank is moving beyond research and development, working with the federal government to establish legislation and strategies for CBDC adoption, signalling a shift toward real-world implementation.

The Regulated Liability Network (RLN) combines the benefits of distributed ledger technology (DLT) with the safeguards of the regulated financial system. RLNs have the potential to revolutionise financial market infrastructures, allowing for programmable, multi-asset operations that function 24/7. This could significantly improve the efficiency and security of cross-border payments. However, the success of RLNs will depend on the development of robust regulatory, legal, governance, and operational frameworks to ensure trust and stability.

Finally, the standardisation of data exchange and messaging protocols is essential for strengthening global interoperability. ISO 20022[8] is emerging as the global standard for financial messaging, offering more structured and data-rich information that is critical for reconciliation, transparency, and compliance with regulations such as Anti-Money Laundering (AML) and Know Your Customer (KYC). SWIFT has driven the adoption of ISO 20022; and by 2025, 90% of cross-border payments are expected to comply with this standard. This shift will enhance global interoperability and lay the foundation for linking real-time payment systems worldwide.

Criminals are exploiting the interoperability gaps

Criminals are increasingly exploiting the speed and anonymity of cross-border payments to commit authorised push payment (APP) fraud, posing significant challenges for financial institutions and regulators worldwide. The allure of cross-border payments for criminals lies in the difficulties law enforcement agencies face in tracing and recovering illicit funds once the money leaves the original jurisdiction. This is compounded by the complexities of international payment systems, which offer a smokescreen for criminal activity. The UK, with its faster payment system, has become a focal point for fraudulent activity, attracting criminals seeking to move funds swiftly and evade detection, but this is a global issue.

The regulatory landscape for combating APP fraud is evolving but faces criticism for its fragmented nature and lack of international consistency. While regulations like the UK's Payment Systems Regulator (PSR) aim to protect consumers through mandatory reimbursement schemes, their limited scope and applicability to cross-border payments highlight the need for greater international collaboration. The complexity arises from the varying regulatory frameworks, KYC, AML and fraud detection rules across different countries. This inconsistency allows criminals to exploit gaps in the system, making it challenging to establish globally effective fraud prevention measures.

APP fraud is not solely a financial services issue. Adjacent financial industries such as cryptocurrency play a significant, yet unmeasured role in financial crime. Consumers have responsibility for their actions, and social media platforms, telecommunications providers, and merchants all play a role in facilitating these scams. Social media's vast reach and anonymity make it an ideal breeding ground for sophisticated social engineering attacks, leading to calls for greater regulation and accountability. This interconnectedness necessitates a comprehensive response that extends beyond the financial sector, involving law enforcement, technology providers, and social media companies.

Several key challenges and opportunities emerge from this complex landscape.

Challenges:

1. **The speed of transactions** enables fraudsters to move funds quickly, often before victims or banks can react.
2. **The lack of global standards** in fraud prevention and financial crime regulation creates a patchwork of approaches that criminals can exploit. And agreeing such standards across multiple jurisdictions, regulating bodies, and industry cultures may be unrealistic...
3. **Data sharing limitations**, arising from data privacy laws and the fragmented nature of the global financial system, hinder collaboration, and timely intervention.
4. **The emergence of cryptocurrencies** provides criminals with new avenues for money laundering and fraud due to their anonymity and lack of comprehensive regulation.

Opportunities:

1. **Leveraging technology**, such as AI and machine learning, offers potential for real-time monitoring, faster fraud detection, and enhanced security measures.
2. **Increased collaboration**, both domestically and internationally, is crucial for sharing data, intelligence, and best practices to disrupt criminal networks and address the cross-border nature of APP fraud.
3. **The Australian "ecosystem" approach**, which involves a coordinated effort from government, law enforcement, financial institutions, and technology companies, provides a potential model for other countries to consider.

This whitepaper will explore these challenges and opportunities in detail, examining the criminal tactics, regulatory frameworks, technological solutions, and collaborative initiatives shaping the fight against cross-border APP fraud. It will analyse case studies, including Australia's ecosystem approach, to consider best practices and offer insights for developing a more robust and resilient global payment system.

"Criminals are increasingly exploiting the speed and anonymity of cross-border payments to commit authorised push payment (APP) fraud, posing significant challenges for financial institutions and regulators worldwide."

Understanding the criminal opportunity of cross-border payments

Criminals are attracted to cross-border payments for several reasons, all of which centre around exploiting vulnerabilities and minimising risks.

Tony Sales
Chief Innovation Officer
WFF

We spoke to Tony Sales, Chief Innovation Officer, We Fight Fraud, a specialist consultant who utilises lived experience to explain how criminals operate. He highlights that moving money across international borders is attractive to criminals as it creates a significant barrier for law enforcement agencies and financial institutions seeking to trace and recover illicit funds. Once money leaves the jurisdiction of the original crime, it becomes more challenging for authorities to cooperate and investigate, especially given differences in legal frameworks and banking systems. Criminals often have a keen awareness of these disconnects and leverage them to their advantage.

The inherent complexities of international payments provide a smokescreen for criminal activity. Criminals exploit legitimate payment channels such as CHAPS, Faster Payments, and BACS payments to blend their transactions into the enormous volume of legitimate global transfers. BACS takes three days to process payments, and CHAPS is reserved for high-value, one-off transactions that require same-day delivery.

Jo Braithwaite explains that "BACS, the 'direct debit' and 'direct credit' payment system, saw the fastest growing number of APP fraud instances between the second half of 2021 and the first half of 2022, up 24% by value and 32% in terms of the number of cases. CHAPS, which is not covered by The PSR's new reimbursement scheme, is the UK payment system used for high-value retail and wholesale transactions, settling 0.5% of UK total payments by volume but 92% of total sterling payments by value. CHAPS turns over the annual UK GDP every six working days. This reflects the high value of transfers using CHAPS, it represents a relatively small, but significant, subset of APP frauds, at 0.2% by number but 4% by value. It is therefore clear that there are serious losses suffered to APP fraud involving transfers other than those executed.

> *"In this way, the faster payment function that is so appealing to criminals is used to launder money through the UK quickly but enables the geographical jurisdiction of both fraudster and victim to be almost anywhere."*

Faster payments' 24/7 availability and, almost instantaneous transactions, make them the preferred channel for criminals moving smaller amounts of money. Toby Evans, Head of Economic Crime at AusPayNet added that with 45% of all scam recipient accounts being in the UK from just one major bank in Australia, the UK is a hot spot for fraudulent and scam activity.

However, where scam recipient accounts are in the UK, this does not necessarily mean that the fraudster needs to reside in the UK too. As Graham Ridley, Strategy Director at IFX, highlights, "The use of virtual IBANS can mean that a domestic transaction in scope for APP Fraud, owned by a party outside of the Country, say Canada, with access to a virtual account that has a British reachable faster payment sort code, once completed, can be followed by a cross border payment to move the fraudulent funds to Canada. In this way, the faster payment function is appealing to criminals to launder money through the UK quickly and it enables the geographical jurisdiction of both fraudster and victim to be almost anywhere." The speed of the faster payment system itself is far more attractive to criminals globally who are trying to move money through multiple accounts quickly to evade detection and launder their illicit funds.

Criminals understand that some policies and processes can flag their activity for investigation. For example, in the United States of America (US), a currency transaction report (CTR) must be submitted if a financial institution processes any cash transaction exceeding $10,000[9]. Therefore, criminals will move money in smaller denominations to avoid detection by financial institutions. By breaking down large sums of money into smaller amounts, criminals can make their transactions appear less conspicuous and therefore less likely to be flagged. This method, known as "structuring" or "smurfing", is a classic money laundering technique designed to obfuscate the origin and destination of illicit funds. For instance, a criminal might attempt to move £10,000 but, instead of transferring the entire sum at once, they would divide it into multiple smaller transactions of £750, £50, £200, £400, and so on.

This approach makes the individual transactions appear more like everyday payments, effectively camouflaging them within the vast volume of legitimate financial activity.

the payments association

Payment "Camouflaging"

"These methods of camouflaging payments make it challenging for financial institutions and regulators to detect illicit activity. As such, governments and financial bodies are increasingly using advanced technologies like machine learning, artificial intelligence, and blockchain analytics to track and uncover suspicious payment patterns."

Payments can be "camouflaged" in various ways to conceal their true nature, often for illegal activities such as fraud, money laundering, tax evasion, or financing illicit activities. Criminals and bad actors use sophisticated techniques to obscure the origin, destination, or purpose of payments, making them difficult to trace or detect. Here are some common methods:

Layering

Layering is a key stage of money laundering, where illicit funds are passed through a complex series of transactions to obscure their origin. This involves:

- Moving funds through multiple accounts, often across different financial institutions or jurisdictions, to create confusion and distance from the source.
- Conducting a large number of smaller transactions (structuring or "smurfing") to avoid detection, especially by anti-money laundering (AML) systems that flag unusually large transactions.
- Using intermediaries or shell companies to disguise the payment's true source.

Use of shell companies

Shell companies, which exist on paper but have no real business operations, can be used to hide the true ownership and purpose of payments. Fraudsters or money launderers can funnel payments through these companies, making it difficult to trace the funds back to their illicit origins. The use of offshore shell companies in jurisdictions with weak regulatory oversight further obscures the trail.

Trade-based money laundering (TBML)

This involves the manipulation of trade transactions to disguise the movement of funds. Methods include:

- Over-invoicing or under-invoicing goods and services to transfer value between countries without arousing suspicion.
- Falsifying the quantity or quality of goods in international trade to transfer illicit funds.
- Using multiple jurisdictions to conduct the trade, making it difficult for authorities to detect irregularities in payments or goods.

Cryptocurrency and digital assets

Cryptocurrencies and other digital assets offer greater anonymity than traditional payment systems. While blockchain transactions are public, the parties involved in the transactions are often pseudonymous, making it harder to identify who is behind the payments. Criminals can use techniques such as:

- **Mixing services:** These blend cryptocurrency transactions from multiple users, making it hard to trace which funds belong to whom.
- **Privacy coins:** Cryptocurrencies like Monero and Zcash offer enhanced privacy features, hiding transaction details such as the sender, receiver, and amount.

Payments via offshore jurisdictions

Payments are often routed through offshore financial centres or jurisdictions with lax regulatory environments, making it easier to hide the identity of the sender or recipient. Offshore banking systems, secrecy laws, and limited disclosure requirements enable bad actors to camouflage the true nature of transactions.

Invoice fraud and false invoicing

Criminals can create fake invoices for non-existent goods or services to justify the movement of funds. This is often used in combination with shell companies or TBML schemes, where the fraudulent invoice makes it appear as though the payment is for legitimate business purposes when, in fact, it is part of a scheme to hide illicit funds.

Peer-to-peer (P2P) payment platforms

Peer-to-peer platforms like Venmo, PayPal, or other mobile payment services can be used to camouflage payments because they often lack the same stringent AML and KYC checks as traditional financial institutions. Criminals may send small, innocuous-looking transactions that fly under the radar of detection systems, and the informal nature of these platforms can make tracing the payments more difficult.

Prepaid cards and gift cards

Prepaid cards, especially those purchased in cash, can be loaded with illicit funds and used or transferred without linking the funds to any identifiable individual. Similarly, criminals use gift cards to move value anonymously. Once loaded with funds, prepaid or gift cards can be used to make purchases, withdraw cash, or sell on secondary markets.

Third-party payment processors

Criminals sometimes use third-party payment processors (TPPPs) or payment service providers (PSPs) to route payments. These intermediaries' aggregate transactions for multiple clients, making it harder for law enforcement to trace payments back to their original source. TPPPs that operate across borders or in loosely regulated environments add an extra layer of opacity.

Cash smuggling and currency exchange

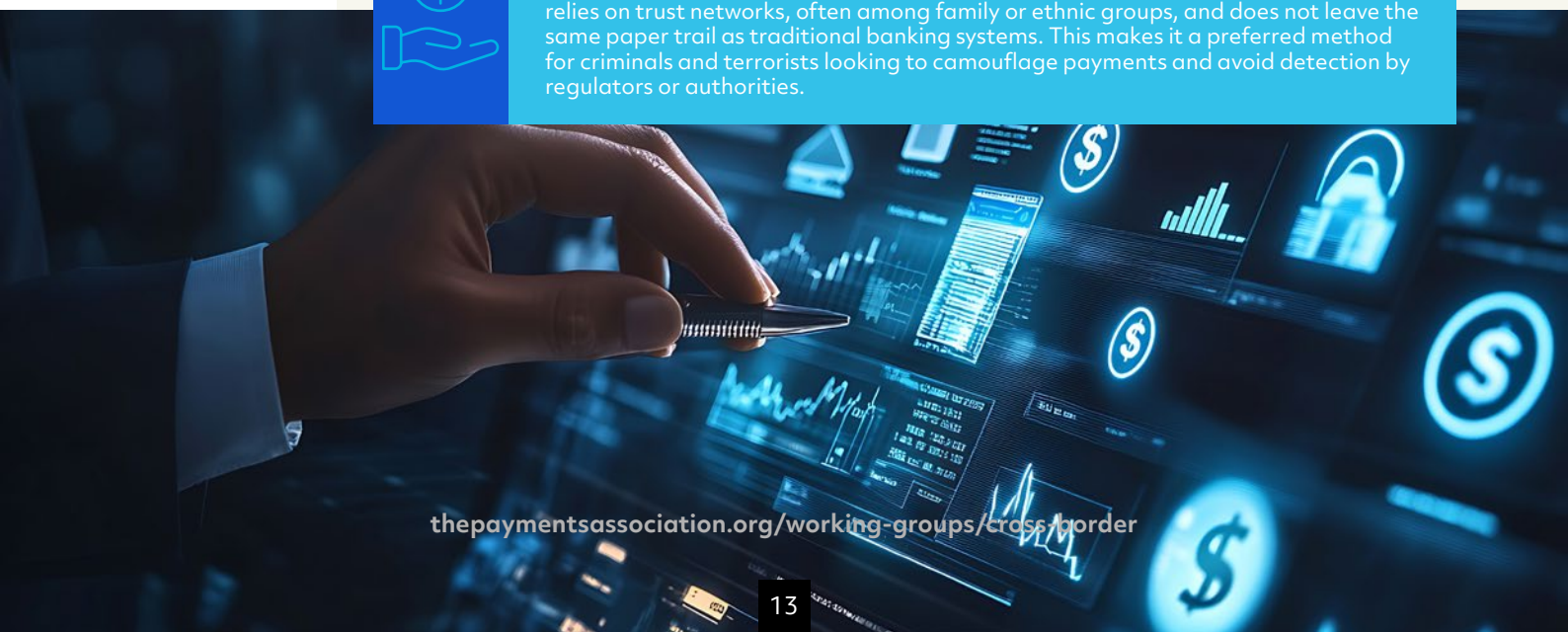
Smuggling cash across borders or using currency exchanges is another way to camouflage payments. Criminals physically move large sums of cash to jurisdictions where financial reporting is weak, or they exchange currencies at unofficial or black-market rates to mask the origin of the funds.

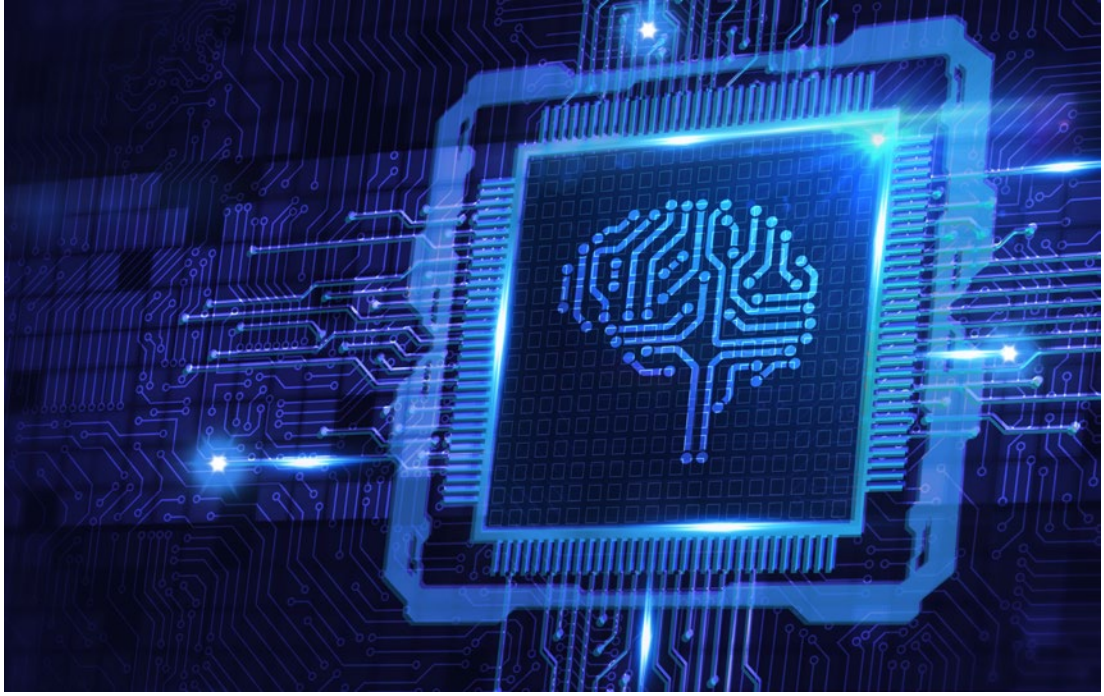
Fictitious loans and financial instruments

Fraudsters may create fake loan agreements or other financial instruments to legitimise the movement of money. These "loans" provide a veneer of legality to what is essentially the transfer of illicit funds, giving the appearance of a legitimate business transaction.

Hawala and informal value transfer systems (IVTS)

Hawala is an informal method of transferring money without moving actual cash. It relies on trust networks, often among family or ethnic groups, and does not leave the same paper trail as traditional banking systems. This makes it a preferred method for criminals and terrorists looking to camouflage payments and avoid detection by regulators or authorities.





By using trusted methods and breaking down large sums into smaller, less conspicuous amounts, criminals seek to avoid triggering fraud detection systems and arouse suspicion. It is the job of compliance teams to detect these payments; how successful they are may well depend upon the risk appetite of the business.

Real-time payments, while convenient for users, also benefit fraudsters. The faster transactions provide less opportunity for banks to identify and halt fraudulent payments, giving them a smaller time window to react. This can be particularly challenging in cross-border payments. This aligns with the view that the UK witnessed a surge in APP fraud following the introduction of Faster Payments in 2008, with the first EMI joining the Faster Payments scheme in 2018. The G20's push for real-time payments, largely driven by economic benefits, failed to anticipate how organised crime could exploit this speed for rapid money laundering.

Criminals are adept at leveraging the "always on" nature of real-time systems to quickly move funds across borders, making recovery more difficult. Adding any kind of friction that is necessary to deal with fraud effectively can impact the commercial model. So, the challenge is to create a culture of fraud prevention within an environment that has long viewed frictionless, faster payments as not only the 'norm' but a necessity.

The tension between criminals' ability to 'structure' illicit fund payments, the risk appetite of the financial institution, and regulatory bodies across different jurisdictions means that the first transaction made during an APP fraud scam is a crucial one. Beyond the initial transfer, funds are often carved up and sent through various money mule accounts, domestically and internationally.

PayNet
PAYMENTS NETWORK MALAYSIA

Gary Yeoh
Chief Marketing Officer
PayNet

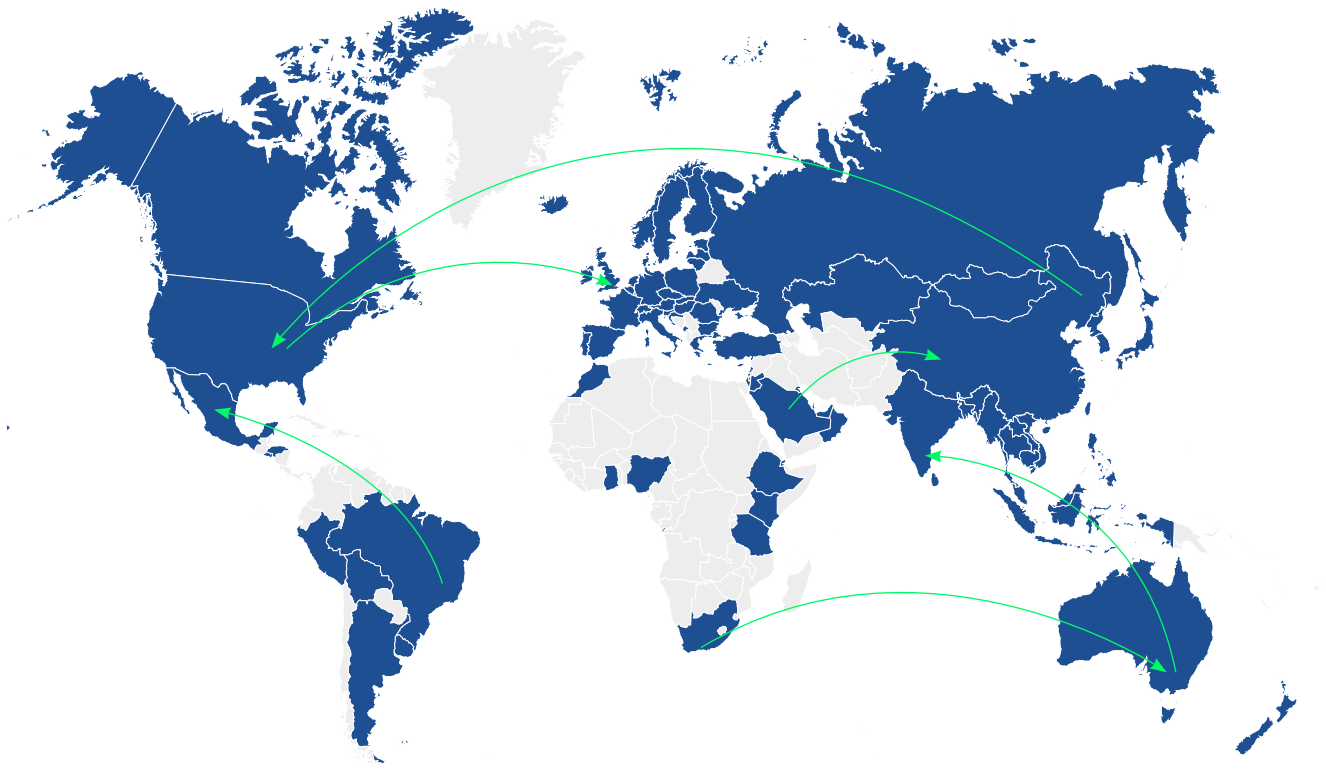
"Most of the time, the money jumps very fast from one account to another before eventually it just disappears from the electronic system through the cash withdrawal. It is about managing how quickly we can stop it while it is still in the electronic format."

This is something that criminals have always done to try to evade detection. However, the digitalisation of finance, while offering benefits for legitimate users, has created a new frontier for criminal exploitation. The speed and relative anonymity of online transfers allow criminals to move money rapidly and across vast distances with ease. This, coupled with the rise of international criminal networks and the increasing sophistication of money laundering techniques, makes cross-border payments an attractive avenue for criminals seeking to obfuscate their activities and maximise their profits.

The types of financial products and services available can restrict the ability of criminals to easily utilise cross-border transactions as a means of accessing their illicit funds. As Gary Yeoh, Chief Marketing Office at PayNet, highlights "There are some situations where somebody compromises your wallet account and they're able to then spend your money abroad, but actually they might as well just try and spend it domestically. There's no real reason to rush off to Thailand to try and spend something that is in a wallet. Most of our Malaysian wallets have a cap of 5000 ringgit. So, it's not worth compromising wallets versus scamming somebody with a Casa account."

Whilst over 80 countries now have domestic real-time payment systems (see map below), some are more widely used than others. The UK, for example, was the first major advanced economy to adopt a fast payment system in 2008 – reducing payment times from days to seconds. This early adoption of Faster Payments as a way to make payments as quick and frictionless as possible for the consumer will contribute to the view that the UK is a 'honey pot' for fraud and scam activity in comparison to other parts of the world where payments may be easier to track and freeze, meaning these jurisdictions present a higher risk for criminals. As such, the first challenge when tackling cross-border APP fraud is the speed of the transaction.

Figure 1- Countries that use real-time payments (Volt.io)



Challenges for the payments ecosystem

"The speed of identifying fraud and requesting a recall is one of the most important things to reduce the impact on customers."

Martin Low
Senior Payments Manager
KPMG

Speed of Transactions

One of the primary challenges in addressing Authorised Push Payment (APP) fraud, particularly in cross-border transactions, is the speed at which fraudulent payments can be identified and recalled. The faster these payments are flagged, and the recall process initiated, the better the chances of recovering the funds.

Fraudsters exploit the inherent speed of electronic 'faster' payments to rapidly move funds through multiple accounts, often withdrawing cash before the victim or bank can take action. The key is to intervene before the money exits the electronic system, typically within a narrow window of time.

However, international payments, which typically involve multiple intermediaries across different jurisdictions, inherently take longer to trace and recover. This delay can significantly increase the risk of the funds being lost before any action can be taken, especially in fraud cases where funds are quickly moved through multiple accounts.

The complexity of traditional banking infrastructures exacerbates the problem. In domestic contexts, many banks have systems in place that allow for faster recalls and tighter relationships between institutions. However, with cross-border payments, there is a lack of direct relationships between the sending and receiving banks, especially when intermediaries are involved. As a result, tracking and recalling funds becomes more challenging and time-consuming. Payments often pass through a chain of banks, each adding time and complexity to the recall process.

Unfortunately, while speed is essential for identifying and stopping fraudulent transactions, the process of recovering the funds can be excruciatingly slow. Gary Yeoh, Chief Marketing Officer, PayNet, explains "The process can take months. Firstly, the victim has to prove that the money belongs to them, and then get a police report. Secondly, the police would have to come in and verify that the money actually does belong to them. At least during the investigation, the money is still there."

Gary Yeoh
Chief Marketing Officer
PayNet

"The last we looked at this challenge, we worked out that we probably had a maximum of 45 minutes from the time you have transferred the money, give or take. Of course this depends on the amount too."

In jurisdictions such as Malaysia, there are systems in place to combat APP fraud, such as the National Fraud Portal. This system is managed by PayNet, the central payment switch for Malaysia, so when victims call 997, they trace the payment and share this intelligence with the financial institution which can freeze the payment whilst an investigation takes place. The victim needs to file a police report and prove ownership of the funds, law enforcement then investigates and works with the financial institutions to return the frozen funds to the victim. However, this is a lengthy process, often complicated by the number of transactions and financial institutions involved. Victims may wait months for reimbursement, as investigations involve police reports and proving the rightful ownership of the funds, slowing down the resolution further.

The complexity of international payment systems and how traditional banking infrastructures are often fragmented, involving multiple intermediaries and communication channels, further slows down investigations and recovery of funds.

KPMG

Martin Low
Senior Payments Manager
KPMG

> *"Domestically, schemes and close domestic bank relationships, cater for the need to retrieve funds quickly. However, when it comes to cross-border transactions, it can be more difficult as payments can move across different jurisdictions. The sending bank may not have a direct relationship with the beneficiary bank. Sending payments via correspondent banking adds more financial institutions to the payment journey which can make it much more difficult to service these payments."*

As Martin references, in the UK, the Payment Systems Regulator (PSR) regulation, which came into force on 7 October 2024[10], introduced a mandatory reimbursement scheme for victims of APP scams within the Faster Payments system. This regulation aims to incentivise payment firms to invest in robust fraud prevention measures by making them liable for reimbursing victims, subject to specific exceptions. The aim is that victims of APP fraud will be reimbursed quickly and not have to wait for funds to be found and frozen, so that the victim of fraud does not bear the cost of criminal activity.

However, the PSR regulation, focusing on APP scam reimbursement within the UK Faster Payments system, has limited direct applicability to cross-border payments. This is because:

1. The PSR primarily targets domestic transactions within the UK, specifically those using Faster Payments and CHAPS. It mandates reimbursement for APP scams where the fraudulent payment originates and ends within UK accounts. This is important since, as Braithwaite explains, "the first half of 2022 shows that international payments, not covered by any current or proposed reimbursement scheme, were the second largest type of APP fraud by value (£12.9 million)."[11]

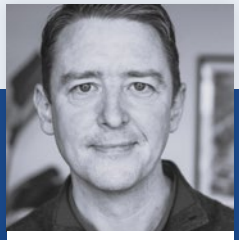
2. The PSR's reimbursement requirement applies only to transactions in GBP. Once a payment involves currency conversion, it falls outside the scope of the regulation, even if the initial fraudulent activity occurred in GBP.

3. The PSR's jurisdiction is limited to the UK. While a cross-border payment may involve a UK-based intermediary or payment institution, if the funds move out of the UK, the regulation's reimbursement requirements cease to apply.

4 Whilst the PSR acknowledges the role of Indirect Access Providers (IAPs) that enable non-UK institutions to participate in Faster Payments. The regulations place the onus on sending PSPs, rather than IAPs, to implement fraud prevention measures. While IAPs must provide information about their indirect PSP customers, they are not directly obligated to enforce the reimbursement rules.

This creates a potential loophole where fraudulent activity initiated through an indirect PSP outside the UK might not be subject to the same level of scrutiny or reimbursement requirements as a domestic UK transaction.

The PSR regulation, while a significant step towards protecting UK consumers, raises questions about its impact on cross-border payments. The limited scope and the challenges inherent in addressing cross-border fraud underscore the need for greater international collaboration and a more holistic approach that combines prevention, detection, and disruption of criminal networks.



Graham Ridley
Strategy Director
IFX

"The use of virtual IBANS can mean that a domestic transaction in scope for APP Fraud, owned by a party outside of the Country, say Canada, with access to a virtual account that has a British reachable faster payment sort code, once completed, can be followed by a cross-border payment to move the fraudulent funds to Canada. In this way, the faster payment function is appealing to criminals to launder money through the UK quickly and it enables the geographical jurisdiction of both fraudster and victim to be almost anywhere."

Regulatory environment

There is a general sense of frustration within the current regulatory environment, particularly in the UK, which is that regulators are too focused on punishing firms for fraud, rather than working with them to prevent it through the development of quality guidance and fraud standards. And that the PSR regulations, while well-intentioned, are poorly designed, with fears over the impact of implementing these rules.

These fears point to a disconnect between regulators and the practicalities of the financial services industry. There is a perception that those working in policy do not understand the practical implications of the regulations they are developing and have not thought through the operational challenges they will cause. The consensus across stakeholders was that consultations do not adequately address the concerns of the industry and leave grey areas and gaps in guidance for implementation or where too much discretion can be used by financial institutions and other stakeholders to create an uneven playing field.

The UK's regulatory environment is complex, with multiple regulators having a significant impact on how financial systems operate. Firms that process cross-border payments are often balancing conflicting rules and guidance as regulators do not always have a clear appreciation of how different firms operate, especially those operating in multiple jurisdictions. Braithwaite identifies this challenge by stating that "in the absence of a single body for the "regulatory oversight... of a broad range of payment scenarios, there is the risk that piecemeal arrangements emerge in response to APP fraud. Such arrangements, in turn, might be unduly complex for payment services providers, potentially detracting from initiatives to tackle fraud, and opaque and difficult for customers to navigate."[12]

Across the industry, there is an underlying feeling that policymakers don't always consider how regulations in different jurisdictions will interact with each other and how the context within which regulations occur often differs. This can create compliance challenges for firms that operate in multiple countries.

Nick Maxwell highlights that 'there is a fundamental disconnect between G20 policymakers responsible for payment system reform and those authorities responsible for fraud prevention and tackling financial crime'.[13] Maxwell argues that policymakers need to ensure that payments reform does not create new economic crime vulnerabilities or undermine existing defences against fraud and financial crime, something that financial crime consultants We fight Fraud highlighted alongside The Payments Association in a recent documentary, "The new APP fraud rules: What they mean for consumers, fraudsters and the UK", which focused on the impact of regulatory responses to APP fraud in the UK.[14]

Maxwell also indicates that there should be:

i. greater coordination and a sense of shared responsibility between payments and economic crime-related policymakers, internationally and at the domestic level;

ii. the establishment of a policy principle of 'economic crime security by design' in payments reform policy; and

iii. the deployment of a risk-based approach in faster cross-border payments that would enable customers to opt into safer corridors for payments, allowing for appropriate analysis, screening and the recall of payments where appropriate from a risk perspective;

iv. a greater understanding of how criminals abuse cross-border systems is needed;

v. full consultation with practitioners at all stages in the payments lifecycle who are working within the regulatory environments affected – something that this paper attempts to begin.

Broader than financial services

Getting to the bottom of how APP fraud scams occur in the first place suggests that cross-border APP fraud is broader than a financial services issue. Call spoofing is largely part of the problem. In the UK, call spoofing has been the focus of domestic and international cooperation, with the National Crime Agency shutting down 'Russian Coms' ', a call spoofing platform that facilitated 1.8 million scam calls. Between 2021 and 2024, over 1.3 million calls were made by Russian Coms users to 500,000 unique UK phone numbers. Of those who reported to Action Fraud, the average loss is over £9,400.[15] Similarly, in Europe, Europol shut down 12 fraud call centres in Operation Pandora, with cooperation from police forces in Germany, Albania, Bosnia and Herzegovina, Kosovo*,[16] and Lebanon.[17]

This illustrates how context is key for how regulation is received and put into practice. The same issue is occurring in different jurisdictions, with fraudsters utilising globally available tools to attack domestically and internationally. Global cooperation is also needed, but with active conflicts between jurisdictions, criminals take advantage of the lack of communication and exceptional wartime circumstances to attack conflict-affected areas and beyond. While financial institutions go on to bear the brunt of PSR regulations and reimbursement obligations, scams frequently originate outside the financial sector, with many across the financial services sector calling upon other bodies to also 'do their part'.

Social media platforms, with their vast user base and often lax security measures, provide fertile ground for fraudsters to connect with potential victims. The anonymity and reach offered by these platforms make them ideal for launching sophisticated social engineering attacks. There is a lack of consistent standards and accountability for such platforms, leading to calls for greater regulation and collaboration to address scams at their source. This has been actioned by some governments, with Singapore passing the Online Criminal Harms Act (2023). This sets out ex-ante requirements that online platforms must adopt, to better protect their consumers. It also allows authorities to order swift blocking of fraudulent accounts or content, to protect other users from falling victim to scams.[18]

Revolut, the global fintech with over 45 million global customers, is now, in light of the new PSR regulations around mandatory reimbursement of fraud victims, calling on Meta to commit to sharing reimbursement of fraud victims. Woody Malouf, Head of Financial Crime at Revolut, stated that what the industry really needs is giant leaps forward…social media platforms not only continue to enable fraud, but the issue is just as bad today as it was last year. Victims and financial institutions still ultimately bear the cost. These platforms share no responsibility in reimbursing victims, so they have no incentive to do anything about it. A commitment to data sharing, albeit needed, simply isn't good enough."[19]

bloomicon - stock.adobe.com

However, it is not simply that social media has facilitated APP fraud, which is seeing victims' money move all around the globe. Financial crime across these platforms has led to an erosion of trust in the digital economy.

This creates additional challenges within society around trust, which ultimately impacts upon business and the economy as people become unsure of who or what is trustworthy. The case of India provides a stark example, where rampant fraud originating from call centres has not only damaged the financial sector but also tarnished the reputation of India's legitimate outsourcing industry. This ripple effect underscores the broader economic consequences of APP fraud, extending beyond immediate financial losses. Toby Evans explains how AusPayNet's responded to this challenge:

Australian Payments Network
Connect Inspire Thrive

Toby Evans
Head of Economic Crime
AusPayNet

> *"We have collaborated with India, and they have been doing an awful lot to close down their scam compounds because it's impacting their legitimate economy with call centre and cyber security industries. A devastating unintended consequence. We have been working collaboratively with them to open better collaboration and intelligence-sharing. Scams are a global problem that require a global solution. We need to overcome data sharing and collaboration challenges to improve disruption."*

This small snapshot shows some of the broader consequences of APP fraud globally, demonstrating the issue of cross-border APP fraud and the transactions associated with it. A united and global approach is needed in order to combat the causes of APP fraud, such as call spoofing, and the harms of fraud to the economy through both financial and reputational losses. The regulation of social media and successful multi-agency, cross-jurisdictional law enforcement initiatives would mean that the pressure would be not just on financial firms to tackle the problem of APP fraud. However, as this is not the case currently, financial firms need to forge that path through the changing regulatory environment and find ways to cooperate internationally despite the challenges.

Lack of global standards

One challenge in tackling APP fraud and managing cross-border payments is the lack of standardised global approaches to fraud prevention and financial crime regulation. Cross-border transactions require navigating different regulatory frameworks related to KYC, AML, and fraud detection, all of which vary significantly across countries. As Martin Low states, "the complexity and lack of consistency of global standards around KYC, AML and fraud regulations makes them more difficult for banks to manage. Additionally, the huge volume of bank accounts offered in the UK and across the globe, combined with fintechs processing payments, creates an enormous volume of transactions which banks need to monitor...In addition, each player in the ecosystem has slightly different processes. These differences vary across regions and geographies, where banks apply different rules for KYC and AML."

The banking industry faces a multitude of different processes across regions and institutions, creating a patchwork of approaches to fraud prevention. This lack of consistency makes it easier for criminals to exploit gaps in regulatory systems, as the differing rules and practices across borders complicate efforts to create effective fraud prevention measures.

The absence of unified global standards in how fraud is tackled introduces vulnerabilities in the financial system. While initiatives like ISO 20022 represent a step toward standardising payment messaging systems, its implementation has been slow and inconsistent.

KPMG

"The sector is trying to bring in alignment. The ISO 20022 standard is a huge step forward in getting all players speaking the same language and sharing more information. It also opens the opportunity to build new value-add services that can help tackle fraud and financial crime."

Martin Low
KPMG

Many financial institutions use interim solutions, such as converters, which create further inconsistencies and risks. For instance, legacy systems with character limits might omit crucial information, potentially hindering efforts to detect and prevent fraud. There is a need for significant upgrades to banking infrastructure. Pavel Guzminov, CEO of Digidoe, states that the "current banking infrastructure while functional, has not kept pace with today's demands for speed, security, and data accuracy. Even with advancements like ISO20022, many banks are limited by rigid data frameworks and manual processes, which significantly impact transaction quality and customer satisfaction.

Even in countries like the UK, where regulations offer protections for internal payments, the definition of "cross-border" payments remains unclear, which is important since the UK's regulations for APP fraud state that the liability does not extend cross-border. Borders are not just international but also institutional. A payment sent within the same bank across different countries may not be considered cross-border, complicating liability and protections. Additionally, the rise of decentralised finance (DeFi) and blockchain systems introduces new layers of complexity, as these transactions often occur outside of traditional banking borders and regulatory frameworks.

Data sharing limitations

Cross-border APP fraud presents significant challenges due to time constraints and the lack of global standards or agreement on how fraudulent transactions should be prevented, detected and dealt with. These two main challenges reveal a third, which is how data sharing limitations, both domestically and globally, present a major obstacle to effective fraud prevention and recovery efforts.

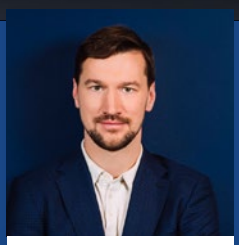
This stems from jurisdictional boundaries, varying data privacy regulations, and the fragmented nature of the global financial system, all of which hinder collaboration and visibility across institutions and borders.

Strict data privacy laws, such as the EU's General Data Protection Regulation (GDPR), are designed to protect individuals' privacy but can unintentionally impede fraud investigations. While privacy protections are essential, the challenge lies in balancing the rights of individuals with the need to share data quickly to prevent financial crimes. Institutions operating across multiple jurisdictions often face conflicting demands, needing to comply with privacy regulations while still participating in global efforts to combat fraud.

Lynx

Daniel Mcloughlin
Head of Pre-Sales
Lynx

"We now have a regulation in the UK that says internal payments have protections for APP Fraud…both parties have a liability that falls away with cross-border. But then what do we define as the border? You've got the traditional cross-international borders, but the bank has its borders as well. You could be making an international payment to the same bank; is that a cross-border payment? The bank has full control over that - so where are we drawing the borders? Is it outside of the financial institution? Is it outside of the regular financial system and into a defi system or a blockchain? These are different areas that we have to consider and cut cloth accordingly. I think there's still a lot to do."



Taavi Tamkivi
CEO & Founder
Salv

"APP/ impersonation fraud is crossing borders and, for example, the Baltic network will need to be connected with the UK network. If our industry doesn't align on business, security, and privacy standards, we risk a scenario like GSM: one standard operating in each country, but no consistent connectivity or simple options for international communication. I'm not looking at governments or regulators to fix this. Rather, it's an opportunity for our industry and technology providers to self-regulate. We need to set and adopt the standards to ensure we can communicate effectively across borders — and I can ensure there are already working best practices being set for this."

Countries across the globe have different legal frameworks that regulate how data can be shared, particularly regarding financial information and personal data. These discrepancies make cross-border investigations difficult, as institutions in one jurisdiction may be hesitant or legally restricted from sharing information with entities in another. Jurisdictional limitations often prevent the timely exchange of critical data needed to track and recover funds in cross-border APP fraud cases.

The global financial system is highly fragmented, consisting of a wide range of financial institutions, payment networks, and regulatory bodies. These entities often operate in silos, with distinct systems, procedures, and data management protocols.

The intricate web of banks, fintechs, and varying regional regulations creates a "complex environment" where data silos and inconsistent KYC/AML rules hinder effective collaboration. Different links within the payment chain can also add or remove the ability to share data and truly know the customer.

The siloed nature of different teams within financial institutions that often deal with KYC, AML, and fraud separately further complicates efforts to track and disrupt cross-border fraud. This fragmentation is exacerbated by the sheer volume of transactions and the speed at which funds can be moved across borders, making it difficult to follow the money trail and recover stolen funds.

thepaymentsassociation.org/working-groups/cross-border

"As long as (the money) remains within banks, we have full visibility and our chances to pick it up are much better than if they put it into other funds as well in the network – such as crypto. It gets really hard when it comes to peer-to-peer crypto…(we have overcome this by) not supporting our customers to use crypto. We have quite strong controls on it. These are working well."

Fraud Lead
UK Financial Institution

The rise of cryptocurrency

Cryptocurrency's rise has also seen an increase in scams and fraudulent schemes, with criminals taking advantage of the hype and public unfamiliarity with digital currencies. The complexity of the market makes it challenging for individuals to distinguish between legitimate investments and scams. But cryptocurrency is not simply a ploy for criminals to defraud, but also a means for criminals to move funds across borders and exit illegally obtained money from the legitimate financial system.

The integration of cryptocurrency into the financial system has created new challenges in combating fraud, particularly due to the anonymity and decentralised nature of digital currencies. As noted by industry experts, once money is converted into cryptocurrency, it becomes much more difficult to trace, making it a favoured tool for criminals involved in money laundering and fraud.

While traditional banks offer greater visibility into transactions, crypto's peer-to-peer structure and lack of comprehensive regulation in certain regions provide criminals with opportunities to obscure their activities. Some financial institutions have addressed these challenges by restricting their customers' access to cryptocurrencies, implementing strict controls to prevent crypto-related fraud.

While these measures are currently effective, the broader financial industry and law enforcement agencies continue to grapple with the complexities introduced by cryptocurrency's potential misuse. The lack of global regulatory frameworks for cryptocurrency exacerbates this issue, as inconsistent KYC and AML requirements across jurisdictions enable criminals to exploit gaps and move funds across borders undetected. Working with digital currency exchanges, a key off-ramp for laundering funds, is essential in the fight against financial crime. his has led to cryptocurrency contributing to the 'dark figure' of financial crime, where we have no real indication how much APP fraud relates to cryptocurrency.

To effectively combat cryptocurrency-related fraud, a multi-faceted approach is necessary. This includes strengthening KYC and AML regulations for cryptocurrency exchanges, improving law enforcement collaboration across borders, and raising public awareness about the risks and safety measures in cryptocurrency investments. All of this is dependent upon regulating a sector, which is by design, unregulated. Therefore, very unlikely to respond positively to the changes needed. Financial institutions must also implement enhanced fraud prevention measures, such as more robust authentication and transaction monitoring systems, while actively cooperating with authorities to track down and prosecute offenders. Without these coordinated efforts, cryptocurrency will remain a significant vulnerability in the global fight against financial crime.

Opportunities to combat cross-border APP fraud

Leveraging technology

Real-time payment systems, while presenting new risks, also offer opportunities to use technologies like AI and machine learning for real-time monitoring, faster detection of fraudulent activities, and quicker response times.

SWIFT is trying to do more to reduce fraud in cross-border payments through the introduction of AI-powered fraud detection. Launching in 2025, this new capability builds on Swift's existing Payment Controls Service, used by many small and medium-sized financial institution, and uses AI to analyse vast amounts of pseudonymised data from global transactions, enabling real-time detection and flagging of suspicious activity. By leveraging cutting-edge technology and collaborating with over 11,500 banks and financial institutions worldwide, Swift aims to enhance security and resilience in the financial ecosystem. This initiative highlights the potential of AI to provide more accurate fraud insights, reducing risk and improving trust in global payments.

Swift

Jerome Plens
Chief Product Officer
Swift

"Swift has been working with leading global financial institutions to explore how federated learning, combined with privacy-enhancing technologies, could enable market participants to share information without revealing their proprietary data. The group has so far developed a number of fraud detection use cases which are set to be tested in a sandbox environment."

Mastercard has announced a similar initiative with updates to its Consumer Fraud Risk (CFR) solution, designed to help UK banks better detect and prevent real-time payment scams. These improvements focus on providing banks with enhanced visibility into potentially fraudulent transactions through AI-powered insights, although planned to have global reach, these insights still remain in the UK only at present.[20]

Mastercard's AI solution has supported 11 UK banks in identifying fraudulent payments before funds leave a victim's account. The system assigns a real-time risk score based on multiple transaction data points, alerting the sending bank of any suspicious activity. However, the latest enhancements now extend these fraud detection capabilities to receiving banks, enabling them to act quickly when payments are heading towards potentially fraudulent accounts, often referred to as 'mule accounts.' Network analysis can be used to trace the flow of funds and identify money mule accounts. This can be challenging, however, as criminals often use multiple accounts and move money quickly, but it is something that fintechs in the payments space, such as Wise, are leading the way by often developing a range of AI models 'in-house'.

"Preliminary tests of Mastercard's new 'inbound risk' alerts have shown a 60% improvement in a bank's ability to detect high-risk mule accounts. This AI-driven advancement could play a crucial role in reducing the impact of APP fraud, which fell by 12% in 2023, from £389 million to £341 million, according to PSR data."

Johan Gerber, Executive Vice President of Security Solutions, Mastercard

Utilising this much data about the payment allows compliance teams to be able to categorise risk more accurately and make decisions. But AI does have its limitations. Models are only as good as the data they are taught with, which requires accurate data about fraud that has already occurred.

Technology can not only help detect fraud, but also prevent it. APIs can connect different systems and allow for the sharing of data and intelligence between institutions, improving risk detection and fraud prevention. For example, a UK Finance pilot showed that Enhanced Fraud Data (EFD) sharing between sending and receiving firms can significantly improve fraud detection.[21] This is particularly important in cross-border payments, where there are often gaps in data sharing due to jurisdictional differences.

Across the industry, privacy concerns and GDPR compliance are cited when discussing the ability to share data, but technology can and is being utilised to share intelligence securely and safely between banking institutions globally (see the opportunity of tokenisation below).

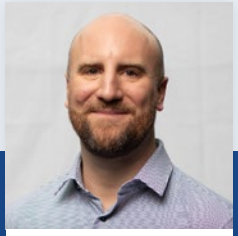
The technology exists to collaborate securely with financial institutions across the world; all it requires is understanding and implementation. This is more of a cultural shift than a technical challenge.

Technology can also be used to implement stronger authentication methods, such as biometrics, to protect customer accounts from takeover. This is especially important as criminals are using increasingly sophisticated methods, such as generative AI, to impersonate legitimate users. It can also be used to re-imagine payment processes to challenge APP fraud social engineering tactics.

Moving from a push payment system to a pull payment system for high-value transactions could enhance security. Implementing pull payments would require the recipient to be authenticated before funds are released, reducing the risk of unauthorised transfers. As Greg Hancell, Head of Product – Fraud at Lynx Tech, explains "I would perhaps change it from push payment to pull payment, where the person who they want to give money to has to pull the payment from their account. Right now, the issue is we push a payment, and we don't know where it's going to."

Hancell continues, adding "Historically, it was more complex to send a large value transfer, and people would use CHAPS which came with a transaction cost and required effort to make the payment by verifying the person you are paying. I recommend that a similar approach is taken for large value payments and to decouple from smaller push payments. So, people must think about the financial repercussion of the transfer and slow it down using an appropriate technology for a large value payment or life changing sum of money."

Overall, technology presents a significant opportunity to enhance fraud detection and prevention in cross-border payments and APP fraud. By leveraging the power of AI, APIs, and other innovative technologies, the financial industry can work together to create a safer and more secure payment ecosystem.



Lynx

Greg Hancell
Head of Product – Fraud
Lynx Tech

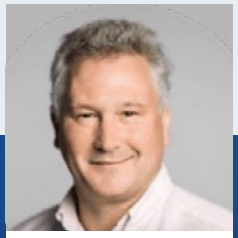
> *"We're adding technical barriers at the wrong place. The focus of the customer is on completing the authentication process rather than focusing on identifying who they are sending the money to and for what amount."*

Tokenisation

At its core, tokenisation is the process of replacing sensitive data, like bank account numbers or payment card details, with a unique identifier or "token." This token can be used to complete a transaction but is useless if intercepted by fraudsters because it does not reveal the underlying sensitive information.

Tokenisation offers cross-border payments enhanced security by minimising the risk of hacking or data leakage by ensuring sensitive financial information is not exposed at any point in the process. Tokens can be passed through systems, and only authorised parties (like the issuing bank or payment processor) can decrypt and use the original data. Tokenisation reduces friction in cross-border payments, as it allows for faster processing by bypassing the need to repeatedly verify sensitive data. This can accelerate the settlement times, which are often longer in international payments due to currency exchanges, compliance checks, and multiple financial institutions being involved.

It can also offer global consistency as it can work across different countries and payment systems, creating a more standardised approach to handling data and reducing the complexity of managing various local regulations and compliance standards. And it can minimise exposure to fraud in transit, as stolen tokens cannot be used to conduct unauthorised transactions. Even if a token is intercepted during the payment process, it is meaningless to the attacker without access to the tokenisation platform.



Dr Mark Goldspink,
Ambassador
The Payments Association

"Tokenisation is already being trialled in the cross-border space by 41 financial firms across the world under Project Agorá. This will not only strengthen the payments system itself, but can also offer a solution to the challenges of data sharing limitations that the industry currently faces."

Project Agorá's[22] aim is to perform screening at the start of the payment process and to share it across the banks, helping to reduce the needs for every bank doing the same compliance checks independently, sometimes with different results. A key benefit of tokenisation is there is no separation of the message and money movement, which should avoid leaving money in limbo.

The benefits of tokenisation when combatting APP fraud are dynamic token generation, with each token generated for one-time use or specific transactions, ensuring that even if one token is compromised, it cannot be reused for future fraudulent transactions.

Coupled with how tokenisation can be combined with real-time validation mechanisms to verify the authenticity of a transaction, ensuring that funds are being sent to a legitimate recipient. It also ensures that sensitive details (such as account numbers) are never directly exposed to the payer or intermediaries, reducing the risk of APP fraud.

Finally, tokenisation can help elevate traceability as it can provide a more traceable record of transactions, making it easier to identify the source of any fraudulent activity. In the event of an APP fraud, tracing the token can help investigators understand how the fraud occurred and potentially recover funds faster.

Tokenisation reduces data exposure, holds less interception risk (for both payment data and compliance messaging) and improves authentication overall. Tokenisation can significantly strengthen the security of cross-border by offering safer transactions, faster payment processing, and better fraud monitoring. It is important to note that technology, including tokenisation, is only part of the solution. Collaboration between financial institutions, regulators, and law enforcement is also essential. Sharing data and best practices can help to close the gaps that criminals exploit, but the culture and policy infrastructure needs to be in place in order to utilise advances in technology for both payments and data sharing.

Collaboration

Collaborative initiatives in cross-border payments and APP fraud prevention demonstrate the power of joint efforts in disrupting criminal networks. Examples such as the international communique signed in the UK[23] and data sharing agreements between Australia and India, as well as significant international partnerships, focused on combatting fraud through shared good practice,[24] highlight the potential for global cooperation to combat financial crime.

PayNet's model plays a pivotal role by enabling cross-institution communication and tracking payments, providing banks with timely intelligence to act on suspicious transactions.

This proactive reporting is crucial, as criminals often rapidly move money through multiple accounts and banks to avoid detection. By notifying banks when fraudulent funds are detected, PayNet helps freeze or hold accounts before the money can be further moved. Lim Wee explains how PayNet "provides intelligence to the bank saying, 'Look, the money is in your bank right now. Please do something about it.' Usually, the bank will take the signal from us, and they will earmark to either freeze or hold the account before allowing any other movements."

Lifting regulatory standards, as suggested by industry experts, would tighten the net on fraud, benefitting both the fight against financial crime and the commercial sector. Furthermore, agreeing on industry-level standards for communication between institutions could vastly improve the speed and efficiency of cross-border fraud prevention efforts, ensuring a coordinated response to criminal activity across jurisdictions.

Governmental, top-down leadership in the strategy and implementation of collaboration between geographical jurisdictions can drive industry behaviour and ensure that collaboration is prioritised and resourced. The new PSR regulations in the UK are designed with this in mind. However, as Taavi highlights, this doesn't need to be operationalised at a governmental level - it is something the industry has within its power now. This is particularly pertinent given that the clock has now run out for financial firms in the UK; mandatory reimbursement of fraud victims is here and has to be dealt with now. There has never been greater urgency. Waiting for international cooperation across Governments to lead this collaboration project will damage the industry, create more victims and see further growth in APP fraud within cross-border payments.

> *"Individuals move money rapidly which breaks into like, three, four pieces. They hop into three, four banks, then three, four mule accounts, then it hops again. These guys are pretty efficient."*
>
> **Gary Yeoh**
> **PayNet**

thepaymentsassociation.org/working-groups/cross-border

Australia: A case study

Toby Evans, AusPayNet

"In Australia we have the view that there is a corporate responsibility on every industry in the scam value chain to do their part. We expect real action, and we expect a collaborative approach. Regulating one industry alone will not effectively mitigate scams. We call it our ecosystem approach."

In Australia, the government has taken a leading role in combating scams by establishing the National Anti-Scam Centre.[25] This government-led approach has fostered a collaborative "ecosystem approach" that brings together stakeholders from various sectors, including government, law enforcement, banks, and telecommunications companies. This approach aims to share best practices, overcome challenges, and develop coordinated strategies to combat scams.

Focus on prevention and early intervention

Australia's approach prioritises scam prevention and early intervention measures. The country's scam prevention framework aims to hold all enablers of scams accountable across the value chain. This includes setting minimum expectations for businesses to implement scam prevention measures and imposing liabilities for failing to meet those expectations. Australia also emphasises proactive measures like intelligence sharing, website takedowns, and enhanced customer due diligence to disrupt scams before they occur. In contrast, the UK's focus on mandatory reimbursement has been viewed as reactive and primarily focused on compensating victims rather than preventing scams.

Australia recognises the importance of data sharing and network analysis in combating scams. The country is working towards building a robust data sharing component within its scam prevention framework. This data sharing aims to enable effective funds tracing, identification of money mules, and disruption of fraudulent networks.

What does Australia's ecosystem approach look like?

Instead of placing the burden solely on banks, the Australian model expects all stakeholders in the digital economy to play their part in preventing scams. This includes telecommunications companies, digital platforms, and government agencies, fostering a collaborative effort to combat scams.

Toby Evans, AusPayNet

"In Australia, we've seen that erosion of trust across the whole digital economy, like all the other countries in the world have. And that's from the telecommunications network where people are not answering their phone anymore. Businesses can't use clickable links. With digital platforms consumers cannot trust advertising whether it on investment or online shopping scams. In the payments industry, confirming who you're going to pay, and overcoming the challenges of the rapid mulling of funds, tracing and recalling the proceeds of crime."

Key to combatting this is government leadership. The Australian government plays a leading role in coordinating efforts and establishing a national strategy. The establishment of the National Anti-Scam Centre, led by the government, is cited as crucial in overcoming the blame game and enabling effective action.

Launched in July 2023, the NASC seeks to incentivise all participants in the scam lifecycle to meet their obligations to stop scams. Through its advisory board, fusion cells and working groups (in which AusPayNet participates), it brings together all key participants: financial institutions, other payment service providers (PSPs), digital communication platforms (DCPs), telcos and internet service providers (ISPs), digital currency exchanges (DCEs), consumers, and law enforcement.

Australian law enforcement identified that victims of card scams were more likely to go on to become victims of even higher-value scams, so in their day of action they disrupted about 30 SIM boxes controlled by transnational organised crime. Each SIM box held about 300 SIM cards, and each SIM card could send an SMS every two seconds across the country. Moreover, the NASC operates a website takedown service and has removed approximately 7,000 malicious websites and advertisements over the past year – or about 20 a day. This programme initially focused on investment scams but has now expanded to online shopping and other phishing sites. By utilising this evidence-based approach they could target 'low-hanging fruit' before it became a much bigger fraud problem.

Australia's approach emphasises the importance of data sharing and intelligence gathering to identify trends, vulnerabilities, and best practices. This involves sharing information on scam methods, money mule networks, and high-risk jurisdictions between banks, law enforcement, and other relevant bodies.

Toby Evans, AusPayNet

"We've had some significant data breaches in Australia followed by criminals using that stolen data to open mule accounts and commit other crimes including scams and fraud. Work is underway to ensure we identify who is producing documents to open accounts and critical services."

Australian Financial Crimes Exchange (AFCX) has established an open intelligence loop for better data sharing between the government and all industries in the scam ecosystem. Once a scam is reported to a bank, the enablers of scams will be expeditiously closed. The AFCX has also developed a fraud reporting exchange to enhance tracing and repatriation between banks and digital currency exchanges. However, the challenges of real-time payments mean effectiveness is limited to when a consumer identifies and reports a scam.

Codes and Standards become central to managing expectations and the Australian government's focus is now on developing a scam prevention framework with clear codes and standards for different sectors. These codes would establish minimum expectations and hold entities accountable for not meeting them. Consumer reimbursement in cases will then be considered where sectors fail to meet the established codes and standards. This ensures accountability and incentivises best practices across different industries.

Has Australia found a 'one size fits all' solution?

Australia's ecosystem approach to combatting scams seems to be achieving results, with government data showing a 13% reduction in scam losses for CY22 to $2.74 billion. However, as government and industry mitigants are implemented across the digital economy, members now report between 30 - 50% reductions in scam losses year on year.

The success of the Australian model relies heavily on strong government leadership and a willingness to invest resources. Replicating this in other countries might be difficult if governments lack the political will or financial capacity. Addressing cross-border scams necessitates international cooperation in information sharing, law enforcement, and extradition. The current lack of global coordination is a significant obstacle, with scams often originating in countries with different legal frameworks or enforcement capabilities.

Sharing data between different entities, especially across borders, raises significant privacy concerns. Countries have varying data protection laws, which could hinder the transfer of information necessary for effective scam prevention. But even where these rules are compatible, there can still be constraints on resourcing. Implementing the Australian model requires significant resources for establishing new agencies, developing and enforcing codes, and facilitating data sharing. Smaller countries or those with limited resources might find it challenging to replicate this model fully.

Toby Evans, AusPayNet, reminds us of the three important pillars that need to be understood and actioned to get ahead of the fraudsters and protect consumers from the harm of financial crime globally:

1. Consumer awareness is one of the best tools in mitigating cybercrimes and coordinated multichannel consumer awareness campaigns would help to educate and build resilience.

2. For Australia, the Government's proposed anti-money laundering and counter-terrorism funding (AML/CTF) reforms will be essential to overcome the limitations created by the tipping-off provision to facilitate improved data sharing and effectively mitigate money laundering networks, including the establishment of mule watchlists to improve customer onboarding and detection.

3. Scams are a global problem perpetuated by transnational organised crime. Scams must become a strategic priority for law enforcement, supported by effective global partnerships and joint operations. Criminals must fear being caught. Scams cannot continue to be a low-risk, high-reward crime. Disruption can identify strategic intelligence for industry and regulators on where and how they can close exploited vulnerabilities across the digital economy.

Combating cross-border APP fraud: A call for global collaboration and technological innovation

Combatting APP fraud and scams in an increasingly interconnected world requires a global, collaborative approach that goes beyond individual countries' efforts.

Addressing the challenges of inconsistent regulations, fragmented infrastructure, and data sharing limitations is crucial for effective international cooperation. Embracing opportunities to share best practices, leverage technology, and develop a common understanding of the problem can pave the way for a more secure and resilient global payment ecosystem.

The complex and evolving nature of cross-border APP fraud underscores the urgent need for a multi-faceted approach that goes beyond reactive measures. Combating this growing threat requires a paradigm shift from focusing solely on reimbursement to proactively addressing the entire fraud lifecycle, from origination to money movement.

There is a critical need to move beyond the traditional silos within the financial industry and foster a collaborative ecosystem that encompasses law enforcement, regulators, technology providers, social media companies, and merchants. This collaborative approach, exemplified by Australia's successful model, emphasises data sharing, intelligence gathering, and shared responsibility across all stakeholders.

Technology plays a pivotal role in this fight. AI and machine learning offer the potential for real-time transaction monitoring, faster fraud detection, and enhanced security measures. APIs can facilitate seamless data sharing and intelligence exchange between institutions, improving risk assessment and fraud prevention. Moreover, exploring innovative payment models, such as pull payments for high-value transactions, could significantly reduce the risk of unauthorised transfers.

Addressing the broader societal impact of APP fraud is equally crucial. Building trust in the digital economy requires not only robust fraud prevention measures but also effective law enforcement actions against scammers and increased public awareness about the risks and prevention strategies.

A global, unified approach is essential to tackle the cross-border nature of APP fraud. This includes:

1. Developing standardised data sharing protocols and overcoming legal barriers to facilitate international cooperation in investigations and intelligence sharing.
2. Harmonising regulatory frameworks and KYC/AML requirements across jurisdictions to close the gaps that criminals exploit.
3. Working collaboratively with social media platforms to address scams originating on their platforms and hold them accountable for enabling fraudulent activities.
4. Investing in advanced fraud prevention technologies and promoting their adoption by financial institutions worldwide.

By embracing these collaborative and technology-driven solutions, the global community can strive towards a safer and more resilient financial ecosystem, safeguarding individuals, and businesses from the devastating consequences of cross-border APP fraud.

Sources

1. https://www.ecb.europa.eu/paym/groups/pdf/omg/2023/230323/item_2_cross_border_payments.en.pdf
2. https://www.fintechfutures.com/2023/02/singapore-and-india-link-up-paynow-and-upi-for-real-time-cross-border-payments/
3. https://www.ebaclearing.eu/news-and-events/media/press-releases/6-october-2022-immediate-cross-border-payments-ixb-pilot-set-to-revolutionise-international-payments/
4. https://www.swift.com/our-solutions/swift-gpi/instant-cross-border-payments
5. https://www.bis.org/about/bisih/topics/cbdc/icebreaker.htm
6. https://www.bis.org/about/bisih/topics/cbdc/jura.htm
7. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm
8. https://www.iso20022.org/
9. https://www.irs.gov/pub/irs-tege/fin104_ctr.pdf
10. https://www.psr.org.uk/publications/policy-statements/ps234-app-scams-reimbursement-policy-statement/
11. *Braithwaite, J (2024) 'Authorised Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like?' Journal.*
12. *Braithwaite, J (2024) 'Authorised Push Payment' Bank Fraud: What Does an Effective Regulatory Response Look Like?' Journal of Financial Regulation, 10, 174–193.*
13. *Maxwell, N (2024) "Speed at the expense of safety? Economic crime security concerns in the implementation of the G20 Roadmap for Enhancing Cross-border Payments" Journal of Payments Strategy & Systems, Volume 18 / Number 1 / Spring, pp. 9-19(11).*
14. https://www.youtube.com/watch?v=vjC2rNKGM0k
15. https://www.nationalcrimeagency.gov.uk/news/nca-shuts-down-major-fraud-platform-responsible-for-1-8-million-scam-calls
16. **This designation is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.*
17. https://www.europol.europa.eu/media-press/newsroom/news/operation-pandora-shuts-down-12-phone-fraud-call-centres
18. https://www.mddi.gov.sg/media-centre/press-releases/measures-to-protect-singaporeans-against-online-scams/#:~:text=In%20July%202023%2C%20we%20passed,from%20falling%20victim%20to%20scams
19. https://www.revolut.com/news/it_simply_isn_t_good_enough_revolut_calls_for_meta_to_commit_to_sharing_reimbursement_of_fraud_victims
20. https://www.bobsguide.com/mastercards-new-ai-update-targets-real-time-payment-scams/?mkt_tok=MjQzLU1SUi00NTkAAAGVx5kNCpSjX4orISmtR9sbLofd4DGvPYFyQ4JZm7g07NbXOGMFEvL-cIuogb-HN_BH5WAR85fASemY8h2DwgZ91aSRoRW3zQp1aK85FtvNd4WWDDzS
21. https://www.wearepay.uk/enhanced-fraud-data-efd/#:~:text=Enriched%20data%20sharing%20between%20banks,with%20existing%20fraud%20monitoring%20tools
22. https://www.ledgerinsights.com/41-institutions-join-bis-tokenized-cross-border-payment-project-agora/
23. https://www.gov.uk/government/publications/communique-from-the-global-fraud-summit
24. https://www.counterfraud.gov.au/news/general-news/australia-deepens-collaboration-international-partners-combat-public-sector-fraud
25. https://www.nasc.gov.au/what-we-do/collaboration

About the Author

Nicola Harding, CEO, **We Fight Fraud**

Dr. Nicola Harding is the CEO of We Fight Fraud, a pioneering organisation dedicated to combating fraud and financial crime through innovative methods. With a PhD in criminology, she is an expert in fraud prevention, cybercrime, and financial crime. An advisor to UK Government, Dr. Harding's career has been marked by her passion for bridging the gap between academia and industry, using research and technology to design practical solutions to combat fraud.

As the CEO of We Fight Fraud, she leads a multidisciplinary team of former law enforcement professionals, cyber experts, and crucially, experts with lived experience. Together, they provide bespoke solutions, including education, training, and advisory services, to help businesses and governments combat emerging threats. Under her leadership, the organisation has become a trusted partner in the fight against fraud, blending innovation, expertise, and practical insight to tackle this global issue.

Dr. Harding's work continues to shape the field of fraud prevention, making her a leading figure in the fight against financial crime.

About the Contributor

Mark Goldspink, Ambassador, **The Payments Association**

Mark is a well-networked, entrepreneurial, and innovative senior board-level leader with extensive hands-on experience in global fintech and mobility SaaS solution innovation. His expertise spans various domains, including AI and real-time machine learning technologies, crossboard/alternative payments methods, universal merchant commerce technologies, and adoption of secure cloud services.

The Interviewees

Cross-Border Payments Working Group

The Cross-Border Payments Working Group has the specific purpose to help identify and increase awareness of the technology in the market that is transforming the cross-border payments ecosystem for its users and providers, as well as informing the evolving regulatory landscape.

Cross-Border Payments Working Group Committee Members

Gary Palmer
CEO
Payall

Kamran Hedjri
Founder and Group CEO
PXP Financial

Noyan Nihat
Advisory Board Member
The Payments Association

Alex Lambeth
Head of Public Affairs
Crown Agents Bank

Matt Williamson
SVP & Industry Principal
Endava

Kamal Naidu
Global Head, Strategy and Insights
PXP Financial

Martin Low
Senior Manager, Financial Services Consulting
KPMG

Robert Turner-Kerr
Senior Relationship Manager
iFAST

Bert de Munter
Product Manager
FIS

Christian Agius
Co-Founder and CEO
Fyorin

Sudeepta Das
Founder
Cohesive Architecture

Natalie Lewis
Head of Fintech, Market Infrastructure and Payments
Travers Smith

Graham Ridley
Strategy Director
IFX

William Lorenz
UK Country Director
Arf

Peter Wilson
Industry Advisor
Fujitsu

Pavel Guzminov
Founder and CEO
DigiDoe

the payments association

About The Payments Association

The Payments Association is the largest community in payments. Founded in the UK in 2008, the association now operates communities in the UK, EU and Asia, helping almost 300 companies enhance their commercial interests, solve societal problems such as financial exclusion and evaluate new opportunities for innovation in payments.

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 our annual conference PAY360 and awards dinner, CEO roundtables and training activities.

We run seven stakeholder working Project groups: Cross-Border, Digital Currencies, ESG, Financial Crime, Inclusion, Open Banking and Regulatory. 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 conduct exclusive industry research. This research is not legal advice. It is made available to our members through our Insights knowledge base to challenge and support their understanding of industry issues. This includes whitepapers, insightful interviews and tips from the industry's most successful CEOs.

---

the payments association

St Clement's House, 27-28 Clement's Lane, London EC4N 7AE
Tel: +44 20 3540 9760
Web: www.thepaymentsassociation.org
Email: info@thepaymentsassociation.org
@ThePAssoc
The Payments Association