APP Fraud

Vixio PaymentsCompliance Outlook

VIXIO

Analyse. Anticipate. Accelerate.

About This Report

This report is part of Vixio PaymentsCompliance's Outlook series, which provides subscribers with forward-looking insights and consolidated research on key segments of the global payments industry.

This edition is designed to provide high-level intelligence on APP fraud in 2025.

Contents

Authors

Writing/Editing:

Adam Parkinson | Editor

Jimmie Franklin | Senior Journalist

Louise Coleman | Chief of Staff

Design:

Victoria Haughton | Content Operations Analyst

Introduction

The growth in use of digital payments has been demonstrable post-COVID, as is evident from global bodies such as the World Bank.

Increased digital skills and more seamless checkout processes through solutions such as Apple and Google Pay have spurred this increase in volume, offering unparalleled convenience, allowing transactions to be completed 24/7 from virtually anywhere, and removing the need for physical visits to banks or stores.

Online payment systems have also enabled global transactions, supporting cross-border business expansion and increasing choice for consumers.

This is especially the case in large trade areas such as the EU, where you can seamlessly order furniture from, say, Italy online and have it with you in Luxembourg within a few days.

Payments are processed instantly or within minutes, creating efficiencies for both merchants and consumers.

But, despite their benefits, online payments carry a heightened risk of fraud, with the remote nature of transactions making identity verification more challenging.

In particular, this is evident with the rise of authorised push payment (APP) fraud.

APP fraud differs from unauthorised fraud, when someone steals your card to make payments, for example, in that it involves voluntarily transferring funds to a fraudster.

Criminals have become master manipulators, tricking consumers into making impulse purchases or posing as genuine accounts on platforms such as Facebook, ready to sell second-hand goods or concert tickets.

Online payments provide the ideal opportunity for fraudsters to impersonate trusted entities — the pickpockets who previously tried to steal cards and cash no longer need a PIN, they just need to be able to charm consumers on platforms such as Facebook Marketplace with believable fake accounts.

The rise of social media and channels such as SMS has resulted in sophisticated phishing schemes and social engineering tactics being deployed by criminals to trick victims into transferring funds under false pretences, often leveraging urgency to prompt immediate action.

In addition, the increasingly rapid speed of instant, or real-time, payment systems such as the UK's Faster Payments makes halting fraudulent transactions difficult once initiated.

This has seen something that should be a booster for the UK economy become a double-edged sword, thanks to the new capabilities it has enabled for fraudsters.

In this outlook, Vixio is exploring how the world is reacting to APP fraud, with new legislation being implemented and market developments taking place in Europe and beyond.

We will be considering how it can be effectively prevented, if at all, and how payments firms should prepare for increased scrutiny and expectations.

Common Types Of APP Fraud

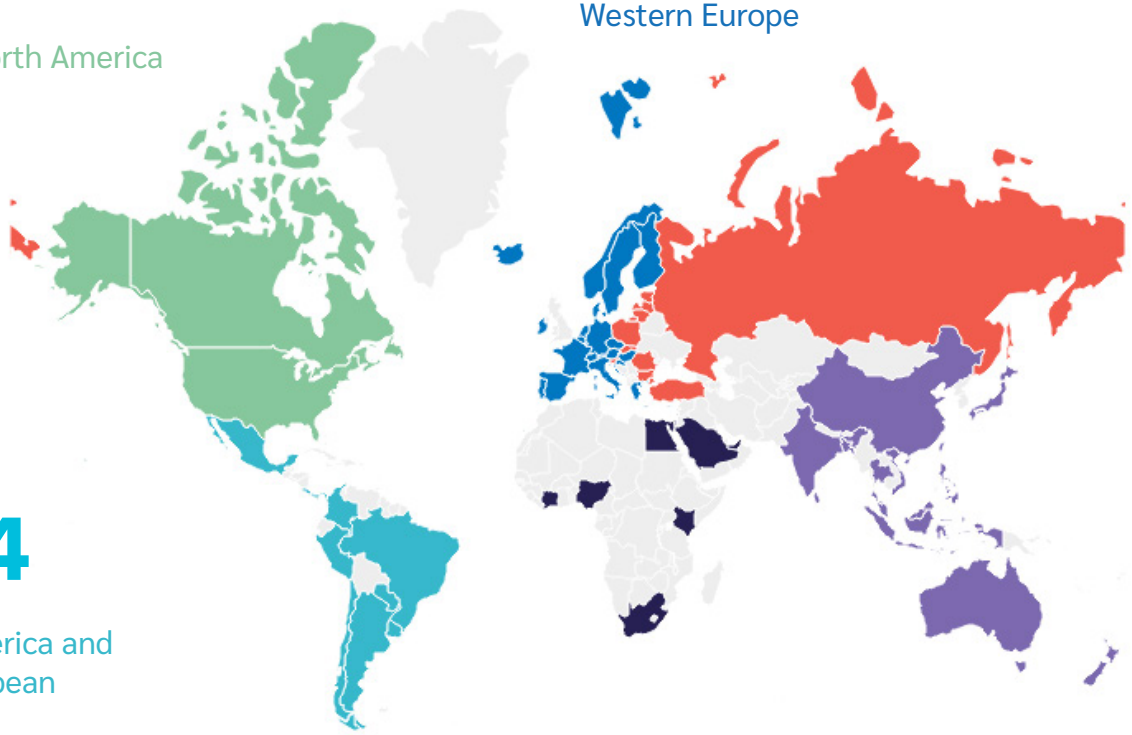
Type	Definition	Scenario
Purchase scam	Occur when a consumer pays for an item or service, but this is never received.	A scammer advertises fake concert tickets for a sold-out event online, demanding immediate payment via bank transfer. Once paid, they ghost the buyer, leaving them without tickets.
Romance scam	A criminal adopts a fake online persona to groom a victim into sending money. Also known as “pig butchering”.	A scammer builds a months-long online romance after matching through a dating app. The scammer convinces the victim to send them money, before disappearing, leaving them with devastating financial losses.
Impersonation scam	The criminal poses as a legitimate person or entity and tricks a consumer into transferring money.	A fraudster posing as Brad Pitt scams a fan out of a considerable sum of money after they ask for help paying medical bills. (This actually happened!)
Investment scam	A victim is tricked into making an investment into something that does not exist.	A scammer promotes a fake crypto investment platform called “Globe Coin”, which promises high returns. Early profits convince victims to invest more but when they try to withdraw the funds, their accounts are frozen, and the platform vanishes.
Invoice scam	A scammer dupes their victim into paying a bogus invoice using fake paperwork and social engineering.	A fraudster is able to hack a company email, sending fake invoices to clients requesting payment. Believing the request to be legitimate, clients transfer funds and the scam is discovered too late, with the payments untraceable.
CEO scam	A scammer impersonates the CEO or member of the senior management at an organisation and gets an employee to transfer funds.	A finance worker at a multinational firm is tricked into paying out $25m to fraudsters using deepfake technology to pose as the company's CEO. (Again, this actually happened).

Vixio Fraud Horizon Scanning Updates Per Jurisdiction, January 2024-January 2025

16
North America

103
Western Europe

17
Central and Eastern Europe



34
Latin America and the Caribbean

Asia Pacific
21

8
Middle East and Africa

Regional Roundup

UK

The UK has an advanced regulatory framework targeting APP fraud and liability, and it includes mechanisms for prevention and for liability protection, which favour consumers while also incentivising PSPs to prevent fraudulent activity.

For example, the UK's Confirmation of Payee (CoP) service checks account names against payment details to reduce fraud and misdirected payments.

Since its 2020 launch, more than 500 organisations have adopted CoP, safeguarding 99 percent of Faster Payments and CHAPS transactions.

Alongside this are the new Faster Payments reimbursement rules, which, though a step forward compared to the rules in place in jurisdictions such as the EU and US, have not best pleased PSPs, which consider them a significant financial liability.

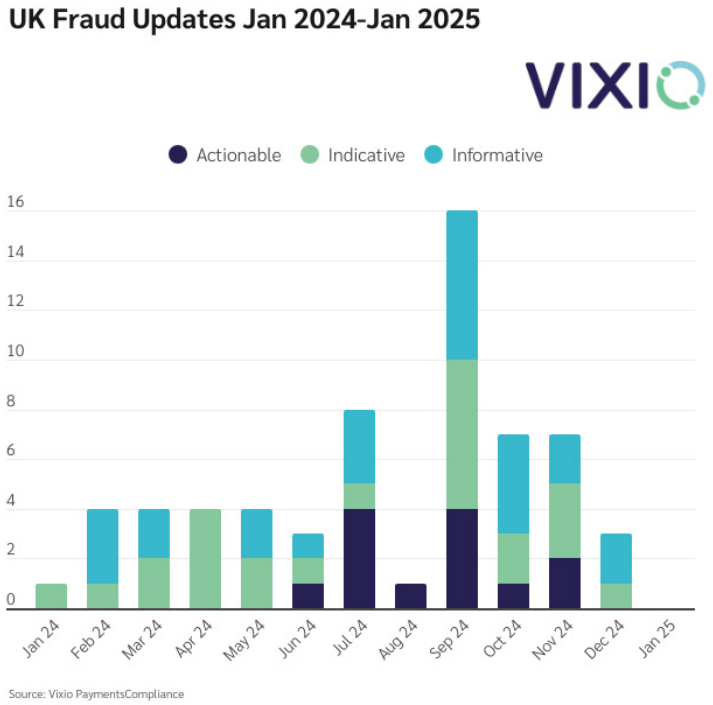
Trade associations including the Payments Association have previously sounded the alarm about issues such as commercial viability, and warned that firms may end up failing or leaving the UK.

Reimbursement rules

Since October 7, 2024, payment service providers (PSPs) in the UK have been required to reimburse victims of Faster Payments APP scams up to £85,000 per claim.

This cap was originally set at £415,000 before the PSR backed down after industry pressure, and covers 99.8 percent of scams by volume and 90 percent by value.

Protections apply to individuals, microenterprises and charities, encompassing a range of payment firms, including banks, building societies and e-money firms, but excluding credit unions and national savings banks.



Reimbursement is shared equally between sending and receiving PSPs, ensuring consumer protections are robust while promoting industry accountability.

Victims can expect reimbursement within five business days, with a maximum processing time of 35 days under specific conditions.

Firms are allowed to apply an optional excess of up to £100, exempting vulnerable consumers, and must demonstrate gross negligence by the consumer to deny claims.

The reimbursement cap aligns with the Financial Services Compensation Scheme limit, but firms can choose to exceed it, and unresolved cases can be escalated to the Financial Ombudsman Service.

The PSR's goal with this policy is to incentivise fraud prevention by the PSPs, requiring them to adopt measures such as behavioural biometrics and payment screening.

However, the rules may not last forever. Trade Associations have expressed concerns about the impact on growth, and the PSR has agreed to review the rules after a year.

It could be that the regulator decides to make changes, including a possible lower cap.

FCA Dear CEO letter

At the same time as the APP fraud reimbursement rules were introduced, the FCA issued a Dear CEO letter detailing expectations for PSPs and their fraud reimbursement approach.

The letter emphasised robust oversight, systems, and controls to make sure that PSPs are in full compliance.

PSPs are expected to enhance their anti-fraud systems, improve transaction monitoring, and review governance structures to prevent fraudulent activities, and the FCA also used the letter to highlight the importance of managing potential liabilities associated with APP fraud reimbursements to mitigate impacts on capital and liquidity.

In addition, the regulator reminded payments players that under the Consumer Duty, firms must avoid foreseeable harm and provide adequate support and redress for affected customers.

The FCA further urged PSPs to incorporate new legislation from HM Treasury that effectively slows suspicious transactions down (see below) into their fraud prevention strategies while ensuring legitimate transactions are processed swiftly.

Stop the clock

In October 2024, the UK government approved new rules allowing PSPs to delay suspicious payments by up to 72 hours, tripling the existing limit. This will begin to apply from March 2025.

This extension aims to reduce fraud by providing more time to investigate suspect transactions.

To effectively "stop the clock", PSPs are required to inform customers of delays, explain necessary actions to unblock payments, and compensate for any interest or late fees incurred.

Althuogh some commentators, such as UK Finance, have welcomed the announcement, payment firms fear the unintended consequences of the government-approved delays to payments, with some calling the requirement "anti-growth" and "half baked".

There is a concern that payment and e-money institutions might face challenges if banks block payments from accounts linked to such firms.

However, although fintechs worry that banks could use this as an excuse to delay payments, the mere fact that a payment is directed to a fintech account does not automatically justify suspicion.

For example, banks would need reasonable grounds to delay payments, and repeated actions could attract regulatory scrutiny.

European Union

Verification of Payee

The EU's Instant Payments Regulation (IPR) introduces similar measures to the Confirmation of Payee rules in the UK, although they are more stringent.

The IPR aims to make instant payments "the new normal" in the EU, and there has been concern that this will mean that a rise in APP fraud will quickly follow.

Some EU member states, such as the Netherlands and France, have already introduced systems like Verification of Payee (VoP), but the regulation will mean that the approach becomes more widespread and unified across the trading bloc.

Article 5 of the IPR stipulates that PSPs are required to verify the payee's details, including the name and account identifier, before the payer authorises a transaction. It states that this service must be offered for all payment methods without exception.

PSPs are responsible for matching the name of the payee with the account identifier provided by the payer. If the details do not exactly match, but are close enough to indicate a potential match, PSPs must notify the payer of the associated name.

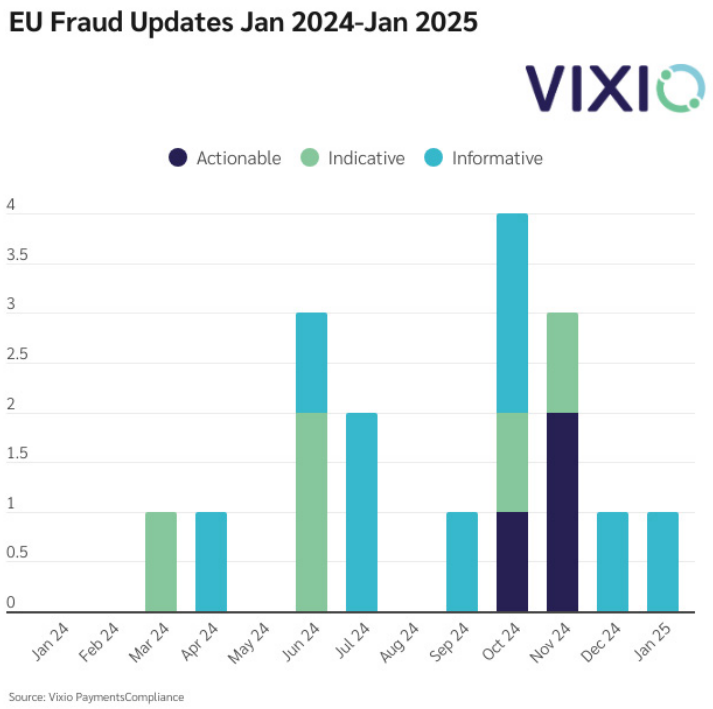
When there is no match, the payer must be informed that the transaction could result in funds being sent to an unintended recipient.

Liability for incorrect transfers is waived if the PSP performs the verification correctly. However, failure to meet the verification requirements obligates the PSP to refund the payer and refund the money.

Non-consumer users that submit bulk payment orders can opt out of the verification service, but PSPs must inform them of the associated risks, and these users retain the option to opt back into the service at any time.

To ensure smooth implementation, the regulation promotes the development of EU-wide standards, but the compliance timeline is still slightly staggered.

PSPs in eurozone countries must comply with the regulation by October 9, 2025, while those in non-eurozone countries have until July 9, 2027.



Possible rules in the proposed Payment Services Regulation

Liability for APP fraud features in the EU's proposed Payment Services Regulation (PSR).

In cases of impersonation fraud, the PSP would be required to refund the full amount if the consumer promptly reports the incident to the police and the PSP.

As in the UK, refunds can be denied if the PSP proves the consumer acted fraudulently or negligently, and PSPs and electronic communication providers must collaborate to prevent such fraud through enhanced security measures.

The PSR's passage is currently uncertain, but it is anticipated that negotiations will be final this year. The final text remains to be seen, but will depend on what the European Council and European Parliament can agree on.

For example, European Parliament suggestions about fraud liability being shared with social media firms could prove too controversial for the final text.

Detecting fraudulent activities

The EU's PSR requires PSPs to implement transaction monitoring systems to detect and prevent fraudulent activities.

These systems must be able to analyse transaction history and data from payment accounts, including transaction amounts, payee identifiers and session data, to identify potential fraud. PSPs would be prohibited from storing this data longer than necessary.

The systems in question must also account for factors such as stolen authentication elements, known fraud scenarios and malware infections.

Information sharing

PSPs are also encouraged to share the unique identifier of a payee with other providers in cases of suspected fraud, but only when there is sufficient evidence, such as multiple reports of fraudulent use of the same identifier.

Shared data must not be retained longer than necessary for fraud prevention, and the European Commission has warned that sharing arrangements among PSPs must be carefully managed, ensuring compliance with data protection regulations.

Participants must notify authorities of their involvement in such arrangements.

Customer warnings

There is also a consumer education angle to the EU's plans.

Banks and payment firms are required to alert customers about emerging fraud risks and provide guidance on how to recognise and avoid fraudulent activities.

They must also offer training programmes to their employees on payment fraud risks and ensure they are equipped to handle fraud prevention.

The European Commission has said that the European Banking Authority (EBA) will be mandated to issue guidelines on these training programmes within 18 months of the regulation's entry into force.

Asia-Pacific

Japan & South Korea

Japan and South Korea were early leaders in terms of their work on APP fraud.

Japan's Act on Damage Recovery Benefit Distributed from Funds in Bank Accounts Used for Crimes, which was enacted in 2008, introduced measures to recover and redistribute fraudulently obtained funds.

The legislation empowered banks to freeze suspicious accounts and built on earlier financial crime legislation, and a subsequent 2012 amendment further limited ATM-initiated transfers exceeding JPY100,000 ($646) to curb scams.

Similarly, South Korea's Special Act on the Prevention of Loss Caused by Telecommunications-based Financial Fraud and Refund for Loss, introduced in 2011, allowed for victims to recover funds without formal lawsuits.

The Financial Supervisory Service (FSS) also established a team for fraud prevention and public awareness, and a 2014 amendment strengthened financial institutions' responsibilities in preventing APP fraud.

Australia

Scams Prevention Framework

In September 2024, Australia's Treasury introduced the Treasury Laws Amendment Bill 2024: Scams Prevention Framework (SPF), which initially looks set to target banks, telecommunications providers and digital platform services, such as social media, messaging and paid advertising platforms.

The framework has been designed to expand to other sectors as scam tactics evolve, and is part of broader efforts to modernise Australia's laws for the digital age, addressing privacy, cybersecurity and payment system reforms.

Stakeholders were invited to provide feedback on the draft legislation until October 4, 2024.

The SPF aims to address the A$2.7bn (US$1.77bn) lost to scams in 2023 by establishing mandatory standards for scam prevention, detection, reporting, disruption and response.

The aim is to close regulatory gaps and create consistency across industries, so that consumers are protected from both financial and psychological harm.

The legislation introduces overarching SPF principles, enforced by the Australian Competition and Consumer Commission (ACCC), along with sector-specific codes tailored to industry needs.

It also creates a cross-collaborative framework for oversight and requires regulated entities to participate in a standard and externally managed dispute resolution scheme, which will be managed by the Australian Financial Complaints Authority (AFCA).

Non-compliance with the SPF carries penalties of up to A$50m (US$33m).

National Anti-Scam Centre

Australia also has a National Anti-Scam Centre (NACC), which was launched in 2023 and is managed by the ACCC.

The NACC aims to disrupt scams before they reach consumers. It brings together experts from government, law enforcement and the private sector to analyse trends, share data and enhance consumer awareness about identifying and avoiding scams.

Through its Advisory Board, working groups and ongoing collaboration with industry, consumer organisations and government, the NACC fosters information-sharing to support businesses in both mitigating scam risks and implementing scam disruption strategies.

Before the NACC's establishment, cross-sector engagement on scams was limited in Australia.

Singapore

Protection From Scams Act 2024

Singapore's Protection From Scams Act, which was passed in January 2024, empowers the police to combat scams by freezing victims' bank accounts without consent.

This landmark law enables "restriction orders", issued by designated officers, to temporarily block transactions and credit access from a victim's account to prevent potential transfers to scammers. Orders last up to 30 days and can be renewed five times if necessary.

The act mandates compliance from banks, and non-compliance is punishable by fines of up to S$3,000 (US$2,224).

It does, however, allow for limited exemptions, such as bill payments, and provides an appeal process through the Commissioner of Police, whose decisions are final, and banks and officers complying with orders are granted immunity from liability.

Shared Responsibility Framework

The Shared Responsibility Framework (SRF), which has been an actionable compliance requirement since December 16, 2024, establishes clear anti-phishing rules for Singapore's banks and telecommunications companies.

Spearheaded by the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA), it targets phishing scams.

Banks and telcos are accountable for financial losses when failing to fulfil their responsibilities under the framework.

Financial institutions are required to meet four key duties:

- Implementing a 12-hour "cooling-off period" for new device logins.
- Sending real-time notifications for high-risk activities and transactions.
- Offering 24/7 reporting with a "kill switch".
- Maintaining real-time fraud surveillance.

Telecommunications firms need to support anti-scam efforts through the SMS Sender ID Registry, which authenticates sender IDs and flags potential scams.

This rule does not directly apply to APP fraud, but in instances where a user has been deceived into sharing details via a phishing scam, it would mean that the telecommunications firm would need to pay out.

Online Criminal Harms Act

Singapore's Online Criminal Harms Act (OCHA) aims to combat scams and malicious online activities through obligations for e-commerce and online communication platforms. The act was enforced in two phases, and became fully effective in June 2024.

Measures set out include requiring platforms such as Facebook Marketplace and Carousell to verify the identities of "risky sellers" and offering payment protection mechanisms to ensure goods or services are delivered before payment is released. If these measures fail to reduce scam activity, broader ID verification will be mandated.

The OCHA also designates platforms including Telegram and Meta's Facebook and WhatsApp as high-risk online communication services.

Because of this, they are required to proactively detect and disrupt scams, implement strong login verification and provide fast channels for law enforcement reports.

The platforms must also submit annual compliance reports.

Anti-Scam Centre

The Singapore Police Force established the Anti-Scam Centre (ASC) in 2019 to combat scams and reduce victims' losses.

Leveraging technology and partnerships, the ASC focuses on issues such as international cooperation and information management.

It collaborates with financial institutions, telcos and online marketplaces to freeze accounts, recover stolen funds and disrupt scammers' operations.

From 2019 to 2022, the ASC froze 40,900 bank accounts and recovered more than S$310m.

Its tech-driven initiatives include ScamShield, an app blocking scam calls and messages, and Project COMBAT, which alerts potential scam victims in real time.

Consumer education has also been an integral part of the ASC's strategy, with campaigns such as "I can ACT against scams" emphasising vigilance, reporting and using protective measures.

Internationally, the ASC cooperates with foreign law enforcement to dismantle transnational scam syndicates.

Vixio Regulatory Influencers

Vixio's Regulatory Influencers deep dive into imperative regulatory changes across the globe. Discover what the world's regulatory leaders are up to and use Vixio's unique insights to understand market developments and accelerate your decision making.

Read these and more:

Industry Debate Continues Over UK APP Fraud Reimbursement Cap

FCA's Dear CEO Letters on APP Fraud Reimbursement — Payment and E-Money Institutions Vs Banks and Building Societies

India

Like its counterparts in other other jurisdictions, the Reserve Bank of India (RBI) has introduced a beneficiary account name look-up feature for payments over its Unified Payments Interface (UPI) app, as well as its Immediate Payment Service.

This is now being extended to Real Time Gross Settlement (RTGS) and National Electronic Fund Transfers (NEFT) transactions.

This new requirement mandates banks and other RTGS and NEFT participants to enable account name verification for clients using mobile and internet banking for fund transfers.

These name-check requirements must be implemented by participating banks by April 1, 2025.

UPI fraud

India has had plenty of success with instant payments, and UPI has been hugely successful in enabling more financial inclusion and spurring a more digitised economy.

However, as has happened with Faster Payments in the UK, India has found itself grappling with fraud problems on the UPI platform.

UPI is vulnerable to APP fraud due to its design and operational features, and its ease of use and speedy transfers make recovering fraudulent payments challenging.

As is the case elsewhere, fraudsters can deploy social engineering tactics, impersonating legitimate entities to trick users into authorising payments or sharing sensitive information such as UPI PINs. Fake apps and malicious QR codes can further deceive users.

India has, however, attempted to tackle the issue and has introduced several initiatives to combat fraud in the UPI ecosystem, focusing on prevention, detection and response.

The National Payments Corporation of India (NPCI), owner of UPI, has implemented stringent device binding measures, ensuring a secure link between a customer's mobile number and their device. Two-factor authentication further enhances transaction security. In addition, in-app notifications during the transaction have been introduced to allow customers to be more alert to risks.

To mitigate risks, daily debit limits and restrictions on high-risk use cases have been established, and NPCI provides banks with a free fraud monitoring solution powered by AI. This provides risk scoring and rule development capabilities to detect and prevent fraudulent activities.

NPCI also works closely with the Reserve Bank of India (RBI), the Ministry of Home Affairs (MHA) and law enforcement agencies.

The MHA has established the Indian Cyber Crime Coordination Centre (I4C) for coordinated responses to cybercrime and has launched the National Cybercrime Reporting Portal and the National Cybercrime Helpline (1930) for public reporting.

The RBI, meanwhile, has introduced the Central Payments Fraud Information Registry (CPFIR), a web-based platform for reporting payment-related fraud by regulated entities.

In addition, in 2017, it issued guidelines limiting customer liabilities in cases of unauthorised or fraudulent electronic transactions, providing greater protection to users.

United States

In the US, there are currently no federal or state laws mandating reimbursement for victims of APP fraud. As things stand, the Electronic Fund Transfer Act requires banks to reimburse consumers for unauthorised transactions.

However, because APP fraud involves transactions that are authorised by customers, albeit under deception, PSPs are under no legal obligation to provide compensation.

How long this situation will last seems uncertain at the moment, given the growing concerns over APP fraud in the US since the rise in payment options such as Zelle and Venmo.

In August 2024, for example, Senator Richard Blumenthal, a Democrat, introduced the "Protecting Consumers from Payment Scams Act" (S.4943) alongside co-sponsor Elizabeth Warren and, in the House of Representatives, Maxine Waters. The latter figures are both titans of financial services consumer protection rights in the US.

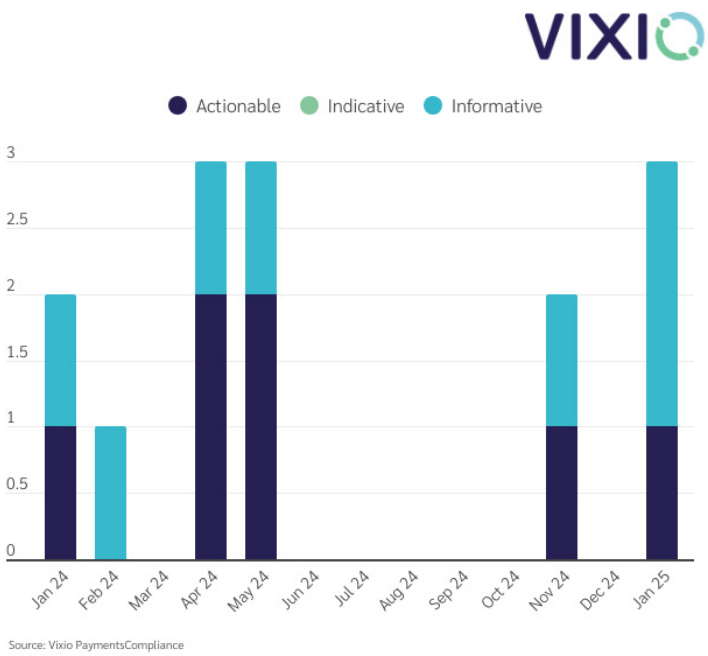
This bill aims to introduce consumer protections by requiring financial institutions to reimburse individuals who fall victim to APP fraud.

It seeks to amend existing laws to extend liability to cases where consumers are deceived into authorising payments to fraudsters. The bill clarifies that consumers are protected when they use bank wire transfers and electronic transfers authorised by telephone call.

It also ensures that error resolution duties apply if the consumer's account is frozen or closed, unless access has been denied due to a court order, law enforcement, or the consumer obtained the funds through unlawful or fraudulent means.

However, it seems unlikely that the bill will pass for now, due to the lack of a Democrat majority in the US Congress.

United States Fraud Updates Jan 2024-Jan 2025



Meanwhile, federal regulators do appear to be making the issue a priority to fix.

The Consumer Financial Protection Bureau (CFPB) has begun to address issues related to digital payment platforms, and in November 2024, announced a regulation requiring oversight of companies such as Apple Pay, Google Wallet, PayPal, Venmo, and CashApp to ensure compliance with federal privacy and fraud laws.

This regulation, which became an actionable compliance requirement in December 2024, aims to improve consumer protections, but has faced legal challenges from industry groups.

In January 2025, the CFPB imposed a $175m fine on Block, the parent company of Cash App, for inadequate fraud prevention measures, and this penalty includes up to $120m in consumer compensation and a $55m contribution to the CFPB's victim relief fund.

Yet, how long this work lasts is unknown. The Trump administration, the greater Republican Party, and allies like Elon Musk have made clear their thoughts on the CFPB - ranging from disinterest to outright disdain, with Musk saying the government should "delete" the regulator.

State-level protections

In January 2025, the CFPB imposed a $175m fine on Block, the parent company of Cash App, for inadequate fraud prevention measures, and this penalty includes up to $120m in consumer compensation and a $55m contribution to the CFPB's victim relief fund.

Yet, how long this work lasts is unknown. The Trump administration, the greater Republican Party, and allies like Elon Musk have made clear their thoughts on the CFPB - ranging from disinterest to outright disdain, with Musk saying the government should "delete" the regulator.

At state level, meanwhile, work has been ongoing for some time, with New Hampshire and Wyoming the first states to implement preventative measures.

Since 2022, PSPs operating in New Hampshire have been able to temporarily hold fund disbursements for up to 15 business days if exploitation of individuals aged 65 and over or vulnerable adults is suspected.

Since 2023, PSPs in Wyoming have been able to delay transactions for five to 30 business days if financial exploitation of vulnerable adults is suspected.

States such as Nevada, Maine and Minnesota have similar rules in place, and New York's governor recently committed to introducing similar legislation, with delayed transactions being between five and 45 business days.

In California, Democrat Governor Gavin Newsom recently vetoed a bill that would have placed more stringent requirements on banks to protect elderly customers against fraud and block suspicious transactions, making them liable if they failed to protect customers.

Unlike in Europe, the US approach to APP fraud, at least at state level, appears to focus on the elderly and most vulnerable. This may be due to cultural differences, such as an expectation of more personal responsibility in financial services, with the regulatory approach in jurisdictions such as the UK.

Market Developments

Swift

Swift launched an AI-powered fraud detection service in January 2025 to enhance cross-border payment security.

The system leverages pseudonymised data from transactions on Swift's network to detect and flag suspicious activity in real time.

It was developed in collaboration with more than 11,500 financial institutions globally, including BNP Paribas and Standard Bank.

Meta's FIRE

Meta's Fraud Intelligence Reciprocal Exchange (FIRE) is a programme that enables banks to share intelligence directly with Meta to combat scams on its platforms.

Launched as a pilot with NatWest and Metro Bank under the Stop Scams UK initiative, FIRE's key successes include dismantling a major concert ticket scam network targeting users in the UK and US.

This collaborative effort, which has been supported by UK-based authorities such as the City of London Police and the National Economic Crime Centre, aims to enhance fraud detection, while instilling a safer online environment.

With plans to onboard more banks, Meta seeks to expand this information-sharing framework globally.

FPAD

The Fraud Pattern and Anomaly Detection (FPAD) system was launched in March 2024 by EBA CLEARING, the pan-European payment infrastructure provider that operates financial services platforms.

It is intended to strengthen fraud prevention for PSPs operating in Europe, and provides a network-wide view of payment activity for SEPA Credit Transfers (SCT) and SEPA Instant Credit Transfers (SCT Inst).

This enables the identification of fraud patterns and anomalies that individual PSPs would not be able to detect on their own.

FPAD also supports compliance with regulatory requirements such as the Instant Payments Regulation, and includes a pan-EU VoP solution, meeting the October 2025 deadline in advance.

Market Developments

Revolut

European fintech success story Revolut has introduced an AI-powered scam detection feature to combat APP fraud and card scams.

This advanced machine learning tool identifies transactions likely to be scams and blocks them before completion.

Customers are guided through an in-app intervention process that includes providing transaction details, educational prompts and access to fraud specialists to counter scammers' influence.

Since launch, Revolut has reported a 30 percent reduction in fraud losses linked to investment scams.

Mastercard

Mastercard's Consumer Fraud Risk solution launched in the UK in 2023 and uses AI-powered insights and a network view of account-to-account (A2A) payments to predict and prevent scams in real time before funds leave victims' accounts.

Mastercard partnered with multiple UK banks, including TSB, Lloyds and NatWest, and the tool analyses factors such as account names, payment values and payer/payee history to identify and block suspicious transactions, particularly APP fraud.

The approach includes tracing funds through mule accounts to dismantle fraud networks and has already prevented $35bn in fraud globally over three years.

Cifas

Cifas is a UK-based, not-for-profit membership organisation dedicated to preventing fraud and financial crime through collaborative data sharing and intelligence.

Since its establishment in 1988, Cifas has worked with more than 750 organisations, including banks, telcos, insurers, public sector bodies and law enforcement.

The membership organisation provides tailored solutions that help businesses and individuals identify and mitigate risks proactively, and it leverages shared intelligence and expert threat analysis as well.

Cifas also promotes fraud awareness through partnerships with organisations such as the City of London Police and banking trade association UK Finance.

Thematic Analysis

Name-checks

Systems such as the UK's Confirmation of Payee (CoP) and what the EU has planned with Verification of Payee (VoP) are perhaps the most effective and cheapest APP fraud prevention tool that governments and regulators can mandate.

This may be why they have proven so popular and less contentious than the reimbursement model.

They are simple, and help prevent misleading transfers by flagging mismatches between the recipient's name and the bank account details provided.

This alerts users to potential fraud, encouraging them to reassess the transaction before completing it, and these protocols improve user vigilance by prompting individuals to double-check account details, thereby reducing errors and fraud attempts.

Furthermore, by requiring name matches, systems like this make it more difficult for fraudsters to succeed in social engineering schemes, as mismatched details are likely to trigger alerts.

For example, if someone has one name but another is revealed in their verification process, then consumers are going to be more aware.

They also establish accountability and drive responsibility among consumers, encouraging more careful input of payment details, and creating an effective barrier against fraudulent transactions.

This sort of method helps to reduce the financial losses caused by APP fraud, and promotes trust in digital payments by making electronic transactions safer.

Their universal applicability across different payment infrastructures makes them a globally appealing solution to tackle APP fraud, and if APP fraud continues to wreak havoc globally, then it is possible that international organisations such as the Financial Stability Board (FSB) or the Financial Action Task Force (FATF) could push for global guidelines.

AI: friend or foe to payments firms in the fraud fight?

It is hard to ignore the impact of artificial intelligence (AI) in the financial services sector and how it is revolutionising how PSPs and consumers engage with payments.

However, the rapid growth of AI is a double-edged sword in the context of APP fraud.

Although it offers sophisticated tools to improve fraud prevention, it also equips criminals with advanced tools and methods to exploit victims, raising questions about its overall role in this landscape.

Advanced tools such as deepfake technology allow criminals to convincingly impersonate trusted individuals or organisations, creating fake audio or video communications to deceive victims.

It is hard to miss the news stories about this. For example, a finance worker at a multinational firm in Hong Kong was tricked into paying out $25m to fraudsters using deepfake technology to pose as the company's chief financial officer in a video conference call.

AI-powered chatbots and language models are getting better and better at mimicking human conversations, gaining victims' trust and manipulating them into authorising payments.

AI also enables fraudsters to personalise phishing schemes by analysing social media and other data sources, tailoring scams to specific targets, and can also be used to bypass detection systems by identifying vulnerabilities.

However, AI is also a valuable ally in combating APP fraud. It excels at real-time fraud detection by analysing user behaviour, transaction patterns and anomalies, allowing systems to identify potential fraud before payments are completed and it enhances verification protocols.

It also contributes to user security through biometric authentication methods like facial or voice recognition, ensuring payments are authorised by legitimate users.

Moreover, AI-driven tools can help mitigate phishing risks by scanning emails and websites for fraud indicators.

The relationship between AI and APP fraud prevention highlights its dual nature, and as fraudsters continue to leverage AI to refine their tactics, it is crucial for governments, regulators and financial institutions alike to stay ahead by deploying AI effectively in prevention efforts.

The cross-border payments problem

It is all very well having a strategy to tackle APP fraud, but often, what makes it more challenging to deal with is that this an international issue, and regulatory actions can only account for payments taking place in a jurisdiction such as the UK or EU.

A landmark APP fraud case in the UK was Philipp v Barclays Bank. In this instance, as a result of the fraud, Mrs Philipp was deceived into transferring £700,000 from her Barclays current account to two bank accounts located in the United Arab Emirates.

Attempts to recall the funds that had been transferred were unsuccessful, and although the UK's Supreme Court ruled in favour of Barclays Bank, it revealed how challenging APP fraud is when there is the added layer of cross-border payments.

Others have agreed with this. For example, a report by J.P. Morgan said "actually executing a cross border transaction remains notoriously complex and inefficient. The fragmented nature of the payments system, along with the rapidly expanding volumes, has made this area especially prone to fraudulent activity."

Other parties, such as UK Finance and the Payments Association, have echoed this.

Cross-border payments are more vulnerable to APP fraud due to their complexity and lack of transparency.

Transactions often involve multiple intermediaries, such as correspondent banks and clearing systems, which obscure details and create opportunities for fraudsters to exploit vulnerabilities in the payment chain.

Jurisdictional differences in regulations and enforcement further exacerbate the issue, as fraudsters can target countries with weaker anti-fraud measures.

In addition, delayed settlement times in cross-border payments provide fraudsters with more time to move or withdraw funds before detection.

PSPs can address APP fraud in cross-border payments by utilising technologies such as machine learning to monitor transactions in real time and better identify anomalies.

Stronger authentication measures, such as multi-factor authentication and name-check protocols, can further safeguard transactions.

As has been stressed with domestic APP fraud issues, collaboration between institutions, including global fraud intelligence sharing and participation in networks like Swift's GPI, is also important for lowering the risk.

However, it is not just down to payments processors to reduce these risks. Governments and regulators can also play a role in tackling APP fraud in cross-border payments.

This could be achieved through pushing for better adherence to anti-money laundering standards issued by organisations such as FATF.

Meanwhile, Legal Entity Identifiers (unique 20-character alphanumeric codes that identify legal entities in financial transactions) and digital identity verification can increase transparency and reduce settlement times.

Increasing the mandation of these tools could be another way of bringing down the risk.

Could the UK be an outlier, rather than a trendsetter?

The UK's Payment Systems Regulator (PSR) has been a first mover in introducing reimbursement rules that aim to shield consumers from the financial harms of APP fraud.

However, this introduces the risk that many, including UK Finance and the Payments Association, have warned could be exploited by fraudsters.

There is a rationale for APP fraud being treated differently from unauthorised fraud, which could be considered by other regulators and governments as they begin to tackle this as a policy issue.

APP fraud occurs when victims willingly authorise payments under false pretences, unlike unauthorised fraud, which involves transactions made without the victim's consent.

This distinction justifies a greater emphasis on personal responsibility and shared liability in APP fraud cases.

In APP fraud, victims bypass opportunities to verify payment requests, whereas unauthorised fraud involves no consumer action, making institutional liability more appropriate.

The PSR's approach could end up sparking moral hazard, with consumers becoming complacent about verifying payment details or spotting scams, assuming any losses will be recovered.

This shift in accountability places more burden on PSPs, as consumers increasingly rely on them for fraud prevention, and reduced consumer vigilance could ultimately lead to an increase in fraudulent activities, exacerbating the strain on already stretched payments firms.

Smaller PSPs have been highlighted as particularly at risk, because accumulating fraud losses could exceed their financial capacity, potentially leading to insolvency and a failure to comply with UK prudential requirements.

It has already been blamed for a market exit, with co-founder of the green fintech Tred saying in a LinkedIn post announcing the firm's wind-down that "recent changes to financial regulations around Authorised Push Payment Fraud (APPF) have significantly impacted smaller disruptors like Tred, which we simply aren't equipped to sustain".

With the PSR, and the UK government through its National Payments Vision, striving for a more competitive payments landscape in the UK, such exits do not bode well for the success of the APP fraud policy.

In addition, the regulatory burden of compliance with the reimbursement rules could deter new entrants, stifling market diversity.

As things stand, PSPs need to meet the PSR's compliance expectations, and need to embrace the new modus operandi.

Firms would do well to enhance fraud prevention measures by investing in advanced transaction monitoring and AI-driven fraud detection tools to seek out possible fraudulent accounts.

They should also make use of new tools afforded to them, such as delaying payments, if it seems necessary to do so.

Strengthening these systems could help reduce fraudulent activity and alleviate some of the financial and operational pressures that have been introduced by the reimbursement rules.

The shared liability conundrum

The problem facing the financial services industry — and governments — is how tricky it is to know how best to allocate liability.

As APP fraud has become more rampant, so have the calls for action. In the UK, this has come from organisations such as the consumer advocacy group Which? and the charity Age UK. Politicians from across the aisle, Conservative and Labour, have also paid increasing attention to the impact of fraud on their constituents.

Shared financial liability between PSPs, telecoms providers and social media firms, of the type being suggested by the European Parliament and financial lobbyists in the UK, could address fraud comprehensively by holding all involved parties accountable.

As fraud often originates on social media platforms or through telecoms channels via phishing or social engineering, shared liability incentivises these sectors to enhance anti-fraud measures such as secure communication and improved account verification.

By distributing financial responsibility, this approach reduces the burden on PSPs and fosters collaboration across industries to address fraud at its source. However, the concept involves substantial challenges, and it is unsurprising that some have warned against the measure in the EU.

Determining liability proportions could lead to disputes, delaying reimbursements and anti-fraud efforts. Divided responsibility also risks diluting urgency, as no single entity may feel sufficiently compelled to implement robust prevention measures, and getting the funds back to users could take much longer than is the case under the PSR's current framework.

Critics argue that the European Parliament's shared liability proposal under the Payment Services Regulation (PSR) is flawed and lacks supporting evidence.

For example, a study by Copenhagen Economics warns of unintended consequences, including high societal costs, barriers for smaller players, slower payments and reduced access to services for vulnerable groups.

The study also noted that such a regime could foster blame-shifting rather than collaboration, undermining fraud prevention efforts.

If the EU agreed to such a regime, or if the UK followed suit — which, considering the attention given to the issue by Chancellor Rachel Reeves in her Mansion House speech, could be a possibility — then there is also the obstacle of diplomatic relations with the US, particularly under a Trump presidency.

Trump's inauguration had attendees such as Mark Zuckerberg, owner of Meta; Sundar Pichai, owner of Google; and of course, Elon Musk, owner of X. Given the wealth of these companies, all American, it is easy to see them exerting significant influence on US policy.

Any move by the UK or EU to impose financial liability on these firms could be viewed as hostile to US interests, potentially leading to retaliatory actions, such as trade disputes, tariffs or political pressure to roll back such regulations.

The consequences of this could be significant for international relations, especially if the US perceives such moves as targeting American companies or infringing on their global operations, as has been felt with regulations such as the Digital Services Act (DSA) and General Data Protection Regulation (GDPR).

Diplomatic tensions could escalate, with the US government potentially leveraging its economic and political influence to push back against such frameworks, pressuring the UK or EU to reconsider or abandon these liability rules to avoid harming their relationships with major US tech firms.

How APAC became the dark horse for APP fraud legislation

The focus in recent years has been on the UK and its adaptation to APP fraud, yet there is plenty to be said about the approaches taken in jurisdictions further afield, especially in the APAC region.

APAC countries such as Japan, South Korea, Singapore and Australia have emerged as leaders in combating APP fraud.

They have been overhauling their legal frameworks and prioritising victim compensation, as well as bolstering collaboration among regulators, financial institutions and technology providers as well — something which can at times feel nascent in jurisdictions such as the UK and the EU.

These APAC nations have responded to the rapid digitalisation of their economies and the increasing vulnerability of consumers, particularly the elderly, to scams with both proactive and reactive measures.

Legislation in these countries focuses on victim compensation and fraud prevention, something their Western counterparts have also been keen to master.

For example, Japan's Act on Damage Recovery and South Korea's Special Act on Telecommunications-based Fraud, enacted more than a decade ago, set the standard by enabling victims to recover losses directly from frozen fraudulent accounts.

Singapore's Protection From Scams Act, enacted last year, empowers law enforcement to block fraudulent transactions swiftly.

And Australia's Scams Prevention Framework mandates prevention and detection standards across key industries, something European legislation still falls short of and the US is nowhere near.

Technological and collaborative approaches further enhance these frameworks. Singapore's Anti-Scam Centre and Australia's National Anti-Scam Centre have been able to leverage technology such as scam-blocking apps and data analytics to disrupt fraud.

In addition, consumer education campaigns and shared responsibility frameworks, such as Singapore's initiatives with financial institutions and telecom companies, emphasise consumer awareness and accountability.

However, it will not be all smooth sailing for Western jurisdictions seeking to bring their legislation up to speed with the APAC region.

Systemic and cultural differences mean replicating APAC measures such as Singapore's Protection From Scams Act would be difficult for the UK, the US and the EU

For a start, public trust in government institutions is higher in Singapore, facilitating acceptance of intrusive measures such as freezing accounts without consent.

In contrast, scepticism toward government authority in Western nations could lead to resistance from citizens and civil liberties groups.

Demographics such as the elderly are likely to find it patronising and distressing seeing their bank accounts frozen, and it is not something that a UK bank, for example, may feel comfortable doing to their customer, even in a circumstance where fraudulent activity appears to be apparent.

As a consequence, it is unlikely something so radical would materialise in any of these places.

Conclusion

APP fraud policy is likely to be an evolving issue, and it is undeniably pertinent when you look at chilling statistics such as those in the UK, showing that it is not exclusive to the elderly or vulnerable.

And yet, the patchwork of regulatory initiatives globally reveal just how challenging it is to tackle, either through preventative or reactive measures.

It also differs from the previous fraud leader, unauthorised payments — such fraud occurs when transactions are made without the account holder's approval, making liability relatively clear.

In contrast, APP fraud involves victims being deceived into approving transactions. Although the victim technically gives consent, their approval is based on false pretences. This inevitably creates ambiguity in liability and complicates reimbursement policies.

In unauthorised payment cases, fault typically lies with the fraudster or weaknesses in the financial institution's security system.

However, APP fraud is more complex. It may arise from customer negligence, such as ignoring fraud warnings, or from failings on the part of the PSP, such as not identifying suspicious activity or lacking effective measures like name checks.

Deciding who should bear the cost of APP fraud, whether it is the banks, intermediaries or the victims, is a contentious issue, and policies need to take this into consideration. It is also more manipulative, meaning that blanket measures such as strong customer authentication, which has been used in the UK and EU, will not help.

And then of course, there is the situation of APP fraud decreasing due to improved regulatory measures. Fraud is a "whackamole" issue, and fraudsters are inevitably going to adapt and shift their focus to other tactics.

They may pivot to exploiting stolen credentials or malware to initiate unauthorised transactions, or rely on social engineering techniques to steal personal data and access accounts.

Synthetic identity fraud may also become more common as criminals create fake identities or use compromised ones to exploit financial products, something that is likely to become easier as AI becomes more advanced.

Then, there is the risk of crypto investments becoming even more of a worry.

The new administration in the US has shown itself to be friendly towards crypto, with President Trump himself engaging in so-called memecoins, along with his colleague and donor Elon Musk.

With a rise in promises regarding crypto, it could be that fraudsters turn their attention to high-return crypto investments to lure in consumers keen to utilise their savings. Governments and regulators will need to be proactive over the coming months and years in seeking to address the APP fraud epidemic.

This is no easy task, and developments in technology offer as many opportunities to the fraudsters as they do to regulators.

It will likely take time to devise effective strategies to take on the scammers, especially as their methods keep evolving.

However, with a range of approaches being adopted in jurisdictions around the world, the authorities should soon have a sense of the best ways to keep consumers protected.

VIXIO
Regulatory Intelligence

About Vixio PaymentsCompliance

Vixio PaymentsCompliance is a fast, effective and user-friendly platform that supports compliance activities, removing time-consuming and resource-heavy manual searches and lowering associated costs. With PaymentsCompliance, customers can access real-time regulatory intelligence and updates in 140+ jurisdictions across the world through horizon scanning, expert analysis, and insights to better understand and prepare for changes in payments regulations.

Find out more at Vixio.com/paymentscompliance.com

UK Office
St Clare House, 30-33 Minories
London
EC3N 1DD
Tel: +44 (0) 207 921 9980

US Office
1250 Connecticut Ave NW Suite 700
Washington, DC 20036
Tel: +1 202 261 3567

info@vixio.com

Vixio.com

Our deep understanding of the industries we serve, globally recognised analyst insights and easy-to-use technology are why Vixio PaymentsCompliance is trusted by some of the largest names in payments and other industries, including:

PayPal DISCOVER ByteDance

Disclaimer

This report has been created by Vixio PaymentsCompliance, a product of Vixio Regulatory Intelligence. Information contained within this report cannot be republished without the express consent of Vixio PaymentsCompliance.

Vixio PaymentsCompliance does not intend this report to be interpreted, and thus it should not be interpreted, by any reader as constituting legal advice. Prior to relying on any information contained in this article it is strongly recommended that you obtain independent legal advice. Any reader, or their associated corporate entity, who relies on any information contained in this article does so entirely at their own risk. Any use of this report is restricted by reference to Vixio PaymentsCompliance's terms and conditions.

© Compliance Online Limited (trading as Vixio) 2025