SymphonyAI

WHITE PAPER

SITUATION REPORT

U.S. Enforcement Action against Major Card Issuer

Sector-Wide Risk Implications & Strategic Response

Executive Summary

Key judgment

An institution can have a formal AML compliance framework and still fail to align risk assessment, controls, resources, and monitoring capabilities with actual business risk. The U.S. enforcement action against a large card issuer on October 8, 2026 is a diagnostic case for the entire regulated financial sector.

Situation

October 8, 2026: The Office of the Comptroller of the Currency (OCC) announced a $350 million civil money penalty and cease-and-desist order against the banking entity of a major card issuer. The Federal Reserve issued a coordinated cease-and-desist action addressing enterprise-wide financial-crime deficiencies.

Critical finding

Approximately $13 billion in suspected trade-based money laundering activity went undetected and underreported over 11 years (June 2014–May 2025) because the bank's risk assessment focused on narrow deposit products rather than its dominant credit and charge card business.

~$13B

undetected and underreported

11 years

June 2014 – May 2025

trade-based money laundering activity went undetected and underreported

Why this matters

This is not a documentation deficiency or an isolated detection failure. It is a foundational risk-management failure: the risk assessment was misaligned with actual business activities. Because the risk assessment is the foundation for every downstream compliance decision—control design, monitoring scenarios, staffing allocation, investigative priorities, and resource deployment—the entire control architecture was built on an incomplete, inaccurate picture of risk.

SECTION 1

Situation assessment

The Regulatory Action

OCC findings identified deficiencies across the compliance infrastructure:

- Risk assessment inadequately tailored to actual business mix
- Weaknesses in customer identification and due diligence
- Systemic breakdowns in suspicious activity monitoring and reporting
- Inadequate resources, expertise, and training
- Gaps in internal controls and weak independent testing

Key Implications

The critical issue is not whether individual alerts were generated. The core question is whether the institution's governance and risk-management processes could recognize, escalate, investigate, and report suspicious activity **consistently over time.**

Financial crime control systems must connect related activity across customers, channels, accounts, and counterparties into coherent risk patterns. When those relationships are assessed in separate systems or silos, individual activities appear less significant than the combined pattern.

SECTION 2

Sector-wide assessments

Assessment 1: Business-Model Alignment is Foundational Control

Priority: High

Finding: Subject of the action had a risk assessment that emphasized its relatively narrow deposit products while insufficiently weighting credit and charge card products, which constitute the subject's primary business lines and generate the majority of transactions.

Implication: A risk assessment can be comprehensive on paper and still materially misrepresent the business. This creates a false sense of control.

Institutional Self-Assessment: Does your institution's risk assessment reflect actual business activity and transaction volumes, or does it overweight inherited product categories?

Assessment 2: Risk Must Translate into Operational Action

Priority: High

Finding: Although the subject of the action had a documented risk assessment, the assessment did not drive proportionate allocation of investigative resources, monitoring coverage design, staffing decisions, or investigative capacity.

Implication: The risk-based approach is only operationally meaningful when assessment results drive control selection, monitoring coverage, investigation priorities, and resource allocation.

Institutional Self-Assessment: Can you trace a material risk through to specific controls, accountable owners, testing procedures, and outcomes?

Assessment 3: Data Fragmentation Obscures Related Activity

Priority: Material

Financial crime often spans customers, merchants, accounts, card transactions, repayments, counterparties, and external entities. When those relationships are assessed in separate systems or operational silos, individual activities appear less significant than the combined pattern.

Critical Example: Iranian shadow banking sanctions evasion uses beneficial ownership changes (KYC signal) + screening matches on Iran-adjacent facilitator banks (screening signal) + transaction routing patterns through high-risk free trade zones(transaction monitoring signal) + systematic commodity over-invoicing. When evaluated separately, each signal appears routine. In combination, the pattern is unmistakable.

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
Product & Business Change	Risk assessments not updated when products or business mix changes	Do your risk assessments keep pace with new products and business lines?
Cross-Channel Activity	Inability to connect activity across cards, accounts, payments	Can you connect related activity across all systems and channels?
Trade-Based Money Laundering (TBML) Risk	Monitoring designed around isolated transactions	Are your controls designed around known TBML typologies?
Governance & Assurance	Management cannot demonstrate controls are effective in practice	Can you show evidence that controls work in practice?
Detection & Reporting	Suspicious activity cannot move reliably from detection to report	Can you demonstrate a chain of custody from alert to regulatory decision?

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 accurately reflect our actual business activities and material exposures?
2. Does it drive operational decisions about controls, monitoring, staffing, and resources?
3. Do we have evidence that material risks are being effectively managed, not just that policies exist?

This enforcement action demonstrates that an institution can answer "yes" to all three conventionally, and still miss $13 billion in suspected criminal activity over 11 years.

Strategic Outlook

Next 30–60 days

Immediate

Validate whether risk assessments reflect actual business activities. Identify largest gaps between documented risk and operational reality.

Next 60-180 days

Near-term

Complete end-to-end traces of material risks. Establish baseline performance metrics. Begin governance restructuring.

Next 6-12 days

Medium-term

Deploy integrated data layer. Introduce analytics and AI into governed workflows. Demonstrate measurable improvements in detection quality.

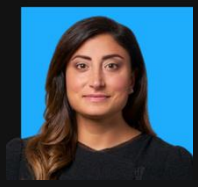
12+ months

Strategic

Operate an intelligence-led risk model. Demonstrate material risks are effectively managed 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