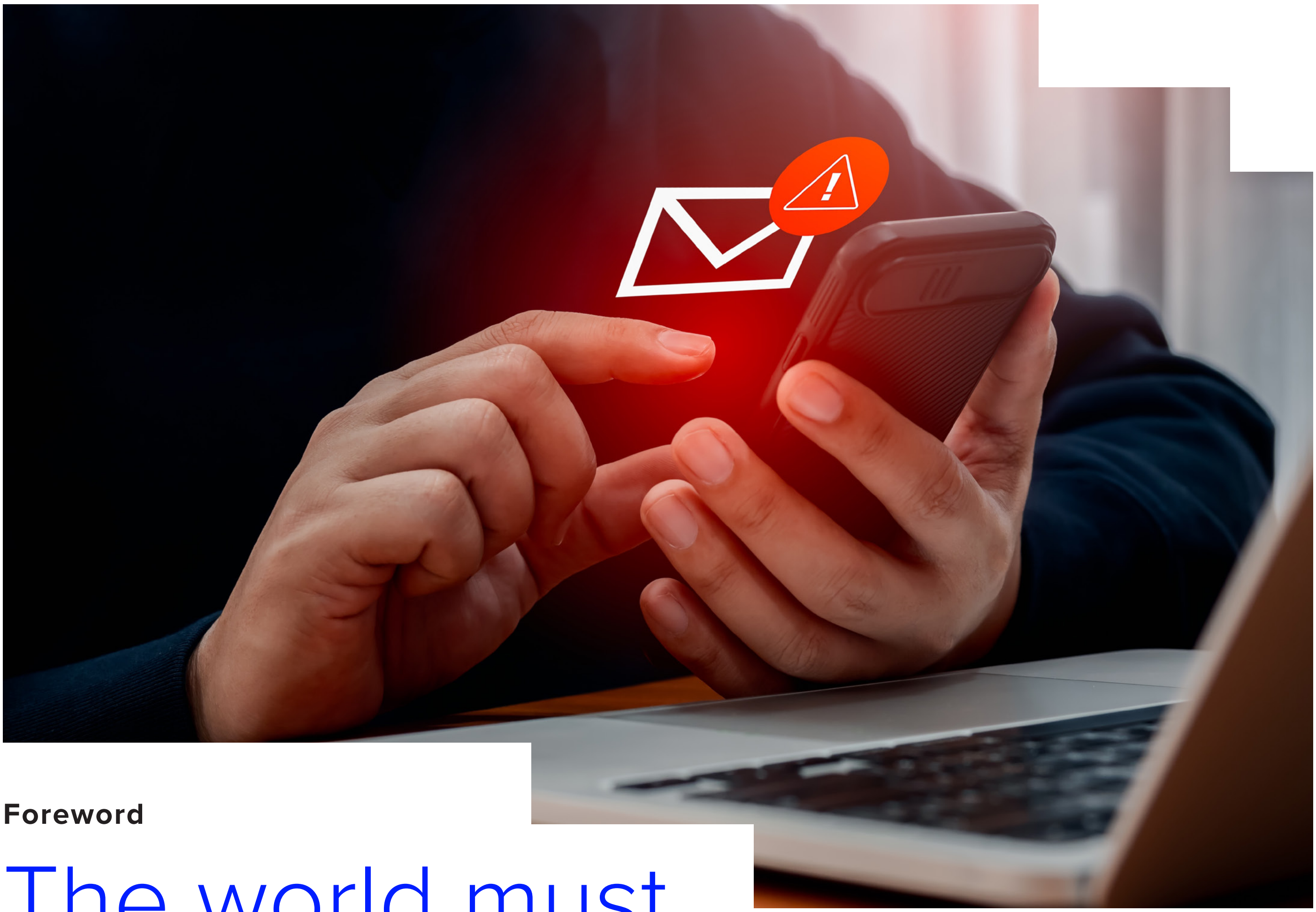
Defeating Authorised Push Payment (APP) fraud

How to ensure going global brings rewards, not risks

LSEG RISK INTELLIGENCE

Contents



Foreword

The world must tackle APP fraud

Dal Sahota,
Global Head of
Trusted Payments

The rapid growth of cross-border payments, driven by globalisation, remittances, e-commerce, and technological advances, presents both significant opportunities and increased risks. One of the most serious threats is authorised push payment (APP) fraud – also referred to as relationship and trust scams or credit push fraud. This type of fraud involves criminals tricking victims into authorising payments by using false information or deceptive claims.

As APP fraud continues to increase globally, it is crucial to examine the vulnerabilities in cross-border payment systems, such as regulatory differences, the proliferation of instant payments, complex transaction processes, and limited data sharing, all of which make scams easier to carry out. There is also an urgent need to raise awareness about the growing sophistication of relationship and trust fraud, including the use of artificial intelligence (AI) for impersonation.

The paper addresses these concerns and reviews global efforts by governments and other organisations to combat credit push fraud, focusing on policies and collaborative strategies. It highlights the importance of continuous monitoring and proactive prevention. Finally, it explores how organisations of all types, including companies, fintechs and banks, can protect themselves and their customers by adopting innovative technologies – such as real-time bank account verification– to enhance security, build trust, and ensure compliance with evolving regulations.

1 Introduction: The rise of cross-border payments

Cross-border payment volumes are increasing, rising from $150 trillion in 2017 to an expected $250 trillion by 2027.[1] Several factors are driving this growth. First, despite current geopolitical uncertainty and increased complexity in supply chains, in part due to the pandemic, economic growth continues in many areas and a growing number of small and medium-sized enterprises (SMEs) are expanding internationally.

Second, as a result of global migration and international employment, remittances are a steadily growing source of payment flows. Third, and perhaps most importantly, the rise of e-commerce and improved logistics have made it easier for consumers to shop from global retailers. Smart retailers have adapted their offer by providing international payment options to appeal to customers.

Technology has enabled this trend. Digital wallets and payment platforms make it easier for SMEs to reach global consumers. And instant payment schemes are critical, with over 80 countries now offering domestic real-time systems.[2] Many international instant payment corridors have also been established, with Singapore connected to India, Malaysia and Thailand, for instance.[3] In Europe, infrastructure provider EBA Clearing has launched 'OCT Inst' service for cross-border instant payments.[4]

To support their customers, banks, payment service providers (PSPs) and fintechs are ramping up their cross-border payment offerings, creating valuable new revenue streams. As well as connecting existing systems, the industry is exploring new technologies. Central bank digital currencies and distributed ledger technology-based payment systems could drive significant growth in the coming years while reducing transaction costs for both businesses and consumers.

Many of today's initiatives were set in train in response to the G20's 2020 roadmap to enhance cross-border payments, in recognition that "faster, cheaper, more transparent and more inclusive cross-border payment services, including remittances, while maintaining their safety and security, would have widespread benefits for citizens and economies worldwide, supporting economic growth, international trade, global development and financial inclusion".[5]

But while the rise in cross-border payments brings undeniable benefits to citizens, businesses and other organisations, it also comes with significant risks.

[1] https://www.bankofengland.co.uk/payment-and-settlement/cross-border-payments

[2] https://www.pymnts.com/tracker/real-time-payments-world-map-global-transactions/

[3] https://www.thebanker.com/Interlinked-systems-are-revolutionising-cross-border-fast-payments-1719830949

[4] https://www.ebaclearing.eu/news-and-events/media/press-releases/17-december-2024-pan-european-oct-inst-service-goes-live-in-rt1/

[5] https://www.fsb.org/2020/10/enhancing-cross-border-payments-stage-3-roadmap/

Why do cross-border payments increase risks?

Ever since there have been payments, there have been attempts of fraud. Cheque fraud, one of the most traditional forms of payment fraud, still results in staggering losses – $21 billion in the US in 2023. As payments have evolved, so too have scammers' tactics.

The rise of online banking and electronic communication over the past two decades has fuelled new opportunities for fraudsters, who are able to strike with greater sophistication and reach.

Cross-border payments exponentially increase the risk of fraud for several reasons. The fragmented regulatory landscape of cross-border payments complicates fraud prevention. Without a single governing body, each country enforces its own regulations and security policies for Know Your Customer (KYC), Anti-Money Laundering (AML), and fraud detection. Inconsistencies create gaps for criminals to exploit, complicating efforts to establish effective safeguards. The lack of standardisation also makes global coordination difficult, impeding investigations across jurisdictions and efforts to trace and recover funds.

Data sharing restrictions and inconsistencies in global data protection laws can slowdown cross-border investigations, and in turn create frictions in fraud prevention. Criminals can take advantage using virtual international bank account numbers (IBANs), cryptocurrencies, and other technologies to conceal their activities and move funds undetected.

Intermediaries in cross-border payments add another layer of complexity. Having multiple parties involved in processing transactions can complicate investigations and recovery efforts. Meanwhile, fraudsters continuously evolve their tactics, employing advanced tools, for example using AI, to carry out increasingly sophisticated scams across borders.

Finally, the rapid pace of modern payment systems exacerbates these challenges. Fraudsters can quickly move stolen funds across multiple accounts and jurisdictions, leveraging real-time payment systems that leave little time for banks to identify and block fraudulent transactions. Once funds leave the original jurisdiction, tracing them becomes significantly harder.

> The rapid pace of modern payment systems allows fraudsters to move stolen funds across multiple accounts and jurisdictions quickly, leaving little time to identify and block fraudulent transactions.

The operational impact of managing cross-currency payment risks

Managing fraud risks associated with international payments creates several challenges for treasury, finance and accounts payable teams at companies and other organisations, such as:

Operational inefficiencies

Increased processing times: Manual verification can delay transactions due to the need to check transactions and beneficiaries and ensure compliance.
Slower onboarding: Lengthy verification processes slow down new client onboarding, impacting business efficiency.
Higher costs: The additional time and resources required for manual verification increase operational costs, which are often passed on to consumers.

Risk and compliance issues

Human error: Manual repetitive processes are prone to mistakes, which can cause delays and lead to compliance issues.
Inconsistent KYC/AML application: Different institutions and regions follow varying KYC and AML procedures, leading to inconsistent results.
Compliance challenges: Navigating conflicting national regulatory requirements increases operational costs for firms operating in multiple jurisdictions.

Fraud and security concerns

Increased fraud risk: Without real-time verification, it becomes harder to detect and prevent fraudulent transactions, exposing companies to financial losses.
Difficulty in tracking funds: In cross-border payments, where no direct relationship exists between sending and receiving banks, tracking and recalling funds is complex and time-consuming. Payments pass through multiple banks, each causing delays and increasing complexity.

Fragmented operations

Siloed teams: Within financial institutions (and some corporates), KYC, AML, and fraud prevention teams often operate separately, making it difficult to coordinate efforts and disrupt cross-border fraud effectively.

2 Understanding APP fraud

Authorised push payment (APP) fraud is a type of scam where a fraudster deceives a victim into authorising a payment under false pretences. Different countries use a variety of names for this type of fraud, including relationship and trust scams and credit push fraud. To further complicate the understanding of what constitutes APP fraud, it also includes a variety of other scams (see next section for real-world examples).

Regardless of the terminology used, however, this type of fraud targets human psychology, exploiting trust, fear, urgency, or curiosity. It takes advantage of individuals – whether consumers or key finance personnel within a business – by using social engineering techniques to deceive or confuse victims into making payment transfers.

Key characteristics include:

1 **Deception, manipulation and exploitation:** APP scams rely on tricking or confusing victims into making payments that they would not otherwise make. Scammers often use personalised persuasion tactics to gain confidence and manipulate their victims. This can involve impersonating trusted parties such as banks, government agencies, or even family members and friends.

2 **Authorisation of payment:** In APP fraud, the payment is authorised by the victim, which distinguishes it from other types of fraud where the payment is unauthorised (such as phishing, which tricks the victim into revealing sensitive information, such as login credentials, passwords, or financial details, which the fraudster then uses to access accounts or steal money). By exploiting human vulnerabilities, APP fraud is difficult to prevent with traditional security measures. Authorisation also makes it more difficult to reverse the transaction or recover funds.

3 **Use of technology:** APP fraud is facilitated by our online lifestyles – in fact, over three-quarters of UK APP fraud cases originate online.[6] Currently, one of the most common types of APP fraud impacting organisations is BEC, while social media is often used for social engineering attacks on consumers. But fraudsters are constantly innovating and are increasingly using sophisticated technology, including AI, to conduct APP fraud. This includes the use of deepfakes, spoofing, and digital injection attacks.

4 **Cross-border nature:** The speed and anonymity of cross-border payments make them attractive to criminals. They take advantage of the difficulties in tracing illicit funds and the complexities of international payment systems. As a result, APP fraud is a global crisis, affecting consumers and businesses worldwide and resulting in billions lost.

5 **Limited reimbursement:** Once payments are authorised, it is often difficult to retrieve the funds, particularly when they are transferred to accounts in other countries or into cryptocurrencies. Governments in some markets (see section on government action) are putting protection in place for consumers.

6 **Impact on businesses:** Businesses are often targeted by APP fraud given the potential for greater rewards. Unlike consumers, organisations are generally not eligible for reimbursement when they fall victim to APP fraud. In addition to financial losses, a major breach may also result in significant reputational damage.

[6] https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf

How widespread is APP fraud?

The different terminology used to describe APP fraud in various countries makes it difficult to accurately assess its scale. However, LSEG Risk Intelligence's analysis of data from the World Bank and leading global consultancies estimates that global losses from APP scams could reach $331 billion by 2027.[7]

In the UK, the value of APP scams was £460 million (around $576 million) in 2023.[8] APP fraud represented about 40% of UK payment fraud, which itself accounted for 40% of all reported crime in the country in 2023, for instance.[9] In Australia, which has a population of slightly over a third of that of the UK, scams resulted in losses of A$330 million (roughly $207 million) in the year to 30 June 2024.[10]

In the US, the FBI's Internet Crime Complaint Center received 880,418 complaints in 2023, with potential losses of $12.5 billion. Investment fraud was the costliest crime, with losses increasing by $4.57 billion – up 38% rise on the previous year. BEC ranked as the second most expensive crime, accounting for 21,489 complaints and $2.9 billion in reported losses.[11] Payment fraud more generally is rampant: in 2024, 62% of US companies surveyed by LSEG Risk Intelligence reported experiencing payment fraud attempts.[12]

In the first half of 2023, fraudulent credit transfers originating from PSPs in the European Union and European Economic Area and sent worldwide totalled €1.13 billion ($1.18 billion), with 57% attributable to scammers manipulating payers into initiating transfers.[13]

The growing role of AI in APP fraud

AI will significantly increase the scale and sophistication of impersonation attacks. Some experts predict a doubling or more of AI-powered impersonation attacks compared to 2024.[14] AI provides malicious actors with potent new tools to conduct more targeted and convincing attacks. Potential AI-powered developments include:

Increased use of deepfakes:
The ability of AI to create convincing deepfakes will lead to a rise in impersonation attacks that use mimicked voices, faces, and writing styles. These deepfakes – imitating loved ones pleading for financial help or impersonating service providers – will be harder to detect. This not only makes AI a powerful tool for fraudsters but could lead to an erosion of public trust in transactions.

AI-driven fraud will reshape authentication:
While use of AI increases the sophistication of attempted fraud, it also has the potential to enhance authentication methods, leveraging digital IDs and digital ID wallets. Financial institutions that fail to address the risks posed by AI (and do not adopt AI-driven fraud prevention tools as they emerge) could be more vulnerable to scams and may suffer reputational damage as a result.

[7] https://www.lseg.com/content/dam/risk-intelligence/en_us/documents/brochures/lseg-trusted-payments-global-account-verification-brochure.pdf

[8] https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf

[9] https://www.ukfinance.org.uk/system/files/2024-06/UK%20Finance%20Annual%20Fraud%20report%202024.pdf

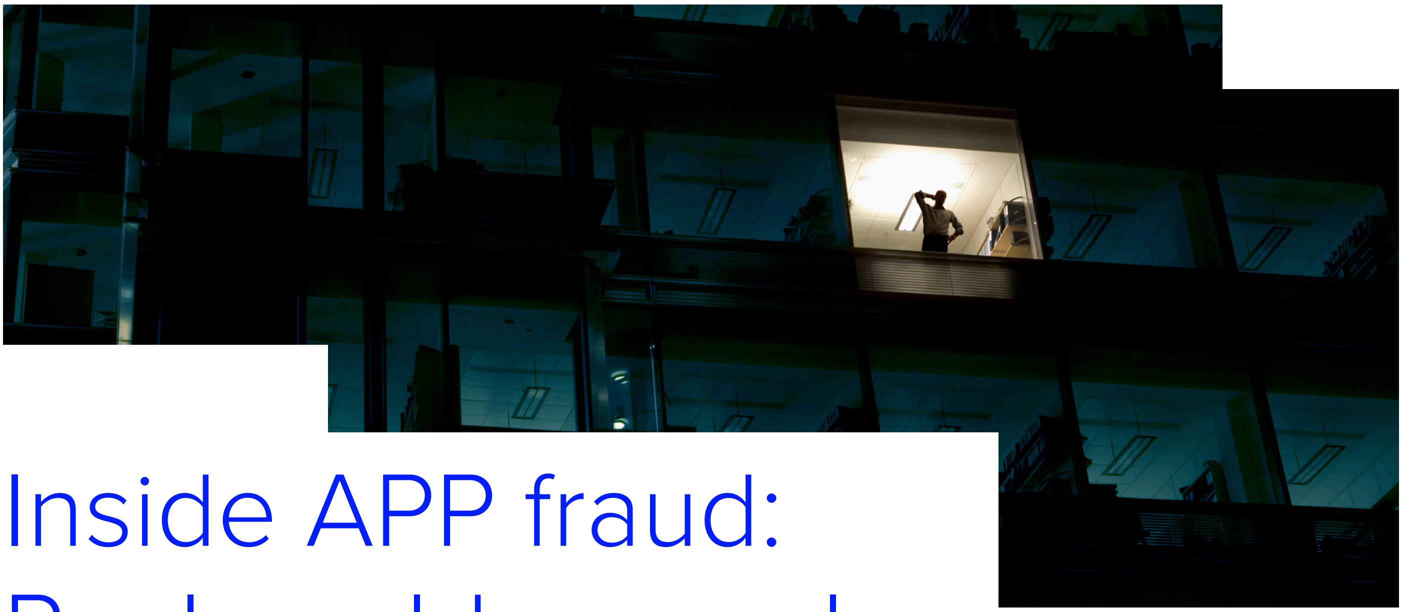
[10] https://www.nasc.gov.au/system/files/NASC-quarterly-update-Q4-2024.pdf

[11] https://www.ic3.gov/AnnualReport/Reports/2023_IC3Report.pdf

[12] https://www.lseg.com/content/dam/risk-intelligence/en_us/documents/gated/white-papers/b2b-payment-fraud-report.pdf

[13] https://www.eba.europa.eu/sites/default/files/2024-08/465e3044-4773-4e9d-8ca8-b1cd031295fc/EBA_ECB%202024%20Report%20on%20Payment%20Fraud.pdf

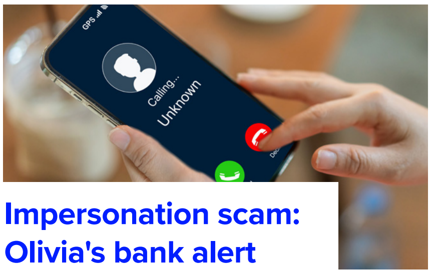
[14] https://www.miteksystems.com/blog/2025-fraud-predictions-industry-innovators



3 Inside APP fraud: Real-world examples

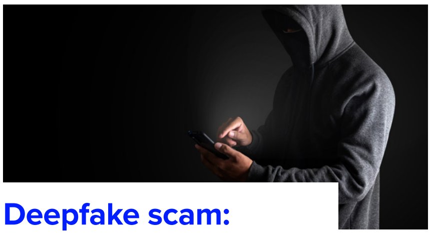
When considering the scale of APP fraud and its global dimensions, it is easy to lose sight of the fact that each scam involves an individual (even when the target is an organisation). The nature of APP fraud – in particular the deception involved (often entailing the impersonation of a trusted friend, family member, or colleague) – means the consequences go well beyond financial losses. Victims often suffer emotional distress and anxiety, particularly about the security of their personal information. Some scams, especially those relating to medical matters or romantic liaisons, can also cause shame and embarrassment.

Various types of APP fraud are profiled below, illustrating the potential impacts on victims:



Impersonation scam: Olivia's bank alert

Olivia received a call from someone claiming to be from her bank's fraud department. The caller warned of suspicious transactions on her account and asked her to verify her details. Trusting the professional tone and familiarity with her recent transactions, Olivia provided the requested information. When directed, she transferred funds to what the caller said was a secure holding account. Her funds were never recovered.



Deepfake scam: David's startling call

David was shocked when he received a video call from his CEO, Laura, instructing him to transfer $100,000 immediately to a new vendor. The call was brief, but Laura's voice and face were unmistakable. Wanting to act promptly, David complied. Later, he mentioned the transfer in an email to Laura, only to discover she had not made the call. A deepfake video had been used to manipulate David into transferring the funds.

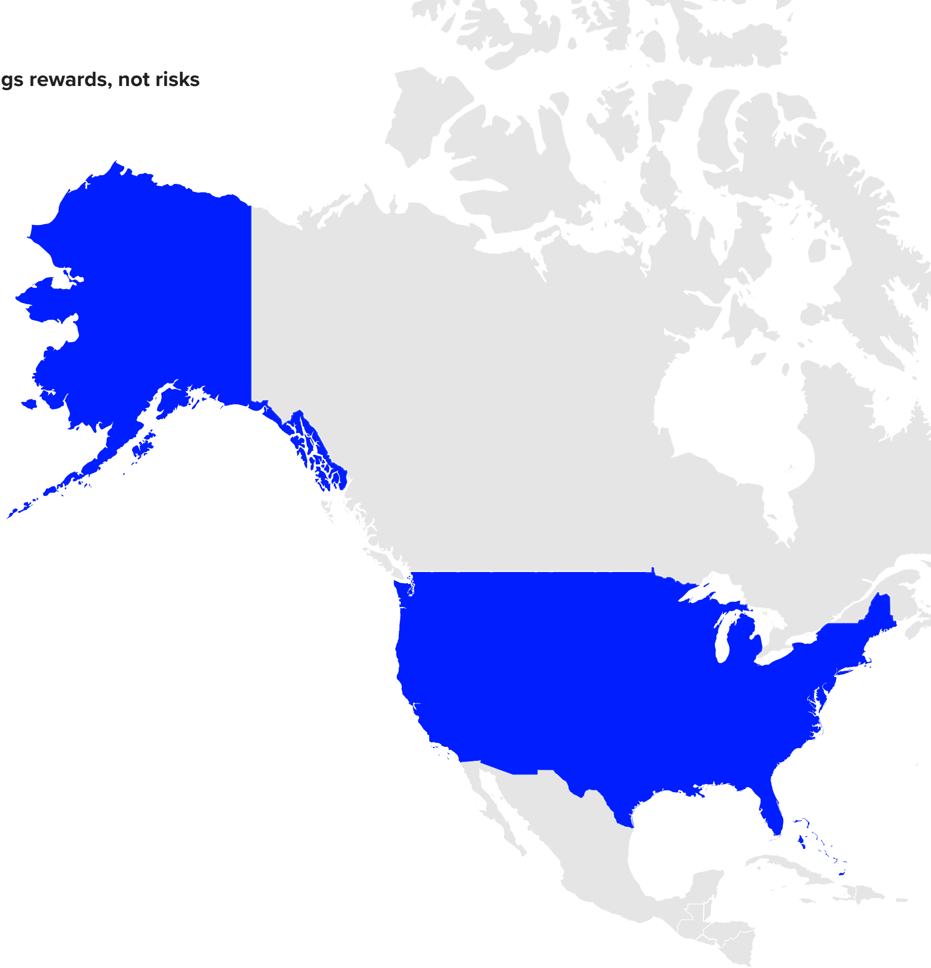
Invoice scam: Emma's business dilemma

Emma, a small business owner, received an email from what appeared to be her regular supplier. The email requested payment for an overdue invoice and included accurate details, including Emma's past transactions. She wired $12,000 to the account listed, only to find out later the supplier had not sent the email. A fraudster had intercepted the supplier's email (a BEC phishing attack) and changed the payment details to their own account.

4 Institutional efforts to combat APP fraud

Governments, regulators and industry bodies worldwide have begun implementing various measures to combat rising rates of APP fraud. These measures vary by country but generally include a mix of regulations, reimbursement schemes, technological solutions, and collaborative efforts.

Looking at actions being taken around the world:



United States

In April 2024, a new rule came into effect, enabling the Federal Trade Commission (FTC) to file federal court cases against scammers who impersonate government agencies and businesses, in order to apply civil penalties and return money to injured consumers.[15]

The FTC is also working to improve its regulatory force in relation to impersonation fraud and is collaborating with law enforcement to prosecute illegal telemarketing and investment schemes.[16]

The Federal Communications Commission (FCC) initiated multiple actions in 2024 to reduce the 4 billion robocalls Americans receive each month.[17]

The US Federal Reserve released a tool called the Scam Classifier in June 2024 to classify, understand, and mitigate various forms of fraud.[18]

Nacha, which oversees the ACH network, has introduced new rules to combat credit push fraud. These are being introduced in a series of phases from April 2025 to June 2026.[19] They require all ACH network participants, except consumers, to conduct fraud monitoring on ACH payments, including ACH credits. They also recognise the role of receiving depository financial institutions (RDFIs) for the first time, establishing specific monitoring requirements for RDFIs on inbound ACH credits.[20]

[15] https://www.ftc.gov/news-events/news/press-releases/2024/04/ftc-announces-impersonation-rule-goes-effect-today

[16] https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

[17] https://www.fcc.gov/spoofed-robocalls

[18] https://fedpaymentsimprovement.org/strategic-initiatives/payments-security/scams/scamclassifier-model/

[19] https://www.nacha.org/content/summary-upcoming-rule-changes

[20] https://www.nacha.org/newrules

United Kingdom

The UK's Payment Systems Regulator (PSR) has mandated a 50/50 reimbursement model for consumers who are victims of APP fraud, effective from October 7, 2024. This means that the banks sending funds and the banks receiving funds will each cover 50% of the loss, up to a maximum of £85,000.[21]

This reimbursement scheme applies specifically to consumers and not businesses (with some exceptions for microbusinesses and smaller charities).

The UK introduced Confirmation of Payee (CoP) technology to alert bank users when the payee's name and account details don't match in June 2020, beginning with the six largest banks and expanded to all PSPs handling Faster Payments and CHAPS in October 2024.[22] The PSR is also improving data sharing between financial institutions to reduce the impact of scams.

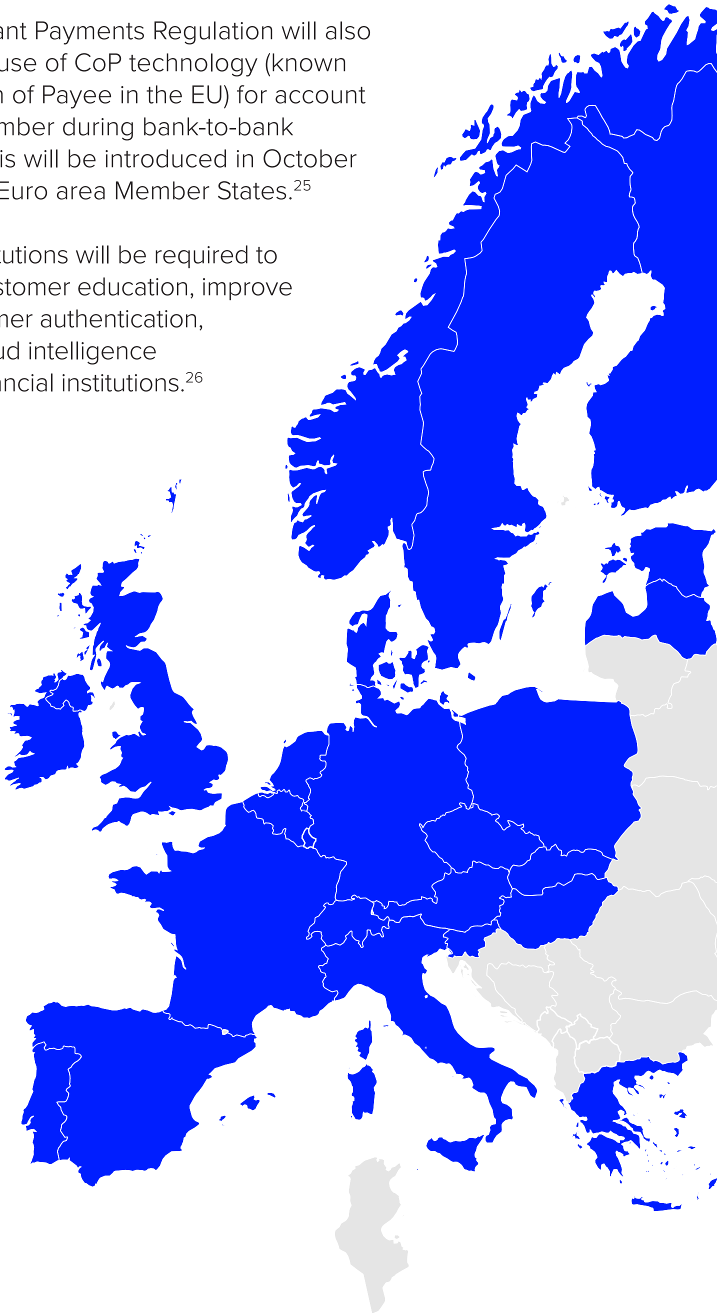
The Economic Crime and Corporate Transparency Act 2023 and the Payment Services (Amendment) Regulations 2024 redefine compliance standards. The new 'Failure to Prevent Fraud' offense requires organisations to demonstrate effective anti-fraud measures for customers, employees, and partners.

European Union

The Payment Services Directive 3 (PSD3) and Payment Services Regulation (PSR) are currently being debated by EU legislators and expected to come into effect in 2026 if adopted.[23] These regulations if implemented would outline liability for fraud between organisations involved in processing the transactions. EU legislators intend to bring in scope more providers involved in the fraud chain (including PSPs, Electronic Communications Service Providers or certain online platforms).[24] As a result, such providers would need have in place fraud prevention and mitigation techniques to combat fraud in all its forms, including unauthorised and authorised push payment fraud.

The new Instant Payments Regulation will also mandate the use of CoP technology (known as Verification of Payee in the EU) for account name and number during bank-to-bank payments. This will be introduced in October 2025 for the Euro area Member States.[25]

Financial institutions will be required to undertake customer education, improve secure customer authentication, and share fraud intelligence with other financial institutions.[26]



[21] https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/

[22] https://trustpair.com/blog/confirmation-of-payee-regulation/

[23] https://www.theglobaltreasurer.com/2024/02/26/psd3-a-significant-leap-forward-in-open-bankin/

[24] https://www.hoganlovells.com/en/publications/psd3-european-parliament-adopts-amended-psd3-and-psr-texts-at-first-reading

[25] https://www.europeanpaymentscouncil.eu/what-we-do/other-schemes/verification-payee

[26] https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3543

Australia

Australia is introducing CoP technology this year in a series of phases. SWIFT is managing the central matching service which underpins the CoP service.[27]

New rules for financial account openings, such as mandatory biometrics, are being implemented.[28]

The government established the National Anti-Scam Centre in July 2023 to bring together stakeholders from various sectors.[29] This includes government, law enforcement, banks, and telecoms companies to collaborate and develop coordinated strategies to combat scams.

The Australian Financial Crimes Exchange (AFCX) intelligence loop, which includes government, banks, telecom companies, and digital platforms, enables near real-time data sharing about tactics and tools used by scammers.[30]

The Australian government is developing a scam prevention framework with clear codes and standards for different sectors, which could include increased regulation of telecoms and social media companies to prompt them to crack down on scams.[31] Organisations will be held accountable for not meeting codes; the government will consider consumer reimbursement where sectors fail to meet the standards.[32]

Singapore

Singapore passed the Online Criminal Harms Act (2023), which sets requirements for online platforms to better protect their consumers. It also allows authorities to order swift blocking of fraudulent accounts or content.

Other global actions

Many countries are implementing measures to increase collaboration between law enforcement agencies, financial institutions and technology providers.

Governments are also focusing on public awareness campaigns to educate citizens about APP fraud risks and prevention strategies.

There is a growing focus on the development of standardised data sharing protocols to support cross-border investigations.

[27] https://www.threatmark.com/behavioral-biometrics-key-australian-banking-compliance/

[28] https://www.threatmark.com/behavioral-biometrics-key-australian-banking-compliance/

[29] https://www.accc.gov.au/system/files/NASC-Quarterly-update-Q3-2024.pdf

[30] https://www.govtechreview.com.au/content/gov-security/news/government-expands-fight-against-scammers-99566149

[31] https://www.theguardian.com/australia-news/2025/jan/05/australia-scams-crackdown-compliance-cost-digital-platforms-banks

[32] https://treasury.gov.au/consultation/c2024-573813

5 How companies, PSPs and other organisations can fight APP fraud

To prevent APP fraud, banks, corporations, PSPs, fintechs and other organisations can implement a variety of strategies. These can be broadly categorised into technological solutions, enhanced security measures, collaboration, and regulatory compliance.

Technological solutions

Implement real-time verification of bank accounts to check that payee and account details match before transfers are confirmed. This helps ensure that payments reach the correct recipients by providing a ‘match’, ‘close match’, or ‘no match’ result, enabling better informed decision-making and payment confidence.

Utilise biometric verification, such as fingerprint scans, facial recognition, and voice authentication, for identity verification. This can help confirm identities, prevent fraud, and meet regulatory demands.

Adopt multi-layered authentication strategies to enhance security and combat the sophisticated methods used by fraudsters.

Employ AI and machine learning for real-time monitoring, faster fraud detection, and enhanced security measures. These technologies can analyse vast amounts of data to identify suspicious activities, enhancing the ability to detect and flag fraudulent transactions.

Explore tokenisation to replace sensitive data with unique identifiers, thereby reducing data exposure, lowering interception risks, and improving authentication. Tokenisation also potentially facilitates global consistency by working across different payment systems.

Use application programming interface (APIs) for data sharing to connect institutions’ different systems.

Move to pull payments for high-value transactions, where the recipient is authenticated before funds are released.

Enhanced security measures

Integrate identity verification processes to safeguard sensitive data.

Implement enhanced fraud data sharing between sending and receiving firms to significantly improve fraud detection.

Regularly update security protocols, introducing more sophisticated identity verification technologies as they become available. Static security protocols are no longer sufficient due to the evolving threat landscape.

Address insider threats to prevent internal collusion and work with law enforcement when associate involvement is detected.

Focus on behaviour patterns to identify good customers and keep bad actors out of systems, rather than simply profiling fraudsters.

Validate phone numbers, email addresses, and devices to detect anomalies associated with fraudulent activities.

Implement robust KYC/know your business (KYB) verifications, along with behavioural analysis, to ensure trust throughout customer and supplier lifecycles.

Collaboration

Contribute to Increased data sharing among financial institutions, law enforcement, regulators, and technology providers to quickly share data, intelligence, and best practices.

Collaborate with social media companies to address scams originating on their platforms.

Work towards industry-level standards for communication between institutions to improve the speed and efficiency of cross-border fraud prevention efforts.

Promote global cooperation to combat fraud, emphasising that scams are an international issue requiring global solutions.

Regulatory compliance and other measures

Shift to proactive compliance rather than taking a reactive approach, embedding it within AML functions and overall strategy.

Stay up to date with regulations as they are introduced, such as the imminent PSD3 and PSR in the EU.

Prioritise fraud prevention before it occurs by establishing measures to detect, deter, and prevent fraud.

Provide training and awareness to educate employees about fraud threats and preventative measures.

Conduct regular risk and systems reviews to determine areas of risk, and implement preventative, detective, and coercive controls.

Develop a comprehensive ecosystem approach that involves all stakeholders in the digital economy (as in the Australian model), to emphasise prevention, early intervention, data sharing, and shared responsibility.

Prioritise consumer awareness with coordinated, multi-channel campaigns to educate the public about cybercrimes and build resilience.

Support efforts to report fraud more consistently to shift the focus from complete prevention to proactive accountability.

Why continuous fraud prevention is essential

A 24/7, holistic approach to APP fraud is crucial due to the nature of modern payment systems and the tactics employed by fraudsters:

Real-time, 24/7 payment systems: Criminals exploit always-on payment systems to move funds quickly, often across multiple accounts and jurisdictions, making it difficult to react and recover funds. The speed of these transactions means that any delay in fraud detection can lead to irreversible losses.

Criminal adaptability: Fraudsters constantly evolve their tactics and methods, exploiting new technologies and opportunities. They are skilled in using social engineering techniques to deceive victims, and they adapt quickly to new security measures. An always-on approach ensures that fraud prevention systems can react to these evolving threats in real-time.

Global operations: Criminal networks often operate across borders, making it essential to have continuous monitoring and detection capabilities. With cross-border payments, the complexity of the international payment system and the involvement of multiple intermediaries makes it difficult to trace illicit funds and requires swift action.

Evolving regulations: An always on approach allows for easier adaptation to new regulations as they are introduced, better data sharing and collaboration across financial institutions and improved detection of internal collusion in fraud schemes.

An always-on approach allows for proactive security measures rather than reactive ones. This can include real-time monitoring, AI-driven analysis, and continuous updates to fraud detection models.

Above all, a continuous approach helps maintain trust in the digital economy by ensuring secure and reliable payment processes. When customers are confident in the security of transactions, they are more likely to engage with digital payment systems.

6 LSEG's solution to support global expansion

Companies, banks, and PSPs seeking to grow their international business, supplier network or global payment support need a solution that can enhance security, streamline processes, and reduce the risk of cross-border credit push fraud.

LSEG Risk Intelligence has developed Global Account Verification (GAV) to help organisations expand their reach and improve their service offerings in a variety of ways:

Expanded reach: GAV enables transactions with clients worldwide, facilitating access to a broader international market. Country coverage is continually growing (for the latest coverage, please refer to the brochure located here). GAV helps organisations comply with local regulations. For instance, it aligns with PSD2's requirement of mandatory verification checks of account name and number during bank-to-bank payments.

Streamlined processes: GAV simplifies and accelerates the onboarding process for international clients, reducing friction and improving user experience. It speeds up payment processes and reduces manual errors and, as an API, enables seamless integration of account data into organisations' systems, enhancing operational efficiency. Higher straight-through processing rates are achievable, cutting overheads and costs associated with message repairs, to improve operational efficiency for treasury, finance and accounts payable teams.

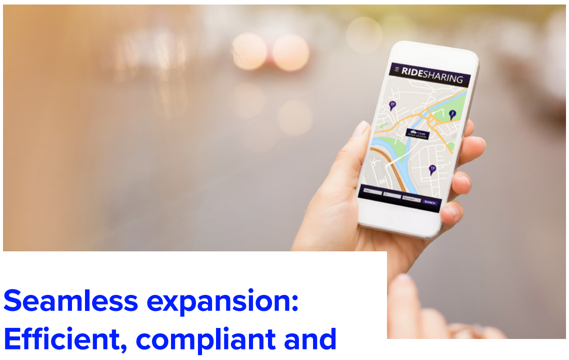
Increased security: By providing real-time verification of bank accounts and ownership across multiple countries, GAV enhances security and the ability to comply with international verification standards. This helps to minimise the risks associated with cross-border transactions, such as APP fraud, protecting businesses from financial losses and reputational damage.

Competitive advantage: GAV positions clients as leaders in their respective markets by offering cutting-edge financial verification services, helping to build trust with international clients through transparent and reliable verification processes. By ensuring payments reach the correct recipients, the solution enables customers to pay with confidence and trust.

Data-driven insights: GAV is supported by a team of experts who provide valuable insights and recommendations to help businesses optimise their fraud prevention strategy.

In the US, LSEG Risk Intelligence also offers domestic bank account verification solutions including bank account validation, ownership authentication, bank account insights and additional fraud and risk signals, covering US consumer and business accounts. Collectively, these solutions enable users to mitigate payments and identify risks across onboarding of vendors and customers, payments transactions and change management events.

GAV use cases: Enabling more secure cross-border payments

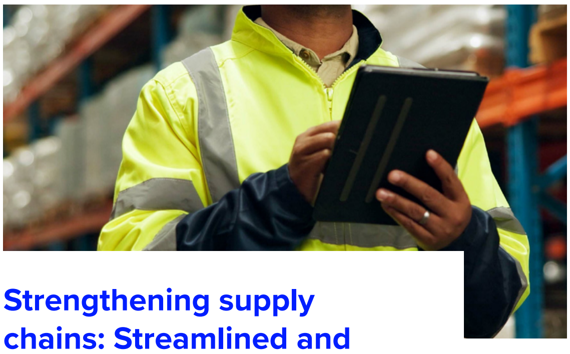


Seamless expansion: Efficient, compliant and driver-friendly payments

A leading ride-hailing company is preparing to expand into multiple G20 countries. However, each internal team has distinct priorities that must be addressed for a successful launch.

The fraud team needs to ensure that payments reach the correct drivers and that bank details – such as IBANs and account ownership – are verified in compliance with local regulations. The onboarding team wants a seamless registration process to prevent unnecessary friction that might deter new drivers from signing up. The treasury team seeks to enhance operational efficiency by integrating an automated account and payment verification process into existing financial systems.

GAV provides a comprehensive solution that meets the needs of all stakeholders. Its extensive global network, connected to national payment verification systems, allows for a single, scalable implementation across all markets. Moreover, its rapid verification process ensures that drivers receive payments faster, boosting satisfaction and long-term loyalty.



Strengthening supply chains: Streamlined and risk-free supplier payments

A global pharmaceutical company is restructuring its supply chain to adapt to shifting geopolitical conditions and tariff policies, reducing reliance on China. India's well-established pharmaceutical manufacturing sector offers a compelling alternative, while Brazil presents opportunities backed by strong government incentives to engage with local firms. However, suppliers in both markets prefer to be paid via instant payments, introducing new challenges for financial oversight.

The company's corporate treasury and finance teams are committed to ensuring payment security and maintaining the company's reputation. Given the irreversible nature of instant payments, they need to eliminate errors and mitigate risks associated with impersonation and invoice fraud – threats that are increasingly prevalent due to BEC.

GAV provides a robust solution by streamlining supplier onboarding in India and Brazil while delivering real-time verification of company names and bank details for every invoice. Suspicious transactions are flagged for further review, preventing fraudulent or misdirected payments before they occur. This safeguards the company's financial integrity while ensuring seamless, secure supplier relationships in key growth markets.

Conclusion

Securing global growth with the right solutions

The prevalence of APP fraud continues to increase, driven by the growing volume of cross-border transactions and changing nature of today's business environment. At the same time, the expanding use of AI in fraud scams, including deepfakes and sophisticated impersonation techniques, make it harder than ever to distinguish legitimate transactions from fraudulent ones. Risks are expected to escalate despite efforts by governments and regulators around the world.

For companies expanding globally – whether as part of international supply chains or entering new retail markets – as well as PSPs and other organisations, managing credit push fraud presents significant operational challenges. Verifying transactions across multiple jurisdictions, navigating fragmented regulatory frameworks, and addressing compliance inconsistencies adds complexity, increasing costs and processing times. The increasingly 24/7 business environment and the growing prevalence of instant payments further compound the challenge.

To ensure that global expansion delivers rewards rather than risks, solutions such as GAV are essential. By providing real-time account verification, GAV enhances security, reduces fraud exposure, and streamlines payment processes. As scammers' fraud tactics evolve, leveraging technology to strengthen payment verification and fraud prevention will be critical in protecting businesses and consumers alike.

About LSEG Account Verification Solutions

Verify bank accounts and their owners quickly and seamlessly – and transact with confidence.

Our US Account Verification product suite includes real-time bank account validation, ownership authentication, bank account insights, and additional fraud and risk signals – all available via a single API. We offer extensive global coverage of US consumer and business bank accounts

Nacha® Preferred Partner

In the US, we are a proud Preferred Partner of Nacha, the ACH governing body, in the categories of account validation, compliance, and risk and fraud prevention. Learn how we help advance the ACH network.

Our Global Account Verification solution provides real-time validation of global bank accounts and their owners, enabling you to make and facilitate cross-border payments with speed and confidence. Offering extensive coverage, it helps reduce the risk of bank-to-bank payment fraud and increase security, while supporting compliance and lowering costs.

About LSEG Risk Intelligence

LSEG Risk Intelligence provides a suite of solutions to help organisations efficiently navigate risks, avoid reputational damage, reduce fraud and ensure legal and regulatory compliance around the globe. From screening solutions through World-Check, to detailed background checks on any entity or individual through due diligence reports, and innovative identity verification and account verification – you can trust us to help you successfully manage your risk, so you can operate more efficiently, more effectively and more confidently. Learn more.