

Analysis of US AML Enforcement in 2022: Control Failures and Regulatory Trends

Executive Summary

The United States anti-money laundering (AML) enforcement landscape in 2022 was characterized by a moderate increase in the number of actions despite a slight decline in aggregate financial penalties. While the primary federal banking regulators recorded 19 actions with approximately \$384 million in penalties, these figures understate the actual enforcement risk. The year served as a critical transition period where traditional banking vulnerabilities—specifically inadequate transaction monitoring and failure to remediate repeat supervisory findings—intersected with heightening scrutiny of the digital asset sector. The central takeaway for financial leaders is that enforcement risk is primarily driven by a "scaling gap": institutions expanding their customer bases, transaction volumes, and product offerings without a corresponding investment in compliance infrastructure. The record-breaking penalties seen in 2023 and 2024 (such as those involving Binance and TD Bank) were preceded by the structural failures identified in 2022.

The Landscape of US Enforcement Activity

The 2022 enforcement record reflects a fragmented system where multiple authorities exercise overlapping jurisdictions. This complexity makes annual comparisons based solely on monetary totals misleading.

Comparative Statistics (Federal Banking Regulators)

An industry analysis of actions by the OCC, FinCEN, FDIC, and the Federal Reserve highlights the following trends:

Metric	2020	2021	2022	2023	2024
Total AML-Related Actions	40	11	19	25	35
Combined Penalties	N/A	\$403 Million	~\$384 Million	\$450 Million	\$520 Million

Regulatory Fragmentation and "Double Counting"

Total enforcement impact is difficult to quantify because:

- **Overlapping Resolutions:** A single institution may face simultaneous actions from the Department of Justice (DoJ), FinCEN, and state authorities like the New York State Department of Financial Services (NYDFS).
- **Crediting Mechanisms:** Authorities often credit payments made to one regulator against the penalty of another to prevent simple additive totals.
- **Non-Monetary Remedies:** Cease-and-desist orders, activity restrictions, and the imposition of independent monitors create significant business impacts that are not captured in penalty statistics.

Core Control Failures and Root Causes

The enforcement actions of 2022 revealed recurring weaknesses that indicate structural rather than isolated system defects.

1. Compliance Failing to Scale with Growth

A primary driver of enforcement was the failure of compliance programs to keep pace with business expansion. Institutions increased revenue and customer volume while leaving staffing and monitoring systems static.

- **Example:** USAA Federal Savings Bank admitted to willful failures in its AML program between 2016 and 2021, where the compliance program failed to scale with the bank's rapid growth.

2. Governance and Repeat Findings

Regulators increasingly view the failure to correct previously identified deficiencies as a governance failure. Recurring findings suggest that senior management is either unaware of the exposure or has failed to allocate the necessary resources to resolve it.

- **Example:** The National Bank of Pakistan faced coordinated action after significant weaknesses persisted across multiple review cycles despite earlier supervisory warnings.

3. Transaction Monitoring and SAR Deficiencies

Transaction monitoring remains a critical vulnerability. Failures often stem from:

- **Static Baselines:** Failing to reassess "expected activity" when customer behavior or transaction destinations change materially.
- **Inadequate Coverage:** Significant portions of transaction volume going unmonitored.
- **Reporting Delays:** Failure to file accurate and timely Suspicious Activity Reports (SARs).

Sector-Specific Analysis

Digital Assets and Cryptocurrency

In 2022, regulators signaled that digital asset firms are held to the same core AML expectations as traditional banks.

- **Bittrex:** Fined \$29.28 million (coordinated with OFAC) for relying on as few as two employees to review 20,000 daily transactions and failing to file any SARs for over three years.
- **Robinhood Crypto:** Fined \$30 million by NYDFS for AML and cybersecurity failures, specifically citing inadequate staffing and manual monitoring systems that were not upgraded during business expansion.
- **Anchorage Digital Bank:** Received a non-monetary consent order for failing to satisfy BSA/AML requirements in its operating agreement.

Foreign Banking Organizations

Foreign branches remain a priority due to their role in providing access to US dollar clearing. The parent organizations are expected to ensure that global governance and data systems support the specific risks of their US operations.

Major 2022 Penalties and Forfeitures

Institution, Lead Authority, Penalty/Forfeiture, Primary Failure

Danske Bank, DoJ/SEC, ~\$2.059 Billion, Conspiracy to commit bank fraud; misleading US banks about high-risk customers.

USAA, FinCEN/OCC, \$140 Million, Failure to maintain minimum BSA requirements; compliance scaling failures.

National Bank of Pakistan, Fed/NYDFS, \$55.4 Million, Ineffective oversight; failure to remediate repeat findings.

Robinhood Crypto, NYDFS, \$30 Million, Inadequate AML staffing and manual monitoring during expansion.

Bittrex, FinCEN/OFAC, \$29.28 Million, Lack of SAR filings; processing transactions from sanctioned jurisdictions.

MoneyGram, NYDFS, \$8.25 Million, Failure to investigate material changes in agent/customer behavior.

Intersection of AML and Sanctions

Sanctions enforcement, though distinct, often shares root causes with AML failures, such as weak customer identification and poor location controls. In 2022, OFAC concluded 16 civil matters with \$42.7 million in penalties. The Bittrex case specifically highlighted how inadequate transaction monitoring leads to both BSA violations and the processing of funds for sanctioned jurisdictions.

Strategic Recommendations for Remediation

An effective remediation program must address the factual root cause of failures rather than just the language of a regulatory order.

The "Resilient Control Stack"

1. **Risk Assessment:** An enterprise-wide assessment connected to actual products, geographies, and channels.
2. **Scalable CDD:** Customer Due Diligence that identifies material changes in ownership or expected activity.
3. **Complete Data Coverage:** Ensuring all relevant transaction types enter monitoring and screening systems.
4. **Risk-Sensitive Surveillance:** Combining behavioral analysis with documented threshold governance.
5. **Effective Case Management:** Ensuring alerts lead to timely, defensible decisions.
6. **Integrated Intelligence:** Shared information between AML and sanctions functions.
7. **Independent Testing:** Demonstrating that controls work against real-world customer data.

Board and Management Oversight

Financial leaders must treat the following as indicators of structural risk rather than routine operational issues:

- Unresolved or repeat supervisory findings.
- Overdue remediation action plans.
- Persistent alert backlogs or overdue customer reviews.
- Commercial objectives that consistently override risk-based compliance decisions.