Cross-Border Payments and Financial Crime: Why Fragmented Monitoring Is No Longer Fit for Purpose

March-3, 2026

By any measure, cross-border payments sit at the centre of the modern financial system. They facilitate global trade, remittances, investment flows, and digital commerce. Yet they also represent one of the most persistently vulnerable channels from a financial crime perspective.

The Financial Action Task Force (FATF) has long identified correspondent banking and international payment flows as inherently higher risk, reflecting their complexity, opacity, and reliance on multiple intermediaries. In its guidance on correspondent banking

services, the FATF has warned that these structures heighten exposure to money laundering and terrorist financing when information degrades across institutions and jurisdictions.

For banks, fintechs, and payment firms operating across borders, the challenge is no longer simply one of regulatory compliance. It is increasingly a question of whether traditional control models are structurally capable of managing risk in an environment defined by speed, scale, and fragmentation.

Structural Risk in a Fragmented System

Cross-border payments expose institutions to financial crime not because money crosses borders per se, but because risk signals fracture as transactions move through multiple systems, legal regimes, and intermediaries.

The Basel Committee's Financial Stability Institute has repeatedly highlighted how correspondent banking chains and nested relationships reduce transparency and weaken accountability. Supervisory studies note that indirect access arrangements can limit a bank's ability to understand the underlying customer risk of transactions passing through its accounts.

In practice, this fragmentation manifests in several ways:

- Originator and beneficiary data may be truncated or reformatted
- Different jurisdictions apply varying KYC and beneficial ownership standards
- Regulatory expectations diverge across regions
- Payment messages pass through multiple screening environments

The result is what compliance professionals often describe as partial visibility. No single institution sees the entire transaction context.

FATF's 2016 guidance on correspondent banking emphasised that these vulnerabilities are particularly acute where respondent banks service third-party clients, leaving upstream correspondents with limited insight into the true economic purpose of transactions.

Risk is further shaped by payment corridors. UK-Africa remittance flows, Asia-Middle East trade routes, and Latin America-US payment channels have each been associated in regulatory and law enforcement reporting with distinct typologies, including informal value transfer systems, trade-based money laundering, sanctions exposure, and cyber-enabled crime.

The Bank for International Settlements (BIS) has consistently observed that divergent regulatory frameworks and operational practices remain a defining feature of cross-border payments.

Enduring Regulatory Expectations

Despite jurisdictional differences, supervisory authorities have converged around a set of core principles for managing cross-border financial crime risk.

FATF continues to frame the risk-based approach as the foundation of effective AML and CFT regimes, requiring institutions to identify, assess, and understand their risks and apply proportionate mitigation measures.

Similarly, Basel Committee guidelines on operational and financial crime risk emphasise governance, accountability, and integration with enterprise-wide risk frameworks.

In the UK, the Financial Conduct Authority (FCA) has repeatedly stressed the importance of risk-sensitive and proportionate controls. Within a 2019 enforcement action against a global bank, the regulator cited failures to maintain adequate policies and procedures for managing high-risk correspondent relationships.

In Singapore, the Monetary Authority of Singapore (MAS) places explicit responsibility on boards and senior management for setting risk appetite and overseeing control effectiveness. Its AML/CFT guidelines emphasise that accountability cannot be outsourced or displaced by automation.

Across jurisdictions, regulators continue to prioritise:

- End-to-end transaction monitoring
- Enhanced due diligence for higher-risk relationships
- Ongoing screening and review
- Robust record-keeping and auditability
- Senior management ownership

FATF has also consistently warned that indiscriminate “de-risking” is not an acceptable substitute for effective risk management.

The Limits of Legacy Monitoring

Despite these expectations, many institutions continue to rely on monitoring architectures designed for a different era.

Traditional compliance systems are typically characterised by:

- Rules-based alert generation
- Static thresholds
- Product-specific silos
- Limited behavioural analysis
- Heavy manual review

While such systems may satisfy minimum regulatory requirements, they struggle to cope with modern cross-border volumes and typologies.

Regulatory reviews and industry surveys have repeatedly highlighted high false-positive rates, fragmented investigations, and weak prioritisation. Compliance teams are often overwhelmed by alert volumes that obscure genuinely high-risk activity.

Another enforcement action that the FCA leveraged against a UK Bank in 2024 illustrates this dynamic. The regulator found that sanctions screening systems failed to keep pace with rapid customer growth, leading to prolonged exposure. The bank was fined £28.96 million for deficiencies in financial crime systems and controls.

Similarly, investigations into a Scandinavian Bank's Baltic branch demonstrated how poor systems integration and weak oversight allowed suspicious non-resident flows to pass undetected for years. External reviews and supervisory findings pointed to fragmented IT infrastructure and inadequate monitoring capability as key contributors.

In the United States, FinCEN's assessment of one bank found that weaknesses in monitoring foreign correspondent accounts delayed the detection of suspicious activity involving more than $11.5 billion in aggregate transactions.

Across these cases, regulators identified systemic weaknesses in governance, data integration, and control design rather than isolated technical failures.

Rebuilding the Detection Architecture

Leading institutions are responding by redesigning financial crime monitoring as an integrated, enterprise-wide capability rather than a standalone compliance function.

Modern architectures increasingly combine:

- Centralised data platforms
- Real-time screening engines
- Behavioural analytics
- Network and relationship analysis
- Unified case management
- Automated audit evidence

Rather than treating sanctions screening, AML monitoring, and fraud detection as separate disciplines, firms are converging these capabilities onto shared data and analytics layers.

SWIFT and CPMI have both emphasised that improvements in payments data quality and standardisation under ISO 20022 are critical enablers of more effective compliance screening and risk management.

Richer, more structured data supports improved identification of parties, transaction purposes, and behavioural patterns.

Regulators, however, continue to caution that technology alone is insufficient. Without governance, quality controls, and skilled oversight, advanced platforms risk reproducing old weaknesses at greater scale.

The Responsible Use of Advanced Analytics

Machine learning and advanced analytics now form a central component of modern monitoring strategies. When deployed responsibly, they can enhance detection across complex corridors and evolving typologies.

High-impact applications include:

- Anomaly detection across payment flows
- Behavioural profiling at customer and entity level
- Network analysis for mule and facilitation networks
- Adaptive risk thresholds
- Natural language processing for investigations

The Wolfsberg Group has stressed that effective monitoring requires the integration of transactional, behavioural, and customer-risk information, and that alerting frameworks must reflect holistic risk assessment rather than isolated rule triggers.

Supervisory scrutiny of AI systems is also increasing. Regulators now expect explainability, model governance, and documented human oversight.

The FCA has emphasised that automated systems must be subject to validation, performance monitoring, and formal approval processes, and that decisions with material customer impact must remain reviewable.

This has reinforced the importance of human-in-the-loop controls and transparent model design.

Data as a Control Environment

At scale, data governance becomes a financial crime control in its own right.

Cross-border monitoring depends on the effective integration of:

- Payments messages
- KYC and beneficial ownership records
- Sanctions and PEP lists
- Corporate registries
- Adverse media
- Device and behavioural data
- Trade documentation

The Wolfsberg Correspondent Banking Due Diligence Questionnaire reflects this breadth, incorporating governance, fraud controls, and identity management indicators.

FATF's trade-based money laundering risk indicators similarly illustrate how transaction data must be assessed alongside shipping, pricing, and commodity information.

Institutions continue to face challenges in data quality, normalisation, lineage, and privacy compliance. Localisation laws and cross-border transfer restrictions complicate centralisation strategies.

The Bank of England's consultation on ISO 20022 adoption in CHAPS has highlighted the importance of improving data quality at source rather than relying solely on format conversion.

Preparing for the Next Phase

Structural changes in payments are intensifying monitoring challenges.

Instant settlement compresses investigation windows, embedded finance expands the regulatory perimeter and central bank digital currencies introduce new intermediaries and transaction models.

FinCEN reported that ransomware-related payments reached $1.1 billion in 2023 before declining to $734 million in 2024 following international disruption efforts, demonstrating the speed with which criminal proceeds can move across borders.

At the same time, supervisors are deploying SupTech tools and demanding more granular data. Continuous supervision is replacing periodic reviews.

These trends point towards a future in which financial crime controls must operate in near real time and across institutional boundaries.

A Strategic Framework for Leadership

For MLROs and heads of financial crime, sustainable cross-border risk management rests on six pillars.

- First, institutions must define corridor-specific risk appetite aligned to business strategy.
- Second, they must establish end-to-end visibility across onboarding, payments, counterparties, and behaviour.
- Third, detection architectures must integrate screening, behavioural analytics, and network analysis.
- Fourth, data governance must be treated as a core control function.
- Fifth, operating models must support global consistency and specialist capability.
- Sixth, vendor management and regulatory engagement must focus on outcomes rather than formal compliance.

Professional services firms, including one of the big 4 consulting firms, have consistently noted that successful ISO 20022 and monitoring transformations require coordinated investment in systems, governance, and people.

Ready to Move Beyond Fragmented Monitoring?

The structural challenges outlined in this article, partial visibility, siloed systems, and overwhelming alert volumes, can no longer be addressed by legacy monitoring tools alone. True resilience in cross-border risk management requires a platform that can see across transactions, behaviours, networks, and data domains in real time, and support meaningful, actionable decision-making.

Quantum Data Engines' *Conquer Fraud* platform does exactly that. Built for complex enterprise environments, Conquer Fraud brings together:

- Real-time screening and transaction monitoring that combines traditional rules with anomaly and network analysis;

- Behavioural, device, and sanctions intelligence tied into unified case workflows;
- Hybrid analytics and auto-prioritisation to reduce false positives and surface genuinely high-risk activity;
- Regulator-ready audit trails and investigation packs.

Rather than patching fragmented feeds and alerts, Conquer Fraud provides a connected detection architecture, giving compliance teams end-to-end visibility, greater precision, and the capacity to act confidently at scale.

Quantum Data Engines™

Quantum Data Engines is a reg-tech company that helps financial institutions detect, manage, and report financial crime more effectively and efficiently.

For more details write to: connect@qde.ai