SymphonyAI

WHITE PAPER

SITUATION REPORT

# Multi-Agency Enforcement Action against Global FI

## Sector-Wide Risk Implications & Strategic Response

# Executive Summary

### Key judgment

A large, global financial institution with an existing cease-and-desist order and an AML program on paper still allowed known monitoring, escalation, and sanctions-screening gaps to persist. On October 13, 2026, FinCEN, the OCC, and OFAC announced coordinated penalties totaling more than $1.21 billion. The message for the sector is that enforcement exposure builds when remediation stalls and when detection logic is never tested against the risks the institution actually faces.

# Situation

On October 13, 2026, the Financial Crimes Enforcement Network (FinCEN) assessed a **$1.2 billion** civil money penalty against a large, global financial institution (FI), and the FI admitted it willfully violated the Bank Secrecy Act in the civil enforcement sense. The Office of the Comptroller of the Currency (OCC) imposed a **$750 million** civil money penalty, the largest the OCC has assessed against a bank. OFAC announced an **$11.66 million** settlement for 475 apparent sanctions violations. Treasury describes the FinCEN penalty as the third-largest in its history and the bank as the second-largest in the United States.

**FinCEN**

$1.2B

CIVIL MONEY PENALTY

Bank admitted willful BSA violations

**OCC**

$750M

CIVIL MONEY PENALTY

OCC's largest-ever penalty on a bank

**OCC**

$11.66M

SETTLEMENT

475 apparent sanctions violations

## Enforcement Summary

| Agency | Penalty | Basis | Conduct Period |
|---|---|---|---|
| **FinCEN** | $1.2 billion | Bank Secrecy Act: AML program, correspondent due diligence, SAR filing (willful, civil sense) | Jan 1, 2018 – Jul 1, 2025 |
| **OCC** | $750 million (record for OCC) | 12 CFR 21.21 and 21.11; breach of Dec. 23, 2024 cease-and-desist order | Monitoring gaps through the 2024 order and after |
| **OFAC** | $11,662,930 | Sanctions programs: Russia, Belarus, Iran, Burma, Somalia, narcotics, global terrorism | Sep 18, 2021 – Apr 24, 2025 |

Figure note: Treasury states a combined total of "more than $1.21 billion," but the three headline amounts sum to about $1.96 billion. The total reconciles only if the $750 million OCC penalty is credited against the FinCEN penalty, as secondary reporting states. The FinCEN consent order's penalty section could not be verified for this report and should be checked against the primary document.

### Critical finding

Over $5 billion in suspicious transactions were not reported on time, more than $1 billion of it linked to priority illicit finance risks. A 2024 lookback found nearly 8,900 SARs were never filed, covering nearly $4 billion in activity.

**$5B+**
in suspicious transactions reported late

**$1B+**
tied to priority illicit finance risks

**~8,900**
SARs never filed

**~$4B**
in missed activity

2024 LOOKBACK

# Why this matters

The record points to design and governance failures, not a shortage of data. Monitoring relied heavily on outside triggers: law enforcement requests accounted for more than one-third of investigations for several years. The 20-point alert threshold for investigation was set by stakeholder judgment and kept until December 2023 and allowed thousands of SARs to go unreported. The OCC found the monitoring system failed to properly cover trillions of dollars in transactions, and that management knew for years that potentially suspicious activity was not reaching investigators. **When the control architecture is built on thresholds and referrals that were never tested against real typologies, the gaps are structural and grow with volume.**

SECTION 1

# Situation assessment

## The Regulatory Action

The three agencies identified deficiencies across the compliance infrastructure:

- **Transaction monitoring** that did not cover trillions of dollars in activity and did not reliably escalate suspicious patterns
- **Trade-based money laundering (TBML)** gaps, including potential TBML transactions still processed after the 2024 order, with about $600 million in transactions showing TBML signs (salvaged vehicles, about one-third with a southwest border nexus)
- **Correspondent and foreign-affiliate due diligence** that was thin, covering more than 250 non-bank financial institutions across 12 examined foreign branches and affiliates
- **Sanctions alert handling** that downgraded exact name-and-date-of-birth matches to low or medium priority, and watchlist updates that lagged designations
- **Staffing, training, and audit** gaps: the BSA officer and staff lacked sufficient skills, and the BSA audit function missed long-standing concerns that examiners later found
- **Remediation failure:** more than a year after the December 2024 cease-and-desist order, many required steps were incomplete

## Key Implications

The core question for the sector is whether governance and risk management can recognize, escalate, investigate, and report suspicious activity **consistently over time.** Individual alert volumes and policy documents do not answer that question. Under FinCEN's remediation terms, the FI must retain independent reviewers whom FinCEN can veto. Those reviews cover monitoring, customer and correspondent due diligence, SAR lookback, and data governance, with a final lookback report due no later than December 2028. **Peers should expect examiners to test the same questions at their own institutions.**

SECTION 2

# Sector-wide assessments

## Assessment 1: Detection Logic Must Reflect Risk, Not Inherited Thresholds

**Priority: High**

**Finding:** Monitoring depended on external referrals, and the alert threshold was set by stakeholder judgment and left unchanged until December 2023. Coverage did not extend to the trillions of dollars in activity the FI processed.

**Implication:** Thresholds that are never validated against typologies create blind spots that scale with volume. Referral-dependent detection means the institution learns about its own risk from law enforcement, not from its controls.

Institutional Self-Assessment: When did you last test whether your alert thresholds and monitoring scenarios cover your highest-risk typologies, including TBML, and who approved the current settings?

## Assessment 2: Enforcement Remediation Must Be Demonstrable

**Priority: High**

**Finding:** The FI was under a December 2024 cease-and-desist order. More than a year later, the OCC found required steps were incomplete, escalation failures known to management for years had not been fixed, and the TBML gap persisted. Comptroller Jonathan V. Gould said the program **"continues to reflect widespread breakdowns in internal controls."**

**Implication:** An order that is open for a long time without verified milestones reads to regulators as a deficiency still in progress. Enforcement escalates when stated commitments are not matched by evidence.

Institutional Self-Assessment: For every open regulatory commitment, can you name the accountable owner, the milestone dates, and the evidence that shows the work is complete?

## Assessment 3: Independent Testing and Third-Party Reliance Do Not Transfer Accountability

**Priority: High**

**Finding:** FinCEN found the FI had outsourced a substantial part of its detection and reporting duties to third parties, and that its testing function failed to detect and describe problems with the primary transaction monitoring control. The OCC found the BSA audit function missed long-standing concerns.

**Implication:** Outsourcing and audit coverage do not reduce the institution's own obligation. If independent testing does not find a failure that examiners later find, the assurance function is not providing the protection it appears to provide.

Institutional Self-Assessment: Would your independent testing have caught a failure in your primary monitoring control, and how is the work of your third parties tested by people outside the function that relies on them?

## Assessment 4: Sanctions Screening Depends on Alert Priority and Watchlist Timeliness

**Priority: High**

**Finding:** OFAC identified 475 apparent violations totaling about $14.8 million. Of these, 403 transactions worth $14.34 million were routed through 35 blocked banks, mostly under Russia sanctions. Exact matches to designated persons were given low or medium priority, watchlist updates were delayed, and an automatic alert suppression rule contributed to the failures. Only 62 of the 475 violations were voluntarily self-disclosed. OFAC applied no reduction to the base penalty and cited prior cautionary letters on similar conduct as an aggravating factor.

**Implication:** Small transaction values do not limit penalty exposure when prior warnings exist and the failures are systemic. Alert logic that deprioritizes exact matches is a control design defect, not a tuning decision.

Institutional Self-Assessment: Can you demonstrate that an exact match to a designated person always routes to the highest priority, and how many hours pass between a designation update and live screening?

# Threat exposure matrix

The following matrix identifies exposure areas where regulated institutions are particularly vulnerable. These are self-assessment questions for institutional leadership.

| Exposure Area | Risk | Self-Assessment Question |
|---|---|---|
| **Alert Design & Typology Coverage** | Thresholds set by judgment and never validated; referral-dependent detection | Are your monitoring thresholds tested against known typologies such as TBML and cross-border risk? |
| **Enforcement Remediation** | Required steps incomplete long after an order is issued | Can you show evidence that each regulatory commitment is complete on schedule? |
| **Sanctions Screening Timeliness** | Watchlist updates lag designations; exact matches deprioritized | Do exact matches to designated persons always route to the highest priority, and how fast does a designation update go live? |
| **Correspondent & Third-Party Reliance** | Thin due diligence on non-bank correspondents; detection outsourced without oversight | Can you show the due diligence and ongoing oversight behind every correspondent and third party you rely on? |
| **Independent Testing & Audit** | Audit and testing miss failures that examiners later find | Would your independent testing have detected the monitoring failure described in this action? |

# Bottom line & strategic outlook

**The strategic question for regulated financial institutions is no longer simply "Do we have a risk-based approach?" It is:**

1. Does that approach reflect our actual business activities, typologies, and material exposures?
2. Does it drive operational decisions about controls, monitoring, staffing, and resources?
3. Do we have evidence that material risks and regulatory commitments are being effectively managed, not just documented?

**This action shows that a large institution can have a documented AML and sanctions framework, an open enforcement order, and a formal audit function, and still fail to convert known gaps into fixed controls.**

## Strategic Outlook

Next 30–60 days

### Immediate

Test alert thresholds and referral dependencies against the TBML, correspondent, and sanctions typologies cited in this action. Confirm that exact matches to designated persons cannot be deprioritized, and measure the time from designation update to live screening.

Next 60-180 days

### Near-term

Build a tracker for every open regulatory commitment with named owners, milestones, and evidence. Scope a lookback on high-risk correspondent and third-party populations, prioritizing where your due diligence is thinnest.

Next 6-12 days

### Medium-term

Integrate card, payment, correspondent, and sanctions data so related activity is visible in one view. Re-scope independent testing to focus on the primary monitoring controls.

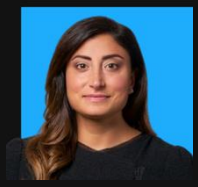
12+ months

### Strategic

Operate an intelligence-led risk model in which controls/thresholds are driven by current threat typologies on a consistent cycle—optimally continuous—and remediation is proven through evidence.

**The regulated sector should assume similar vulnerabilities exist in its own institutions and remediate them systematically.**

## About the Author



**Elizabeth Callan** is a recognized leader and innovator in the fight against money laundering and financial crime with over 25 years of experience across intelligence, law enforcement, and the private sector.

At SymphonyAI, she is at the forefront of redefining the future of financial crime compliance and risk management. She drives strategy and innovation, developing groundbreaking AI-led, intelligence-driven solutions that are transforming how global institutions detect, disrupt, and prevent money laundering, sanctions evasion, and other sophisticated financial crimes. Her work is helping shift the industry approach from reactive, technical compliance to proactive, risk-aligned, and highly effective risk management.

Prior to SymphonyAI, Elizabeth served in the U.S. intelligence and law enforcement communities. As a Senior Intelligence Analyst at the U.S. Department of the Treasury, she shaped high-impact U.S. policy and enforcement actions — including Section 311 designations — while directly advising senior officials at OFAC and FinCEN on critical threats and national security strategies. She also served as Intelligence Liaison and Senior Advisor to the DEA's Special Operations Division, where she led complex, large-scale money laundering investigations, enhanced intelligence collection efforts, trained law enforcement agents and analysts, and forged strong international partnerships.

In the private sector, Elizabeth has held leadership roles in financial institutions and consulting firms, where she built and managed investigations teams, designed robust AML and sanctions programs, and developed risk management strategies for complex products and services.

A recognized subject matter expert, Elizabeth teaches AML and sanctions courses at the university level. She holds a master's degree in economics and the prestigious ACAMS Advanced Certification in Financial Crimes Investigations (CAMS-FCI).

**About SymphonyAI**

SymphonyAI, is building the leading enterprise AI SaaS company for digital transformation across the most critical and resilient growth verticals, including retail, consumer packaged goods, finance, manufacturing, media, and IT/enterprise service management. SymphonyAI verticals have 2000 leading enterprises as clients globally. Since its founding in 2017, SymphonyAI has grown rapidly to 3,000 talented leaders, data scientists, and other professionals. SymphonyAI is an SAI Group company, backed by a $1 billion commitment from Dr. Romesh Wadhwani, a successful entrepreneur and philanthropist.

SymphonyAI provides AI-focused SaaS solutions developed from the ground up for fighting financial crime. An end-to-end offering compiled from more than 25 years of knowledge in tackling money laundering and fraud, our award-winning product ecosystem comprises an innovative and modern approach to financial crime investigation using world-leading predictive and gen AI. From KYC/CDD and transaction monitoring through to payments fraud, entity resolution, and sanctions, PEP, and adverse media screening, SymphonyAI is a trusted name in finance technology with more than a third of the world's top 100 banks enjoying the power, efficiency, effectiveness and productivity that our solutions provide.

Get in touch to discuss how your organization can build a more effective, scalable, and continuously aligned financial crime program across insurance and investment advisory operations using AI-enabled screening, monitoring, network analytics, and intelligent automation.

Email us directly at connect.fs@symphonyai.com
Visit www.symphonyai.com