

GUIDE

Fraud and BSA/AML: what the board should receive, and how the reports should agree

The board's duties for the BSA program and suspicious activity reports, and why fraud, BSA/AML and cyber figures should tell the same story.

Current as of October 13, 2026 · 3 minute read

Fraud, BSA/AML and cybersecurity usually report to the board separately, from different teams, in different months. Yet one event, such as an account takeover, can appear in all three: as a cyber incident, a fraud loss and a suspicious activity report. If the three reports never meet, the board cannot see the pattern.

The board's BSA/AML duties

- Approve the written BSA compliance program, and record it in the minutes. Credit unions: 12 CFR 748.2(b)(1). Banks: 12 CFR 21.21 (OCC), 208.63 (Federal Reserve) and 326.8 (FDIC).
- The program must provide for internal controls, independent testing, a designated person responsible for day-to-day compliance, and training (12 CFR 748.2(c) and the bank equivalents).
- Management must promptly notify the board, or a committee it designates, of suspicious activity reports filed. Credit unions: 12 CFR 748.1(d)(4). Banks: 12 CFR 21.11(h), 208.62(h) and 353.3(f). A director who is a suspect is not told.
- SARs are confidential. No director, officer or employee may disclose a SAR or reveal that one exists (31 CFR 1020.320(e)). Board reporting should use counts and trends, not case details.

A change to watch

In April 2026 FinCEN proposed new AML/CFT program rules, replacing a 2024 proposal, and the banking agencies and NCUA proposed matching changes. The proposals would allow the program to be approved by the board, an equivalent governing body or senior management. None is final, so today the board still approves the program.

How the reports should agree

- Fraud losses for the quarter, by channel or product, beside the board's limit.
- SAR counts and trends, in aggregate, with the share linked to fraud or cyber events.
- Cyber incidents that led to a loss or a SAR, counted the same way in each report.
- A one-line reconciliation when the numbers differ, explaining why.

Why cyber belongs in the conversation

FinCEN's 2016 advisory on cyber-events says a SAR is required when a cyber-event was meant to affect transactions of \$5,000 or more, asks institutions to include cyber indicators such as IP addresses and device identifiers, and urges BSA/AML and cybersecurity teams to work together. The board can ask whether they do.

BoardAlign reads the fraud, BSA/AML and cyber reports side by side and shows where the figures for the same events agree and where they do not.

Sources

12 CFR Part 748 (748.1(d), 748.2). <https://www.ecfr.gov/current/title-12/chapter-VII/subchapter-A/part-748>

12 CFR 21.11 and 21.21 (OCC). <https://www.ecfr.gov/current/title-12/chapter-I/part-21>

12 CFR 208.62 and 208.63 (Federal Reserve). <https://www.ecfr.gov/current/title-12/section-208.62>

12 CFR 326.8 and 353.3 (FDIC). <https://www.law.cornell.edu/cfr/text/12/326.8>

31 CFR 1020.320 (SAR confidentiality). <https://www.ecfr.gov/current/title-31/section-1020.320>

FinCEN proposed AML/CFT program rule (April 10, 2026). <https://www.federalregister.gov/documents/2026/04/10/2026-07033/anti-money-laundering-and-countering-the-financing-of-terrorism-programs>

FinCEN Advisory FIN-2016-A005. <https://www.fincen.gov/resources/advisories/fincen-advisory-fin-2016-a005>

General information for directors, not legal advice. Current as of October 13, 2026. Rules change: check the cited source before relying on it.