Bank's Penalties Highlight Key AML Compliance Expectations

By **Laurel Loomis Rimon, Benjamin Seelig and Gina Shabana** (October 26, 2023)

Laurel Loomis Rimon

Benjamin Seelig

Gina Shabana

Shinhan Bank America, a New York-based subsidiary of a Korean bank, faced coordinated enforcement actions on Sept. 29 from the Financial Crimes Enforcement Network, the Federal Deposit Insurance Corporation and the New York Department of Financial Services.

These concurrent actions resulted in a total of $25 million in civil penalties for failing to develop and implement an effective anti-money laundering program in accordance with the Bank Secrecy Act and New York law, based on ongoing, unremedied compliance failures the agencies allege were apparent dating back to at least 2015.

The consent orders provide valuable insight into current areas of regulatory oversight and focus, applicable not just to traditional financial institutions, but to fintechs and virtual asset companies as well.

In fact, although it took more than six years of alleged failures to meet the AML requirements outlined in formal agreements between Shinhan and regulators before the bank faced civil penalties, we know that fintechs and virtual asset entities are likely to face a much shorter grace period from federal and state regulatory agencies who feel the fintech risk environment demands faster action.

Key Takeaways

There are several key takeaways financial institutions can glean from Shinhan's AML noncompliance mistakes:

- This coordinated action between FinCEN, the FDIC and the NYDFS reflects increased coordination and cooperation among federal and state financial regulators.

- Part 504.3 of the New York Codes, Rules and Regulations' certification requirement sets up a complicated risk analysis for certifying annual transaction monitoring compliance.[1]

- Compliance governance, change management and appropriate staffing are key elements to a defensible AML compliance program.

- Regulators expect AML compliance data systems to provide a 360-degree view of customers, meaning integrated systems that flag shared customer attributes and are properly tuned for alerting.

Not surprisingly, recurring AML deficiencies and repeated failures to remediate create a high risk of penalty action as regulators with overlapping jurisdiction share information among themselves.

An enforcement action of one regulator can generate a related enforcement action by another.

Here, Shinhan was the subject of two earlier FDIC consent orders in 2017 and 2022, along with an NYDFS memorandum of understanding in 2020, all of which detailed the compliance shortcomings that became the subject of the most recent actions taken in a coordinated fashion by FinCEN, the FDIC and the NYDFS.

NYDFS Certification Requirements

Under Part 504.3, companies must attest that their transaction monitoring programs meet New York's requirements. Part 500.17(b) of the New York Codes, Rules and Regulations contains a certification requirement related to a firm's cybersecurity program.

New York's transaction monitoring regulations are both more specific and expansive than related federal requirements, and require regular risk-based internal audits, improvements, and data management and integration.

Part 504 certifications must also be authorized by a company's board of directors or senior officer.

Here, the NYDFS points to Shinhan's inability to complete the action plans developed as part of the 2020 MOU as evidence that the bank certified Part 504 compliance even though it still had several outstanding compliance gaps.

This shouldn't come as a surprise to financial institutions licensed in New York — past consent orders[2] have similarly reflected the department's expectation that annual Part 504 certifications adhere to the proscriptive requirements of Part 504.3.

Compliance Resources and Board Management

Understaffed or underqualified compliance teams are low-hanging fruit for regulators looking to measure the adequacy of an institution's BSA program.

Corporate governance, sufficient oversight, and the involvement of boards of directors and compliance committees are also crucial, especially for New York-regulated entities that have specific corporate governance requirements under Title 3 of the New York Codes, Rules and Regulations, Section 116.2,[3] and Part 200.15[4] for virtual asset BitLicensees.

In these actions, the regulators highlight that Shinhan's AML department was "chronically understaff[ed]," which contributed to a sizable backlog of transaction monitoring alerts and the inability to timely file suspicious activity reports.

The recent FinCEN action also highlights Shinhan's "difficulty ensuring continuity in

leadership, particularly in the BSA compliance officer role," and failure to establish clear lines of communication between employees and the board.

In its consent order, FinCEN calls out Shinhan's board of directors' failure to adequately bring the bank into compliance. Directors and officers can be personally liable for AML violations and, in some situations, may be barred from reimbursement through their organization's directors and officers' liability insurance.

For example, in its 2013 financial institution letter,[5] the FDIC reminded FDIC-supervised banks and savings associations, including community institutions with total assets under $1 billion, that depository institutions and their holding companies are prohibited from purchasing insurance policies that "would indemnify institution-affiliated parties (IAPs) for civil money penalties (CMPs) assessed against them [in an administrative proceeding or civil action commenced by any federal banking agency] ... [e]ven if the IAP agrees to reimburse the depository institution for the cost of such coverage."

AML Data and Systems Management

Shinhan was also faulted for failures related to its compliance with FinCEN's 2018 customer due diligence rule in risk rating of customers during its know-your-customer onboarding process.

Specifically, the bank allegedly collected information from its customers about their anticipated activity, but then failed to use or validate that information, instead relying solely on the customer's early actual transaction activity to establish a risk baseline.

Further, the bank's automated and rigid risk rating calculations used factors not tailored to the bank's cash-intensive customer base, which had a high volume of wire transfers.

FinCEN also flagged Shinhan's failure to identify common elements across customer accounts, e.g., customers acting as signatories or owners of related accounts, that should have triggered transaction monitoring alerts for multiple accounts belonging to the same customer relationship.

FinCEN noted the bank's transaction monitoring tools were unable to holistically analyze related accounts and aggregate transaction activity to identify patterns of potentially suspicious activity.

Because these processes did not adequately address and facilitate investigation of potentially suspicious activity, the bank was unable to file suspicious activity reports within the 90-day timeline stipulated by the BSA.

The Bottom Line

In addition to the risks of continued noncompliance and the unique risk posed by NYDFS' certification requirement, the Shinhan consent orders reveal regulators' expectation that financial institutions utilize the know-your-customer information collected for customers across all related accounts to inform customer and risk profile systems.

Data integration of transaction monitoring, onboarding and other back-end systems should, in an ideal world, allow processes to speak to each other and identify related accounts and suspicious activity patterns across customer populations.

At the same time, regulators assess a financial institution's compliance profile by evaluating the urgency and comprehensiveness of its remediation efforts and the adequacy and investment of its directors and officers in necessary compliance programs.

Laurel Loomis Rimon is a partner and co-chair of the fintech and crypto assets practice at Jenner & Block LLP. She previously served as an assistant U.S. attorney, head of litigation for the U.S. Department of Justice's Asset Forfeiture and Money Laundering Section, and as assistant deputy enforcement director for the Office of Enforcement at the Consumer Financial Protection Bureau.

Benjamin Seelig is an associate at the firm.

Gina Shabana is department counsel at the firm. She previously served as the associate director of data privacy and protection in the Financial Industry Regulatory Authority's Office of General Counsel.

[1] https://govt.westlaw.com/nycrr/Document/If190167b58ac11e6806bc9321b10fb4e?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default)&bhcp=1.

[2] https://www.dfs.ny.gov/system/files/documents/2022/08/ea20220801_robinhood.pdf.

[3] https://govt.westlaw.com/nycrr/Document/I4e749d01cd1711dda432a117e6e0f345?transitionType=Default&contextData=%28sc.Default%29.

[4] https://govt.westlaw.com/nycrr/Document/I85908c8f253711e598dbff5462aa3db3?viewType=FullText&originationContext=documenttoc&transitionType=CategoryPageItem&contextData=(sc.Default).

[5] https://www.fdic.gov/news/financial-institution-letters/2013/fil13047.html.