Beyond Compliance:

Building a Trusted Global Payments Framework

LSEG RISK INTELLIGENCE

Table of contents

Executive summary

Global payment systems are converging around shared objectives of transparency, consumer protection and traceability as instant payments expand, cross-border volumes grow and fraud tactics evolve. While regulatory frameworks and payment infrastructures continue to vary by jurisdiction, the direction is clear: trust must be established earlier in the payment lifecycle and supported by high-quality data and effective verification.

Fraud remains a material risk for organisations operating at scale. In the United Kingdom, total fraud losses reached £1.17 billion in 2023 (UK Finance 2025). In the United States, 79 percent of organisations reported attempted or actual payments-fraud incidents in 2024, while recovery rates have declined steadily since 2023 (Association for Financial Professionals 2023; 2024; 2025). Globally, businesses lost an average of 7.7 percent of annual revenue to fraud in 2025, with industry estimates suggesting authorised push-payment fraud (also known as authorised payment scams) losses could exceed USD 330 billion by 2027 (TransUnion 2025; World Economic Forum 2025).

Regulators are responding through reforms that raise baseline expectations for transparency, accountability and data integrity. Updates to FATF Recommendation 16, the EU Instant Payments Regulation, proposed Payment Services Directive 3, reimbursement regimes in the United Kingdom and enhanced monitoring obligations across the United States and Asia-Pacific reflect a common emphasis on verification and shared responsibility across payment chains (Financial Action Task Force 2025; European Commission 2024; Payment Systems Regulator 2025; Nacha 2025).

Despite this momentum, compliance alone has not reduced overall exposure. Fraud increasingly exploits trust and process weaknesses before payments are executed, limiting the effectiveness of post-event controls. For organisations, this reframes payment risk as a strategic resilience issue rather than a narrow compliance challenge, particularly as cross-border payment volumes are projected to reach USD 250 trillion by 2027 (Bank for International Settlements 2020; 2024; 2025).

In this context, approaches to trusted data, standards adoption and risk intelligence vary by region and payment scheme—but many organisations are moving earlier in the payment lifecycle to strengthen verification and assurance.

LSEG supports multinational corporations, fintechs, payment service providers, and financial institutions with data, analytics and risk intelligence to inform decision-making and operational controls across the payment lifecycle.

With its combined strengths in financial markets, data, analytics and regulatory insight, LSEG provides organisations with tools that can inform their approach to understanding regulatory change and evolving fraud risks.

Organisations remain responsible for determining their own regulatory obligations and compliance approach.

Introduction:

Global payments are converging around shared goals

Global payment systems are increasingly working towards the same core objectives: improving transparency, strengthening consumer protection and ensuring traceability across payment flows. While market structures, payment rails and regulatory regimes continue to differ by region, the underlying directional trend is consistent. Regulators, financial institutions and market participants are responding to common pressures driven by faster payments, growing cross-border activity and increasingly sophisticated fraud.

The scale of the challenge is material. In the United Kingdom, total fraud losses reached £1.17 billion in 2023, highlighting the financial and societal impact of payment-related crime (UK Finance 2025). In the United States, exposure is similarly widespread, with 79 percent of organisations reporting attempted or actual payments-fraud incidents in 2024, reflecting the breadth of risk faced by businesses across payment types and channels (Association for Financial Professionals 2025).

In response, regulatory frameworks are evolving. Authorities across Europe, North America and Asia-Pacific are introducing new requirements focused on payment transparency, verification and shared accountability. These measures signal a clear intent to raise baseline standards across the payments ecosystem.

However, despite growing alignment at a policy level, material differences remain in how regulations are designed, implemented and enforced across jurisdictions. For organisations operating across multiple markets, this creates a complex compliance landscape that cannot be addressed through a single, uniform approach.

In practice, this fragmentation is most visible in large, decentralised organisations. Treasury and payments teams often operate across multiple banking partners, local payment formats and approval workflows, making it difficult to apply consistent verification controls at the point where payments are released.

As regulation converges around common principles, organisations face a dual imperative: meeting local compliance obligations while contributing to a globally consistent standard of trusted payments. Achieving this requires moving beyond minimum regulatory requirements towards verification-led approaches that protect businesses, customers and counterparties throughout the payment lifecycle.

The regulatory landscape:

Recent developments shaping the next phase of payments compliance

Regulatory reform across major payment markets reflects a shared recognition that legacy controls have not kept pace with the speed and complexity of modern payments. **Recent and forthcoming measures focus on strengthening transparency, improving data quality and extending accountability across payment chains.**

At a global level, the Financial Action Task Force updated Recommendation 16 in June 2025, reinforcing requirements for complete and accurate originator and beneficiary information for transfers exceeding USD/EUR 1,000 (Financial Action Task Force 2025). The revised standard emphasises ISO 20022-structured data to improve traceability and interoperability across domestic and cross-border payments. FATF has indicated a multi-year implementation horizon extending into 2027–2030, signalling that compliance expectations will increasingly apply not only to financial institutions, but also to corporates and organisations generating, receiving and managing payment data.

In the European Union, regulatory momentum continues through a combination of legislative reform and supervisory guidance. **The Instant Payments Regulation introduces mandatory real-time Verification of Payee across the SEPA zone** (European Commission 2024). In parallel, the proposed **Payment Services Directive 3** and the **Payment Services Regulation extend liability and consumer protection measures for impersonation and authorised push-payment fraud** (European Commission 2023). Additional implementation guidance published in 2025 by the European Banking Authority and the European Central Bank clarifies supervisory expectations around fraud reporting, data quality and operational controls (European Banking Authority 2025; European Central Bank 2025).

European Union

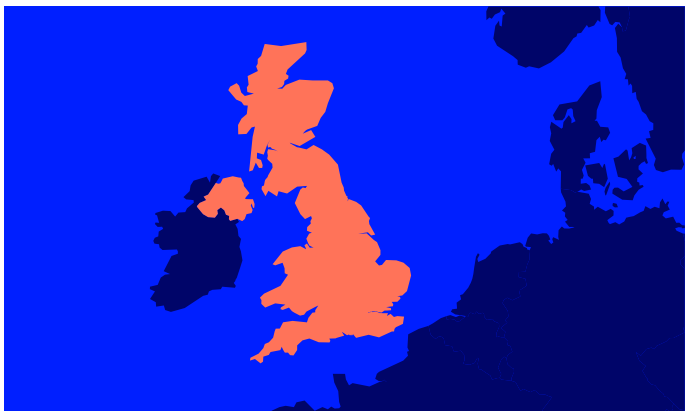
In the United Kingdom, the Payment Systems Regulator's mandatory reimbursement regime for authorised push-payment fraud, effective from October 2024, formalises shared accountability between sending and receiving institutions for losses of up to £85,000 per case (Payment Systems Regulator 2024). Subsequent PSR performance reporting releases in 2024 and 2025 show significant variation in reimbursement outcomes across institutions, underlining that compliance alone does not guarantee effective fraud prevention (Payment Systems Regulator 2025).

Similar developments are evident elsewhere. **In the United States, Nacha's 2025 guidance clarifies fraud-monitoring obligations for both originating and receiving financial institutions** (Nacha 2025). **Across Asia-Pacific, regulators are advancing anti-scam frameworks, including mandatory payee-name validation in Hong Kong** (Hong Kong Monetary Authority 2024) and expanded enforcement and industry obligations under Australia's National Anti-Scam Centre (Australian Competition and Consumer Commission 2025).

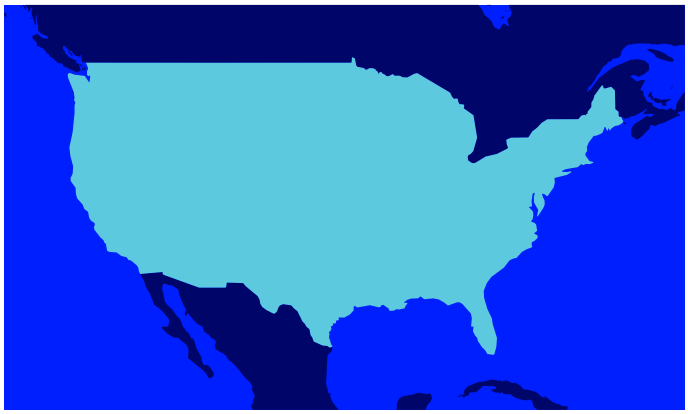
For organisations operating across Europe and Asia-Pacific, this increasingly means parallel requirements for payee validation, structured payment data and faster settlement timelines. Meeting these obligations through manual checks or fragmented systems has proven difficult to sustain at scale.

Collectively, these developments illustrate a clear regulatory trend. **Authorities are raising baseline expectations for transparency, verification and accountability, while leaving implementation choices largely to market participants.**

United Kingdom



United States



Asia-Pacific

Compliance as a baseline, not the endpoint

Despite regulatory progress, fraud continues to generate material losses. In the United Kingdom, 72 percent of authorised push-payment fraud (also known as authorized payment scams) cases in the first half of 2024 originated online, accounting for 32 percent of total losses (UK Finance 2024). Among major UK banks, authorised push-payment fraud losses equated to £266 per £1 million of outgoing transactions, underscoring the scale of exposure embedded in routine payment activity (Payment Systems Regulator 2025).

In the United States, recovery outcomes remain limited. Only 22 percent of organisations recovered 75 percent or more of their fraud losses in 2024, down from 41 percent in 2023, indicating a sustained decline in recovery rates despite increased controls (Association for Financial Professionals 2023; 2024; 2025).

Globally, businesses lost an average of 7.7 percent of annual revenue to fraud in 2025, equating to an estimated USD 534 billion across industries (TransUnion 2025). Industry estimates suggest global authorised push-payment fraud losses could exceed USD 330 billion by 2027, reflecting the combined impact of instant payments, cross-border complexity and social engineering (World Economic Forum 2025; Bank for International Settlements 2024; International Monetary Fund 2025).

At the same time, threat vectors continue to evolve. Phishing and social engineering remain dominant enablers of payment fraud, with both the ENISA Threat Landscape and the Verizon Data Breach Investigations Report identifying sustained growth in these attack methods across regions and sectors (ENISA 2025; Verizon 2025).

In many reported cases, fraud is only detected after internal approvals have been completed and funds have left the organisation. At that stage, recovery depends on the speed and cooperation of counterparties and intermediaries rather than the originating organisation's own controls.

Regulatory frameworks mitigate liability and establish minimum standards, but they cannot prevent operational disruption, reputational damage or liquidity risk once payments are executed. These limitations highlight the need for controls that operate before payments are initiated, rather than relying solely on post-event remediation.

Building a trusted, global payments framework

Fraud risk remains widespread across payment types. In the United States, 63 percent of organisations reported attempted or actual cheque fraud in 2024, illustrating that both legacy and modern payment rails remain vulnerable (Association for Financial Professionals 2025).

Real-time account verification and structured payment data improve control and reconciliation across payment processes. Regulators and industry bodies increasingly emphasise pre-payment verification as a foundational control within modern payment systems (European Commission 2024; Nacha 2025).

A common risk scenario involves changes to supplier payment details. Organisations frequently report that otherwise legitimate invoices are compromised through email-based social engineering, with amended bank details submitted shortly before payment deadlines.

This risk is amplified in cross-border payments, where unfamiliar counterparties, time zone differences and language barriers reduce the effectiveness of manual checks and increase reliance on upstream data quality.

Embedding account-owner validation, payee-name matching and behavioural analytics within enterprise payment workflows strengthens both compliance and fraud prevention. These controls help detect anomalies earlier, reduce reliance on post-event recovery and support consistent payment assurance across jurisdictions.

Greater collaboration between financial institutions and corporates further enhances effectiveness. Sharing intelligence on emerging fraud patterns, typologies and mule activity improves collective detection capabilities and supports faster, more coordinated responses across the payments ecosystem.

Building resilience beyond compliance

Authorised push-payment fraud (also known as authorised payment scams) losses in the United Kingdom totalled approximately £459.7 million in 2023, reflecting the growing exposure faced by both consumers and businesses (Financial Times 2024). At the same time, cross-border payment volumes are projected to reach USD 250 trillion by 2027, increasing the scale and complexity of payment risk (Bank for International Settlements 2020; 2024; 2025).

Compliance obligations alone cannot address the operational, reputational and liquidity risks businesses face as payment speeds increase and fraud tactics evolve. For organisations operating across multiple markets, fragmented controls increase exposure at precisely the point where payments are most difficult to recall.

In several reported incidents, organisations have noted that the most significant impact was not the immediate financial loss, but delayed settlements, strained supplier relationships and escalation to senior management and boards.

Proactive verification, integrated identity assurance and continuous monitoring are therefore increasingly viewed as strategic enablers. These capabilities support regulatory compliance while also protecting supplier relationships, safeguarding cash flows and maintaining trust across the global payments ecosystem.

Conclusion:

A verification-led approach to payment trust

Across major markets, regulatory and scheme reforms are placing greater emphasis on transparency, traceability and accountability—while implementation requirements and liability models continue to differ by jurisdiction.

For organisations, this points to a practical operating approach: treat compliance as the baseline, and build additional assurance through verification-led controls that operate before funds move. In practice, that means **improving data integrity, using structured payment data where available, and embedding payee/account-owner checks and change-event validation at key points in the payment lifecycle.**

As payment ecosystems evolve, organisations that invest in stronger verification, robust data governance and collaborative intelligence-sharing will be better positioned to reduce preventable errors and fraud exposure, and to demonstrate well-governed payment processes across markets.

The fraud and loss statistics cited in this paper are presented to illustrate the scale and direction of risk, not as a prediction of outcomes for any individual organisation. Organisations remain responsible for assessing their risk profile and regulatory obligations, and for determining the appropriate mix of controls for their markets and payment rails.

About LSEG Trusted Payments Solutions

Confidence in every payment, across the payments lifecycle.

Trusted Payments helps organizations ensure money moves where it should – securely, and at the speed of business.

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 coverage of US consumer and business bank accounts. 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, spanning 45+ countries and actively expanding, 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, limit reputational damage, reduce fraud and comply with legal and regulatory obligations 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, account verification – organisations can trust LSEG Risk Intelligence to help them manage their risk, so they can operate more efficiently, more effectively and more confidently.

To learn more, visit **www.lseg.com/risk-intelligence.**

LSEG RISK INTELLIGENCE