The Cost of Non-Compliance: What Recent FCA Fines Tell Us About AML Weaknesses

January-1, 2026

In the last three years, the UK's financial regulators have delivered one message with absolute clarity: weaknesses in anti-money laundering (AML) systems are no longer a side-note in supervisory reviews but a defining benchmark of a firm's operational integrity.

Enforcement activity since 2023 shows a sharply evolving landscape in which the Financial Conduct Authority (FCA) is moving away from episodic mega-fines and towards a more frequent cadence of targeted, mid-tier actions that cut across the retail, wholesale, fintech and payments sectors.

These cases, viewed collectively, demonstrate that the FCA's core concerns remain unchanged, customer due diligence (CDD), enhanced due diligence (EDD), ongoing monitoring, sanctions screening, and governance. What has changed is the FCA's expectation that firms will internalise lessons from previous enforcement, modernise systems at pace, and establish a culture that treats AML as a strategic imperative rather than a technical compliance burden.

Across banks, trading intermediaries, payment institutions and digital-first challengers, the same pattern emerges again and again: poor understanding of customer risks, inconsistent application of rules, under-resourced monitoring teams and a tendency to prioritise commercial growth over foundational financial-crime controls. These failings carry a high financial cost for firms, but a higher systemic cost for the integrity of the UK's financial system.

This article aim to explore the most recent FCA enforcement actions between 2023 and 2025, drawing out the recurring weaknesses, the regulator's shifting expectations, and the deeper lessons for boards and senior management across the industry.

A Turning Point in Compliance Enforcement

The enforcement cases of 2023–2025 reflect a shift in regulatory tone. While the past decade saw several eye-catching sanctions, often exceeding £100 million for a single institution, the recent cycle is characterised by sharper, more frequent interventions focused specifically on systemic weaknesses.

Across the period from early 2023 to late 2025, the FCA issued a series of significant AML-related penalties across a diverse set of institutions. These included a UK subsidiary of a large African-headquartered bank, an Islamic retail bank, a wholesale brokerage firm, a UK payment institution supporting cryptoasset trading, a mid-sized high-street bank, a

digital-first challenger bank, and a longstanding UK high-street banking group with global operations. Each case was distinct in its operational context, yet strikingly similar in its root causes.

What binds these cases together is not the industry or business model, but the fundamental breakdowns in AML systems and controls during periods of rapid commercial activity. Whether onboarding retail customers at speed, managing high-risk corporate clients, or processing millions of payment flows daily, these firms encountered the same fault line: a mismatch between risk exposure and the strength of the controls designed to mitigate it.

When Oversight Fails: The Early 2023 Cases

The year began with two separate enforcement actions involving specialist banks operating in the UK. One, the UK arm of a large financial group headquartered in West Africa, was fined just over £7.6 million after a skilled person review examined 314 customer files and identified significant deficiencies in due diligence, record-keeping and risk assessment. The firm's AML framework suffered from outdated policies, fragmented processes and limited senior management oversight, failings that persisted despite several internal warnings and external reviews.

Only a day later, another institution, this one a UK-based Islamic retail bank, was fined £4 million for systemic failures in CDD, EDD and ongoing monitoring. Here too, the FCA identified insufficient risk assessment at onboarding, inconsistent application of policy, and a failure to escalate red flags appropriately.

These early actions set the tone for what would follow: the FCA was signalling that delays in remediation, however well-intentioned or operationally justified, would no longer be tolerated. The regulator was also making explicit that firms operating in niche or

specialist segments are not exempt from the same standards applied to larger institutions.

A Wake-Up Call for the Wholesale Sector

In October 2023, the FCA issued a £6.47 million fine to a long-established wholesale brokerage firm providing execution and clearing services to institutional clients. While retail banking has traditionally attracted the most AML scrutiny, this case underscored the regulator's increasing attention on the wholesale markets, where large transaction volumes, complex structures and cross-border flows can obscure financial-crime risks.

The FCA found that the brokerage's financial crime controls were not aligned with the scale and complexity of its business. Among the issues raised were insufficient due diligence on high-risk counterparties, gaps in monitoring processes, and poor governance oversight of financial-crime responsibilities. As intermediaries play a crucial role in safeguarding market integrity, this case served as a strong reminder that wholesale firms are expected to maintain rigorous controls even when dealing primarily with institutional clients.

The UK's First Crypto-Linked FCA Enforcement

In July 2024, the regulator issued a landmark enforcement action against a UK-regulated payment institution supporting cryptoasset trading. Although the firm did not operate a crypto exchange itself, its e-money permissions allowed it to provide fiat access to crypto platforms, a role that placed it at the frontline of financial-crime risk.

The FCA fined the institution £3.5 million for breaching a voluntary requirement (VREQ) that imposed restrictions on the onboarding of high-risk customers. Despite those restrictions, the firm onboarded 13,416 high-risk customers, of whom about 31 percent

made 12,912 prohibited deposits totalling USD $24.9 million. These funds were subsequently used for withdrawals and cryptoasset trades totalling approximately USD $226 million.

The FCA emphasised that this was the first enforcement action involving a regulated firm enabling cryptoasset activity under the UK's money-laundering framework. The case established a clear precedent: firms providing infrastructure for crypto flows, regardless of whether they touch the cryptoassets directly, must apply a heightened standard of monitoring and oversight.

A Major High-Street Bank and the Scale of Missed Alerts

In November 2024, a mid-sized high-street bank received a fine of £16.7 million after the FCA uncovered severe failures in its transaction-monitoring systems. The regulator found that over 60 million transactions, totalling more than £51 billion, were not appropriately monitored over prolonged periods due to system misconfigurations and flawed governance.

The issue had begun with an apparent technical error, but escalated into a multi-year breakdown of oversight in which alarms were ignored, escalations were ineffective and senior management engagement was insufficient. The case served as a stark reminder that operational resilience in AML systems is not merely a technology question but a governance one. When transactions on this scale pass through a bank without appropriate scrutiny, the risk to the financial system is profound.

The Fintech Reckoning: Challenger Banks Under the Microscope

Perhaps the most telling trend in recent enforcement is the rise in penalties against digital-first banks, firms that built their reputation on agility, customer-centric design and modern technological infrastructure.

In September 2024, a fast-growing UK challenger bank was fined £28.95 million after the FCA discovered that it had onboarded 54,359 accounts for 49,183 high-risk customers in breach of a VREQ designed to restrict precisely this activity. Weaknesses in sanctions screening compounded the issue; at one point, the bank's controls limited sanctions checks to a narrow subset of designated persons, leaving large gaps in the firm's defences.

Then, in 2025, another digital-only bank, one of the UK's best-known fintech challengers, was fined £21.09 million for CDD, EDD and monitoring failures that emerged during a period of rapid customer growth. These failures were especially concerning because they suggested that despite advanced technology stacks and strong revenues, some firms had prioritised expansion over financial-crime controls.

Across 2024 and 2025, these two challenger banks together accounted for over 90 percent of all AML-related fines issued in that period. The signal from the FCA was unmistakable: innovation is welcome, but not at the expense of systemic safeguards.

A High-Street Institution Under Scrutiny: The 2025 Penalty

In July 2025, the FCA levied a £42 million combined fine against a longstanding, widely recognised UK banking group and its sister entity for long-running financial-crime control failures. The case centred on the bank's failure to detect and interrogate suspicious

incoming funds, amounting to £46.8 million, received by a high-risk client closely linked to a well-known money-laundering scandal in the UK.

This client relationship, involving significant cash-intensive activity, presented clear red flags. Yet the bank's oversight mechanisms, risk assessments and escalation processes failed to identify or act upon the risk. The case illustrated the consequences of inadequate scrutiny in high-risk commercial relationships, particularly those involving complex corporate structures and international money flows.

Recurring Themes: What These Cases Reveal

Despite differences in business model, scale and customer base, the recent enforcement actions share a set of common weaknesses that cut across every segment of the sector.

1. Customer Due Diligence Failures

Nearly every case involved insufficient CDD or EDD, either outdated processes, inconsistent application or poor documentation. Firms often underestimated the risk level of their clients or failed to respond when customer profiles changed.

2. Weak Transaction Monitoring Systems

The mid-sized retail bank's failure to monitor over 60 million transactions is the most dramatic example, but other firms also suffered from fragmented monitoring, ineffective alert logic, or systems poorly integrated with customer-risk ratings.

3. Poor Governance and Senior Management Engagement

In several cases, including those involving wholesale firms and digital challengers, governance committees were either unaware of ongoing breaches or did not act decisively to address them.

4. Delayed or Inadequate Remediation

A consistent theme was the gap between identifying an issue and resolving it. Some firms had recognised weaknesses years earlier but failed to implement effective remediation, often focusing on short-term operational pressures instead.

5. Misuse or Breach of VREQs

The FCA increasingly relies on voluntary requirements (VREQs) to constrain high-risk activity. Several recent cases show firms breaching these obligations, whether through oversight failures or misaligned incentives.

A Regulator Redefining Its Expectations

Taken together, the enforcement actions illustrate how the FCA's supervisory expectations have evolved. The regulator is now signalling that:

- Financial-crime controls must scale with commercial growth. High-growth fintechs are particularly exposed to this risk.
- AML systems must be resilient and continuously tested. Technical errors that result in unmonitored activity will not be forgiven.
- Governance must be proactive, not reactive. Boards are expected to challenge management and demand tangible progress.

- VREQs are binding commitments, not mere supervisory tools. Breaching them is seen as a direct governance failure.
- Crypto-related activity is under heightened scrutiny. Even indirect exposure brings high expectations.

The regulator is no longer focused solely on punishing catastrophic failures. Instead, the FCA is tightening perimeter expectations and pushing firms to demonstrate that they can sustain robust AML frameworks even during transformation, expansion or operational stress.

Lessons for the Future

These cases offer important insights not only for firms recently fined, but for every organisation active in the UK's financial sector.

1. Rapid growth cannot outpace AML capabilities.

Firms must invest early and significantly in scalable AML infrastructure.

2. Data quality is as important as data volume.

Without accurate, actionable customer data, even sophisticated monitoring systems will fail.

3. Governance must be consistent and forensic.

Boards and executive teams must maintain direct oversight of AML risks, rather than delegating them entirely to second-line functions.

4. Technology is not a silver bullet.

Whether legacy or cloud-native, systems must be tested, calibrated and monitored—technology without governance is simply automation of risk.

5. VREQs demand absolute compliance.

They are warnings in all but name; breaching them invites severe consequences.

Conclusion: The True Cost of Non-Compliance

The FCA's recent enforcement actions reflect more than isolated supervisory interventions, they represent a recalibration of regulatory expectations across the industry. In a period defined by digital transformation, rising geopolitical tensions and an increasingly complex financial-crime landscape, the regulator has made clear that AML failures pose a threat not only to individual firms but to the wider financial ecosystem.

The direct financial penalties across the 2023–2025 period are substantial. But they pale in comparison to the indirect costs: reputational damage, operational restructuring, remediation spend, and the erosion of stakeholder confidence. The message is simple but uncompromising: in the modern UK financial system, robust AML controls are not a compliance formality, but a foundational pillar of institutional credibility.

For boards, senior managers and shareholders alike, the lesson is clear. The cost of non-compliance is far greater than the cost of getting AML right from the start.

How Quantum Data Engines can help

The recent FCA cases make one point unmistakably clear: AML resilience now depends on the strength of a firm's data, the robustness of its transaction-monitoring systems, and its ability to scale controls as quickly as the business grows.

Whether the risk arises from high-risk onboarding, fragmented CDD and EDD processes, inconsistent sanctions screening, crypto-linked payment flows, or millions of unmonitored transactions hidden by system misconfigurations, the underlying issue is the same; inadequate financial-crime infrastructure.

Quantum Data Engines (QDE) helps firms close exactly these gaps. QDE's platform strengthens the full AML lifecycle: integrating customer data, upgrading monitoring logic, improving alert quality, enhancing risk-model governance, and modernising legacy systems that can no longer keep pace with regulatory expectations.

For institutions operating in retail banking, wholesale markets, payments, or fast-scaling digital channels, QDE's expertise provides the kind of end-to-end AML transformation that prevents the operational weaknesses seen across recent FCA actions.

For firms looking to build monitoring frameworks that are accurate, scalable and regulator-ready, Quantum Data Engines offers a practical path to turning AML vulnerabilities into long-term operational strength.

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