LESSONS FROM 2024 ANTI-MONEY LAUNDERING ENFORCEMENT ACTIONS

Date: 12 February 2025

US Policy and Regulatory Alert

By: Jeremy M. McLaughlin, John ReVeal

In 2024, FinCEN and the federal bank regulators announced more than three dozen enforcement actions against banks and individuals arising from alleged Bank Secrecy Act (BSA), anti-money laundering (AML), and countering the financing of terrorism (CFT) compliance failures. One of these enforcement actions resulted in record-breaking civil and criminal monetary penalties.

In this article, we summarize certain key compliance failures and issues indicated by these enforcement actions against banks. Rather than focusing on any specific institutions, we focus on broader industry issues. The aim of this article is to provide guidance to BSA officers and the boards of directors and senior management of banks as they consider ways in which their institution's BSA/AML compliance program might need improvement.[1]

THE FIVE PILLARS

BSA/AML enforcement actions typically cite failures with respect to one or more of the five “pillars” of an effective BSA/AML program: (1) a system of internal controls to assure ongoing compliance; (2) independent testing for compliance; (3) designation of an individual or individuals responsible for coordinating and monitoring day-to-day compliance; (4) training for appropriate personnel; and (5) appropriate risk-based procedures for conducting ongoing customer due diligence (CDD), including, but not limited to, (a) understanding the nature and purpose of customer relationships for the purpose of developing a customer risk profile; and (b) conducting ongoing monitoring to identity and report suspicious transactions and, on a risk basis, maintaining and updating customer information, including customer beneficial owner information. A significant portion of the 2024 enforcement actions cited deficiencies in all of the first four of these pillars, and in many other cases, the bank was required to adopt an improved CDD program.

These are the pillars of an effective BSA/AML compliance program because a failure in any of them is likely to cause a failure in an institution's overall BSA/AML compliance obligations. The whole foundation can collapse when any pillar is weak. Perhaps most important is the failure to file suspicious activity reports (SARs) when required, which in the end is the primary reason for many of the BSA's regulatory requirements.

The following discussion of compliance issues does not track the five pillars in the same order as listed in the applicable regulation, because we believe that results in a more logical flow. For example, a discussion of suspicious activity monitoring systems logically follows after discussing institutional risk assessments and customer due diligence because the activity monitoring systems should take these other requirements into account.

©2005-2026 K&L Gates LLP. All Rights Reserved.

INTERNAL CONTROLS

When an examiner cites an institution for weak internal controls, that generally reflects a determination that the institution has weak policies, procedures, or processes to mitigate and manage money laundering and terrorist financing risks. This can mean anything from a poor reporting structure, unclear assignments of compliance responsibilities, poor risk assessments, failures to update policies and processes in response to regulatory changes or changes in the institution's risk profile, weak suspicious activity monitoring systems, or weak risk rating of customers, among other issues. A bank's system of internal controls, including the level and type, should be commensurate with the bank's size, complexity, and organizational structure. When an institution is experiencing BSA/AML compliance weaknesses, that often reflects weak internal controls. In the summaries below, we note which of the deficiencies reflect an internal control weakness.

BOARD AND MANAGEMENT OVERSIGHT

The Examination Manual states that the board of directors of each bank is responsible for approving the institution's BSA/AML compliance program and overseeing the structure and management of the institution's BSA/AML compliance function. The boards of about half of the banks subject to enforcement actions in 2024 were directed to enhance their oversight of their bank's BSA/AML compliance program. The board also is responsible for setting an appropriate “culture of compliance” with respect to BSA/AML matters, and when an institution is subject to a particularly serious enforcement action, the directors and senior managers may be fined individually.

Oversight by the board requires that the board receive regular reports from compliance staff on the institution's BSA/AML program, which reports are part of the institution's internal controls. This would include, among other things, reports from the BSA officer as to SAR filings, reports on any negative findings in compliance audits, reports on remediation steps to address negative audit results, reports on any changes to the institution's risk assessments, and reports on any deficiencies in the resources that are allocated to the compliance function.

BSA OFFICER DEFICIENCIES

The BSA officer is central to the effective function of a BSA/AML compliance program. A few of the enforcement actions in 2024 noted that the bank had designated an ineffective BSA officer or one with no prior banking or BSA officer experience.

Other enforcement actions raised these concerns:

- BSA/AML staffing that is not proportionate to the bank's size, risk profile, and ongoing compliance concerns.
- BSA officer without appropriate authority or independence. For example, one institution was criticized for having a BSA officer who did not have unilateral authority to file SARs, such as where a senior manager or a committee consisting of business managers made the ultimate decisions. This authority and independence is important to a sound compliance system, in part to avoid any conflicts of interest.
- AML monitoring and compliance staff reporting through business line management rather than directly to the BSA officer, thereby weakening the BSA officer's authority and independence.

©2005-2026 K&L Gates LLP. All Rights Reserved.

It also is important that all AML compliance staff, even if not designated as an “AML officer,” have appropriate experience in BSA and AML matters.

TRAINING

Banks must provide BSA/AML training to appropriate personnel, including all persons whose duties require knowledge or involve some aspect of BSA/AML compliance. This training should be tailored to the specific functions and positions of each individual within the institution. For example, the board of directors and certain staff may receive more general training than that provided to compliance staff and those individuals processing transactions or new accounts. Training generally should address higher-risk customers and activities, depending on the role of the individual to receive such training. In addition, targeted training may be necessary for specific money laundering, CFT, and other illicit financial activity risks for certain business lines or operational units.

Many of the banks entering into consent orders in 2024 were required to develop and implement a new training program. Banks were cited in 2024 for failure to tailor training for frontline retail branch personnel, to train staff on the “AML typologies and risks” associated with the bank's products and services, and to train on the specialized red flags for specific business lines or higher-risk activities. At least one bank was criticized for inadequate training on the completion and filing of currency transaction reports (CTRs), resulting in the filing of incomplete or inaccurate CTRs. A robust training program for all aspects of BSA/AML compliance is clearly required for every bank.

INADEQUATE COMPLIANCE RESOURCES

A common finding when an institution is subject to an enforcement action is that the institution did not dedicate sufficient financial and personnel resources to BSA/AML compliance. Multiple institutions were cited in 2024 for this failure, and in at least one case for the failure to invest in improvements to address compliance gaps when those investments were deemed to be too costly. At least one institution was accused of maintaining a compensation system that appeared to provide a disincentive for the BSA officer to incur costs to ensure compliance.

AML staffing also should be proportionate to the bank's size, risk profile, and any ongoing compliance concerns. When these factors change, an increase in staffing and other resources is often called for.

Inadequate staffing and resources can result in failures in numerous areas of BSA/AML compliance. These failures can include having significant backlogs in addressing suspicious activity alerts, an inability to adequately investigate alerts, and backlogs of customers for whom their relationship with the bank should be severed.

INITIAL AND ONGOING RISK ASSESSMENTS

Banks' BSA/AML compliance programs should be risk-based. A well-developed BSA/AML risk assessment assists the bank in identifying its money laundering, CFT, and other illicit financial activity risks and then developing and maintaining appropriate internal controls to address the identified risks. A risk assessment generally involves the identification of specific risk categories (e.g., products, services, customers, and geographic locations) unique to the bank and the bank's analysis of such risks.

©2005-2026 K&L Gates LLP. All Rights Reserved.

A bank should update its risk assessment from time to time, particularly when there are changes in the bank's products, services, customers, or geographic locations, when the bank expands through mergers or acquisitions, and in response to regulatory changes, alerts, or negative compliance findings.

Many of the recent enforcement actions directed the bank to develop, implement, and adhere to a revised and ongoing BSA risk assessment methodology. Those risk assessments were to address the risks outlined above and include an analysis of the volumes and types of transactions and service by geographic location and the numbers of customers that typically pose higher or elevated BSA risk for the institution.

All risk assessments then should be used by the institution to develop and implement appropriate risk-mitigating strategies and internal controls. The results of each risk assessment should be reported to the board and appropriate senior management, and they then should require progress reports from the BSA officer with respect to any steps needed to reduce risks to appropriate levels.

CUSTOMER DUE DILIGENCE, RISK ASSESSMENTS, AND MONITORING

The Examination Manual notes that "[t]he cornerstone of a strong BSA/AML compliance program is the adoption and implementation of risk-based CDD policies, procedures, and processes for all customers…." Conducting ongoing CDD is the fifth pillar of an effective BSA/AML compliance program. Its objective is to enable a bank to understand the nature and purpose of customer relationships, including understanding the types of transactions in which a customer is likely to engage. These processes assist the institution in determining when transactions are suspicious and when a SAR might need to be filed.

CDD should enable the bank to assign risk ratings to each customer, and those risk ratings then should be taken into account when establishing customer transaction monitoring systems, with higher risk customers being subject to more stringent transaction monitoring. Customer risk ratings also should be taken into account in the institution's overall BSA/AML compliance risk assessments.

If a bank determines through ongoing CDD and transaction monitoring that its information on a particular customer has materially changed, that customer information and risk rating should be updated accordingly. In the event a bank discovers that it failed to identify a customer as being a higher risk customer, the bank should revise its risk rating of the customer and consider conducting a transaction review to determine if suspicious activities were not identified.

A large majority of the banks subject to enforcement actions in 2024 were required to develop and implement a new CDD program. The actions often stated that the CDD program must ensure appropriate collection and analysis of customer information when opening new accounts, when renewing or modifying existing accounts, and when the bank obtains "event-driven information" indicating that it should obtain updated information to better understand the nature and purpose of its customer relationships and generate and maintain an accurate customer risk profile.

SUSPICIOUS ACTIVITY MONITORING SYSTEMS AND PROCESSES

Having an effective suspicious activity monitoring system and reporting system is a critical internal control and essential to ensuring that a bank has an adequate and effective BSA/AML compliance program. Without such, an institution is more likely to miss suspicious activities and file appropriate SARs.

©2005-2026 K&L Gates LLP. All Rights Reserved.

Per the Examination Manual, the sophistication of a monitoring system should be dictated by the bank's risk profile, with particular emphasis on the composition of higher-risk products, services, customers, entities, and geographies. It likely would be inappropriate, however, to use a monitoring system that wholly disregards domestic and supposedly lower-risk transactions, and at least one institution was criticized for that in 2024.

The five key components to an effective monitoring and reporting system are:

- Identification or alert of unusual activity, which may include employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output.
- Managing alerts.
- SAR decision making.
- SAR completion and filing.
- Monitoring and SAR filing on continuing suspicious activity.

A transaction monitoring system may have manual elements. These systems may target specific types of transactions, such as large cash transactions or transactions from foreign geographies, with a manual review of reports generated by the bank's systems. The type and frequency of reviews and resulting reports used should be commensurate with the bank's BSA/AML risk profile and appropriately cover its higher-risk products, services, customers, entities, geographic locations, and methods of delivering its products and services.

Automated monitoring systems also are appropriate for most or all banks. These systems, sometimes called “surveillance monitoring systems,” include rule-based systems that apply transaction parameters, scenarios, and filters. In all cases, however, those parameters, scenarios, and filters should be tailored to the bank's risks, and they should be tested periodically to ensure that they are effective.

We therefore have seen enforcement actions criticizing banks for relying on “off-the-shelf” scenarios provided by its vendor without consideration as to whether those scenarios needed to be tailored to the bank's business. Some enforcement actions also criticized the bank for failure to conduct appropriate testing and gap assessments of their transaction monitoring system.

Finally, we should note that at least one institution was criticized for appearing to have designed at least portions of its monitoring system to focus more on operational burdens and risks rather than BSA/AML compliance.

FAILURES TO FILE SARS; POTENTIAL CONSEQUENCES

Not surprisingly, those institutions that were cited for having weak CDD or transaction monitoring programs also were often cited for failures to identify suspicious transactions and file SARs as warranted. At least 16 banks were ordered in 2024 to conduct reviews of prior transactions to determine if any SAR filing might have been missed, sometimes referred to as a “look back” review.

When a look back is required, the institution generally must hire an independent consultant to conduct a review and provide a written report on the bank's suspicious activity monitoring, investigation, decisioning and reporting, identifying any instances in which the bank failed to file a SAR. The regulator then uses this information to decide

©2005-2026 K&L Gates LLP. All Rights Reserved.

what fines it will impose and whether to increase any prior fines. If the results of the look back are very negative, the regulator might also order an expanded look back, going further back in time.

INDEPENDENT TESTING

Banks are required to conduct independent testing or audits (the Examination Manual uses these terms interchangeably) of the bank's BSA/AML compliance program. The testing can be conducted by the bank's internal audit department or by qualified third parties, but the auditor never should be involved in business operations or BSA-related functions due to the potential for conflicts of interest or lack of independence. The results of all independent testing should be reported directly to the board of directors or a designated committee thereof that is composed primarily or completely of outside directors.

The Examination Manual directs examiners to obtain and review the independent testing reports, including any scope and workpapers. If the examiner finds that the testing was adequate given the bank's risk profile, that can comfort the examiner and might lead to a softer-touch examination. If the examiner concludes that the testing was deficient, the bank can expect a rigorous examination.

Several of the banks subject to enforcement actions in 2024 were found by the examiner to have deficient independent testing. In one instance, the examiner concluded that the testing was insufficient in scope given the institution's risk profile and that it only determined whether controls existed and not if they were in fact being used. In certain other instances when the enforcement action did not specifically criticize prior testing, the bank still was required to perform new independent testing and provide the results to the examiner.

Many other banks were directed to establish a new independent audit program that would address and determine, among other things, the bank's money laundering, terrorist financing, and other illicit financial activity risks; whether the bank's policies, procedures, and processes for BSA/AML compliance were appropriate for the bank's risk profile; whether the bank actually adhered to such policies, procedures, and processes; and whether management took appropriate and timely action to address any deficiencies.

NEXT STEPS

In light of these enforcement actions, there are a number of steps that a bank might want to consider and questions that it might want to ask of itself.

Risk Assessments

Is the assessment of your institution's money laundering, CFT, and sanctions risks appropriately tailored to your products, services, customers, geographic locations, and your methods of delivering your products and services? Have any of these factors changed since your last risk assessment such that a new risk assessment is advisable? Some institutions might decide that it is appropriate to engage a third party to conduct a new risk assessment, both to obtain an independent view of your risk assessment and so as not to over-burden internal resources who need to focus on day-to-day compliance matters.

Customer Due Diligence

Is your customer due diligence thorough and ongoing? Are customers appropriately risk rated, and is that risk rating adjusted when new information about the customer is obtained? Is customer information and their risk

©2005-2026 K&L Gates LLP. All Rights Reserved.

rating incorporated into your transaction monitoring systems? If you rely on a fintech partner or other third party for customer due diligence, you might want to confirm that they are obtaining and updating customer information as needed to ensure BSA/AML compliance.

Transaction Monitoring

Are your transaction monitoring thresholds, filters, and scenarios appropriately tailored to your products, services, customers, geographic locations, and your methods of delivering your products and services? If you are relying on third-party monitoring systems, have you reviewed their thresholds, filters, and scenarios and confirmed that they are appropriate for your institution? Have these thresholds, filters, and scenarios been tested recently?

Independent Testing

Unless your institution recently performed or had performed thorough independent testing, you might want to consider new testing. As with your risk assessments, it might be best to engage a third party to conduct this testing, both to obtain an independent opinion of your organization and so as not to overburden your internal resources who need to focus on day-to-day compliance matters.

Resources

Has your BSA officer or any independent testing provider suggested that additional resources are needed, and have these suggestions been heeded?

Voluntary SAR Look Back

If the results of independent testing or testing of your transaction monitoring system suggests that the institution might have failed to identify suspicious transactions or file SARs, you might want to consider voluntarily conducting a SAR look back. In this way, you might be able to reduce the negative impacts of your next BSA/AML compliance program.

BSA/AML compliance is not inexpensive, but enforcement actions can cost far more. In addition to needing to spend time and money to address the issues raised in the action, and potentially paying fines, banks with serious BSA/AML compliance deficiencies may be blocked for a period of time from offering new products or services, opening new branches, or engaging in acquisitions. A bank that is subject to a consent order or a formal written agreement with its regulator also generally is not an “eligible bank” for purposes of corporate applications, meaning that expedited treatment of those applications is unavailable. For all of these reasons, we recommend that banks take heed to the lessons that can be gleaned from 2024's round of enforcement actions so as to avoid being a target in 2025 or beyond.

FOOTNOTES

[1] This article focuses only on the compliance issues that were raised by the 2024 enforcement actions. We are not attempting to provide a complete guide to BSA/AML compliance, but only to highlight areas in which an examiner concluded an institution was deficient. In order to provide regulatory background, we sometimes draw from the Bank Secrecy Act/Anti-Money Laundering Examination Manual of the Federal Financial Institutions Examination Council, often without attribution but sometimes by referring to the “Examination Manual.”

©2005-2026 K&L Gates LLP. All Rights Reserved.

KEY CONTACTS



JEREMY M. MCLAUGHLIN
PARTNER

SAN FRANCISCO
+1.415.882.8230
JEREMY.MCLAUGHLIN@KLGATES.COM



JOHN REVEAL
PARTNER

WASHINGTON, DC
+1.202.778.9055
JOHN.REVEAL@KLGATES.COM

This publication/newsletter is for informational purposes and does not contain or convey legal advice. The information herein should not be used or relied upon in regard to any particular facts or circumstances without first consulting a lawyer. Any views expressed herein are those of the author(s) and not necessarily those of the law firm's clients.

©2005-2026 K&L Gates LLP. All Rights Reserved.