

Beyond Record Fines: A Deep Analysis of UK and French AML Enforcement

Executive Summary

Anti-money laundering (AML) enforcement in the United Kingdom and France is undergoing a significant shift. While public attention often focuses on record-breaking fine totals, the underlying regulatory reality is far more complex. Modern enforcement reveals two distinct systems using a combination of supervision, administrative sanctions, criminal proceedings, and asset recovery to address persistent systemic weaknesses. Critical takeaways from recent enforcement actions include:

- **Move Beyond Metrics:** Fine values are often misleading; the true measure of enforcement is the identification of control weaknesses and the subsequent change in institutional behavior.
- **Systemic Failures in Established Banks:** Major penalties, such as the £107.8 million fine against Santander UK, highlight long-standing failures to reconcile expected customer activity with actual transaction behavior.
- **Challenger Bank Scrutiny:** Rapid onboarding and automated decision-making in the fintech sector have outpaced financial-crime controls, leading to significant penalties for firms like Starling and Monzo.
- **Data Integrity as a Compliance Pillar:** As demonstrated by Metro Bank, transaction monitoring is ineffective if data quality and system configurations are flawed, leading to millions of unmonitored transactions.
- **Regulatory Consolidation:** Both jurisdictions are moving toward more centralized oversight, with the UK's FCA expanding its remit and the EU establishing the Anti-Money Laundering Authority (AMLA) for direct supervision starting in 2028.

Comparative Enforcement Landscape: UK vs. France

The enforcement strategies of the UK and France are often compared via annual fine totals, yet this approach overlooks legal and procedural nuances.

The United Kingdom

The UK's model is distributed across multiple bodies, including the Financial Conduct Authority (FCA), HM Revenue and Customs (HMRC), and the Gambling Commission.

- **2022 Overview:** The FCA imposed £215.8 million in fines across all categories, dominated by the Santander penalty.
- **Diversified Tools:** Enforcement extends beyond fines to include asset-forfeiture orders (e.g., the £2 million recovered from QPay Europe) and regulatory settlements for non-traditional sectors like gambling (e.g., the £17 million Entain settlement).

France

French enforcement involves the Autorité de contrôle prudentiel et de résolution (ACPR) for financial institutions and the French Anti-Corruption Agency (AFA) for integrity offenses.

- **2022 Overview:** The ACPR's Sanctions Committee issued three primary AML/CFT decisions with combined penalties of €2.35 million.
- **Regulatory Precision:** Unlike the UK, French authorities distinguish sharply between anti-corruption compliance (AFA) and AML/CFT supervision (ACPR). Smaller fines in France often accompany extensive remediation requirements and increased supervisory scrutiny.

Analysis of Systemic Control Failures

Enforcement cases concluded between 2022 and 2025 reveal recurring deficiencies in how institutions manage financial crime risk.

Failure to Reconcile Expected vs. Actual Activity

A primary driver of enforcement actions is the failure to monitor whether actual account activity matches the profile established during onboarding.

- **Case Study (Santander UK):** The bank failed to verify the nature of over 560,000 business accounts. In one instance, a "small translation business" expecting £5,000 in monthly deposits moved millions of pounds within six months.
- **Operational Gap:** Institutions frequently treat "expected activity" as a static field rather than a dynamic component of monitoring logic.

The Detection-to-Disruption Gap

Many institutions identify "red flags" but fail to take timely action. This creates a gap between the detection of an alert and the disruption of illicit activity.

- **Ineffective Escalation:** Alerts are often closed without investigation, or account-exit recommendations remain in queues due to unclear ownership between compliance and relationship management.
- **Governance Failures:** Regulators increasingly view unresolved backlogs as governance failures rather than mere operational delays.

Data Quality and Technical Configuration

The effectiveness of AML programs is fundamentally limited by the quality of the data entering monitoring systems.

- **Case Study (Metro Bank):** A £16.7 million penalty was issued after 60 million transactions (totaling £51 billion) went unmonitored due to system configuration errors and data-quality problems.
- **Data Lineage:** Without clear data lineage—tracking how info moves from source systems to monitoring platforms—firms may have false assurance regarding their compliance coverage.

High-Risk Sectors and New Market Entrants

Challenger Banks and Fintechs

Digital banks have faced intense scrutiny as their commercial growth has frequently outpaced their risk controls.

- **Starling Bank (2024):** Fined ~£29 million for weaknesses in sanctions screening and breaching restrictions on high-risk accounts.
- **Monzo (2025):** Received a £21.1 million penalty for inadequate systems and repeated breaches of account-opening restrictions.
- **Theme:** The assumption that "speed" and "customer experience" justify simplified customer due diligence (CDD) has been rejected by regulators.

Correspondent Banking and MSBs

These sectors remain high-priority due to their inherent exposure to unverified third parties and high-risk jurisdictions.

- **Ghana International Bank:** Fined £5.8 million for failing to perform or evidence Enhanced Due Diligence (EDD) on overseas banking relationships.
- **W-HA (Orange Money France):** Fined €700,000 for relying on transaction limits rather than behavioral analysis, leading to suspicious transaction reporting failures.

Notable Enforcement Penalties (2022–2025)

Institution, Jurisdiction, Penalty Amount, Primary Failure Identified

Santander UK, UK, £107.8 Million, Persistent weaknesses in business-banking AML controls.

Nationwide Building Society, UK, £44.1 Million, "Weaknesses in CDD, risk assessment, and monitoring."

Barclays Entities, UK, £42 Million, Financial-crime risk-management failings.

Starling Bank, UK, ~£29 Million, Sanctions screening failures; high-risk account breaches.

Monzo, UK, £21.1 Million, Inadequate systems and repeated restriction breaches.

Entain, UK, £17 Million, AML and social-responsibility failures (Gambling).

Metro Bank, UK, £16.7 Million, Data quality and transaction monitoring configuration.

Ghana International Bank, UK, £5.8 Million, Correspondent banking control weaknesses.

Crédit Agricole (Languedoc), France, €1.5 Million, Incomplete monitoring scenarios; missed unusual activity.

Treezor, France, €1 Million, Deficiencies in risk classification and controls.

W-HA, France, "€700,000", Inadequate behavioral analysis; reporting failures.

Future Regulatory Trajectory

The landscape is moving toward structural change and supervisory consolidation.

- **UK Centralization:** The UK government has shifted AML supervisory responsibility for legal, accountancy, and trust providers to the FCA to reduce fragmentation and improve consistency.
- **European Union (AMLA):** The new Anti-Money Laundering Authority began operations in 2025. It is expected to select 40 high-risk cross-border financial institutions for direct

supervision by 2028, signaling a move toward a common European framework for enforcement and risk assessment.

Conclusion: Building a Resilient Control Stack

Regulatory findings suggest that a robust AML program must move beyond "design" to "effectiveness." Financial crime leaders are encouraged to treat penalties as signals for preventive enhancement rather than isolated incidents. **Components of a resilient control stack include:**

1. **Enterprise-wide Risk Assessment:** Connected to actual customers, products, and channels.
2. **Dynamic CDD:** Establishing business purpose and source of funds rather than just collecting ID.
3. **Rigorous Data Governance:** Tracking data lineage and monitoring "rejected" or "unprocessed" transactions.
4. **Behavioral Analytics:** Moving beyond simple scenarios to identify complex unusual patterns.
5. **Root-Cause Analysis:** Determining why a failure survived internal audits and board oversight before it reached a regulator.