



INDUSTRY INSIGHTS

Enforcement Actions Provide Roadmap to Meeting Current BSA/AML Regulatory Expectations

By Rawan Abdelrazek and Kari Trautvetter

U.S. regulators and enforcement agencies continue to introduce new regulatory requirements under the Bank Secrecy Act and Anti-Money Laundering rules (BSA/AML), while stringently enforcing existing rules and expectations. The financial services industry has seen a cascade of activity, from the [Financial Crimes Enforcement Network's \(FinCEN's\) proposed rules on investment advisors and beneficial ownership](#) to a flurry of enforcement actions by the Office of the Comptroller of the Currency (OCC), Federal Reserve, Federal Deposit Insurance Corporation (FDIC), and New York Department of Financial Services (NYDFS)¹

A review of recent consent orders provides insight into heightened regulatory expectations and focus areas. It also illustrates the complexity of building effective programs and implementing remedial actions. Proactively navigating and adapting to the current BSA/AML regulatory landscape enables banks to steer clear of regulatory scrutiny and mitigate the risk of costly enforcement actions. Such actions could potentially lead to restrictions on business activities and the onboarding of new clients, and impact new or existing third-party relationships.

Enforcement Actions Provide an Operational Roadmap

There is no "one-size-fits-all" design for an effective and risk-based compliance program for BSA/AML and Office of Foreign Assets Control (OFAC) sanctions, so long as the program complies with requirements set forth in the BSA and other applicable laws. However, recent enforcement actions taken against smaller banks and institutions offering banking as a service (BAAS) point to heightened regulatory expectations, a heavier hands-on approach, and more prescriptive demands by regulators regarding what constitutes an effective BSA/AML compliance program.


Recent consent orders have common themes and necessary actions, so they provide useful and actionable guideposts to meeting regulatory expectations for effective BSA/AML program development and remediation. They focus on program design, staffing and expertise, independent testing, risk assessments, training, suspicious activity reporting (SARs), and third-party risk management, particularly of fintech partners.


From an operational perspective, the areas for BSA/AML remediation focus on the establishment of board Compliance Committees, mandated staffing assessments, enhancements to customer due diligence (CDD) programs, SAR lookbacks, and overhauls of independent testing and third-party risk management.


In the table below, we break down recent enforcement actions and provide insight into regulatory expectations, the practical implications, and concrete actions banks can take to design or enhance their programs to avoid getting caught in any regulatory crosshairs. The table is grouped by BSA/AML and sanctions compliance program elements.²


¹ In Q1 2024, there were no fewer than six BSA/AML orders by the OCC and FDIC.



² The table contains anonymized and aggregated regulatory actions.

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>BSA/AML Program</p> 	<p>The bank failed to adopt and implement a compliance program that sufficiently covers BSA/AML program elements, including internal CDD controls, procedures for monitoring suspicious activity, adequate BSA officer and staff, and training.</p> <p>The bank must ensure compliance with the BSA and its regulations within 90 days of the effective date of the order.</p>	<p>From an operational perspective, the timeframes imposed by regulators can be unrealistic and place undue pressure on banks and their staff to implement “quick fixes.” Three months is generally not enough time to overhaul a BSA/AML program and does not allow for effectiveness and sustainability. Where regulatory expectations for sustainability are expected but not explicitly communicated, it raises the risk that regulators cite lack of effectiveness during an exam and impose further penalties, such as restrictions on business. The design and execution of a robust and realistic action plan, as described below, is where the rubber meets the road.</p> <p>To achieve maturity and sustainability in a realistic timeframe, banks that are in growth or remediation mode should consider developing a “Target Operating Model” that maps the pathway to a target state of the BSA/AML compliance program, including program elements, systems, and requisite expertise and staffing. These documented exercises can evidence to regulators that bank management “gets it” and can guide conversations with examiners about achievable timeframes.</p>

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Action Plan</p> 	<p>The bank must develop a comprehensive written action plan within 30 (or 45) days of receiving the regulatory order (time frames have varied). This action plan should outline specific steps and timelines for correcting the deficiencies identified in the BSA/AML and sanctions compliance programs.</p> <p>The action plan should address all deficiencies cited by the regulator, covering areas such as CDD, suspicious activity monitoring, recordkeeping, sanctions compliance, and any other aspects of BSA/AML compliance where the bank has fallen short.</p>	<p>Action plan content can vary depending on the extent of the remediation but should be realistic, responsive to the feedback, and sufficiently detailed with timelines, milestones, and deliverables. Regulators do not want to see a “checklist” approach to the design and implementation of actions but rather remediation that identifies and addresses the root cause of the cited deficiencies. This can be challenging if the regulator is concurrently mandating short or unrealistic time frames for remediation.</p> <p>Finalization and implementation of the action plan may be a protracted and iterative process if the regulator seeks to provide “supervisory non-objection” and gives feedback around content, deadlines, and deliverables. In the worst-case scenario, the action plan may be rejected by the regulator and require significant overhaul (e.g., new plan, more or less detail, shorter deadlines, alternative milestones, etc.). Once implemented, material changes to the action plan generally require “no supervisory objection” or approval from the regulator.</p> <p>To manage implementation, banks should establish a project management team to drive and report on progress, especially if a new Compliance Committee with reporting requirements is established. The board should also approve the plan and take an active role in overseeing its implementation (see next section).</p>


Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Board Oversight</p> 	<p>Within 90 days, the board must improve its supervision and direction of the AML/CFT (countering the financing of terrorism) program and take full responsibility for the development, approval, implementation, and adherence by the bank to a sound BSA/AML program.</p> <p>The board must increase oversight of BSA compliance and establish a subcommittee to monitor and oversee the bank’s compliance with the order (Compliance Committee). This committee should provide monthly reports on compliance actions to the board.</p> <p>Within 30 days of each meeting, the Compliance Committee must submit a report to the board about the status of the action plan/remediation, which the board must then submit to the regulator within 10 days of the first board meeting after receipt of such report.</p>	<p>Board members, particularly independent directors, are under heightened scrutiny for their oversight (or lack thereof) of banks’ BSA/AML compliance programs. Regulators expect them to take active, almost managerial, roles in overseeing the BSA/AML program. The establishment of a Compliance Committee will only magnify the microscopic focus placed on board members’ expertise, skills, and level of engagement. More active involvement by independent members may also cause tensions with the bank if their activities cross the line into day-to-day management of business-as-usual (BAU) activities.</p> <p>From an operational perspective, establishment of a Compliance Committee will require significant time by the BSA compliance team and management for project management, regular update meetings, and periodic written reports.</p> <p>In cases where the committee must submit periodic or monthly reports to the regulator, the reports should be detailed, accurate, and realistic, since regulators have criticized management and the board for overestimating the effectiveness of remedial efforts. Such criticism ties back closely to the regulatory expectation noted above that banks not take a “check the box” approach to remedial actions.</p>

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Staffing Assessment</p> 	<p>The board shall ensure that the BSA compliance department is appropriately staffed with personnel who have the requisite skills, expertise, training, and authority. The board should also ensure the bank has a permanent and qualified BSA officer vested with sufficient independence, authority, and resources.</p> <p>The board must, within 90 (or 180) days of the order, review and assess the capabilities and qualifications of the bank’s BSA officer and BSA department and document its determination in writing.</p>	<p>Regulators want to see qualified and experienced compliance teams regardless of a bank’s size. They are not hesitating to direct management or the board to replace staff and to cite specific names in exam reports. Regulators are particularly focused on the skills, background, and stature of the BSA officer (BSAO), as well as his/her access to the board. They are also voicing their expectations that the BSAO be solely dedicated to BSA/AML compliance (i.e., not responsible for other areas of the compliance program) and operate independently of management. Small institutions where the chief compliance officer (CCO) wears two hats may need to consider hiring a dedicated BSAO.</p> <p>Regulators are also scrutinizing the adequacy, composition, and skills of the BSA/AML compliance team. This means that banks can no longer deploy a small BSA/AML compliance team of generalists to conduct all activities. The team must include subject matter experts in “know your customer” (KYC) procedures, transaction monitoring, investigations, sanctions, and risk assessments.</p> <p>As a matter of best practice, the BSAO should conduct and document annual and periodic staffing assessments to ensure they have sufficient levels of personnel to address BAU activities and any anticipated growth in business. The assessments should take into account the institution’s size, complexity, products, clients, and AML systems. Importantly, the assessments should account for any staffing needs to address remediation. Regulators will review these during exams and expect to see both quantitative and qualitative assessments that are clearly documented and justified by underlying data.</p> <p>Several orders have required boards to conduct independent staffing assessments and report those results to the OCC or FDIC. In such cases, the use of independent third</p>

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Staffing Assessment (cont.)</p> 		<p>parties can ensure that the assessment is not influenced by management or the BSAO/team. As with any internal periodic exercise, these independent assessments should be both qualitative and quantitative in nature. Banks should be prepared for regulators to scrutinize these reports and the underlying work papers and to anticipate needing to hire additional staff/replace certain staff upon receipt of a report, including the BSA officer. Examiners may also interview team members to validate (or challenge) the findings in an internal/external assessment.</p>
<p>BSA/AML Training</p> 	<p>The board shall ensure the bank develops, implements, and adheres to an acceptable written training program for bank employees and board members to ensure their awareness of the responsibility for compliance with the requirements of the BSA program.</p> <p>The bank shall perform an independent assessment of the bank's BSA/AML training to include its operational effectiveness and provide that report to the Compliance Committee and regulator.</p> <p>Required training shall be conducted by qualified staff and/or independent contractors, include training in all aspects of regulatory and internal policies and procedures related to BSA regulations, and provide specific training on certain products.</p>	<p>Training is one of the foundational elements of a BSA/AML program and can be low hanging fruit for regulators to critique. Simple delivery of training is not a sufficient indicator of success. It is critical that banks draft a written training program with topics, frequency, target audience, and procedures to track and ensure completion. The plan must also include board training. Regulators also expect the written program to detail the consequences for non-compliance. Delivery of training should be documented with dates, attendance records, and test results where applicable.</p> <p>Regulators will assess the operational effectiveness of BSA/AML training during their assessments of various program elements, such as CDD and transaction monitoring, and may mandate additional topic-specific training.</p>

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Customer Due Diligence (CDD)</p> 	<p>The bank must develop, adopt, and implement a written risk-based CDD program within 60 (or 90) days, addressing customer risk profiling, enhanced due diligence (EDD), ongoing due diligence, and beneficial ownership information—and effectively use this information to monitor and investigate suspicious or unusual activity.</p> <p>The bank shall develop a proposed plan to provide for a lookback of prepaid card customers (“CIP lookback review”) to ensure that all required customer identification program information has been obtained and that the bank has formed a reasonable belief that it knows the true identity of the customer.</p>	<p>Recent enforcement actions have underscored the importance of the CDD process for building an accurate risk profile of customers and driving effective transaction monitoring. Where they have found weak programs or inadequate client files, they have mandated lookbacks or refresh exercises.</p> <p>A critical component of any effective CDD program is the customer risk rating process (CRR), which weighs the risks associated with client type, product, anticipated/ actual activity, jurisdiction, presence of negative news, and other factors. Banks often hire third parties to design a CRR based on best practices in the industry. But examiners have been critical of this approach, including the use of judgmental overlays, weighing in with their own opinions on “appropriate” weightings and risk assignments. They want to see, and will test, that the CRR tool is tailored to the bank’s business, products, client types, and risk profile (as seen by the regulator). An equally significant component of the program, no matter the size and maturity of the institution, is data management and documentation. This includes client lists, due diligence files, the client risk profile, event-based refreshes, and the exception process. One recent order, for example, underscored the importance of documenting the process for resolving issues when customer information is insufficient or inaccurate.</p> <p>Poor data management can negatively impact the regulatory exam process and raise suspicion on the part of regulators around transparency. Data gaps have led examiners to express frustration with, and distrust of, management.</p>

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Third-Party Risk Management (TPRM)</p> 	<p>The board and management must implement a written program to assess and manage the risks posed by third-party relationships, including fintech partners and sub-partners (third-party risk management). The program should include policies and procedures to assess the risk of third-party products, services, and activities; details about how the bank selects, assesses, and oversees each third party; a strategic plan; and criteria for board review and approval, among other elements.</p> <p>The bank shall not contract with any third party to perform BSA/AML functions unless the bank has conducted and documented an assessment of these third parties' skills and training, including a quality control program to evaluate performance against specific standards.</p>	<p>Regulators continue to be laser-focused on third-party risk management, placing a heavy focus on the BSA/AML components of this process. Where regulators are finding significant deficiencies, they are imposing restrictions on banks entering into any new third-party arrangements (limiting business growth) or are mandating remedial efforts. For example, the OCC recently required one bank to undergo remedial efforts to "immediately" ensure that the onboarding of new end user accounts within existing third-party fintech relationships and sub-partners complies with BSA/AML requirements.</p> <p>From an operational perspective, regulators want to see banks conducting detailed BSA/AML risk assessments of their third parties, particularly fintechs, and their products and services. The assessments should analyze the BSA/AML and sanctions risks of the bank's relationship, as well as that third party's own internal BSA/AML controls. Where the bank has delegated AML activities, such as KYC or transaction monitoring, the bank must conduct and document a detailed assessment of the third party's BSA/AML compliance program and test its controls. Banks should expect that these reports and the underlying workpapers will be read and critiqued by regulators.</p> <p>Banks should also incorporate these third-party risk assessments into their annual BSA/AML program risk assessments and ensure that the BSA/AML audit program includes independent risk-based reviews of activities conducted through third parties.</p>

Recent Enforcement Actions: Key Actions and Takeaways		
Program Element	Regulatory Findings and Actions Required	Implications
<p>Suspicious Activity Monitoring and Reporting Program</p> 	<p>The bank is required to establish a risk-based program to identify, evaluate, and report suspicious activity across all business lines, accounts, and sub-accounts provided by and through the bank’s third-party relationships.</p> <p>A third-party consultant must conduct a SAR lookback to determine if additional SARs should be filed for previously unreported suspicious activity. The board shall submit, for prior written determination of no supervisory objection, a proposed scope and timeline for completion. (The scope of the SAR lookback shall be determined in writing by said regulator.)</p> <p>The board shall engage an independent, qualified third party to conduct a lookback activity for the largest fintech partnership account to ensure any suspicious activities are identified and reported.</p>	<p>The requirements for an effective program are consistent across current and past orders, but regulators are increasingly mandating SAR lookbacks for small banks, regardless of risk profile or transaction and alert volumes. Where one or more BSA/AML program elements are deemed insufficient, including the CDD process, regulators will question the ability of the bank to identify risk and suspicious activity and thus the sufficiency of its prior monitoring efforts. And by extension, they focused on individual accountability, requiring banks to document individual decisions to file/not file a SAR.</p> <p>Regulators may not communicate the timing of actions on their end. This means that, where the bank must obtain supervisory non-objection for a SAR lookback methodology and/or the third party engaged, approval and execution may be a protracted waiting game. And in the worst-case scenario, the regulator may, based upon lookback results, expand the scope and time-period of the exercise.</p> <p>Any SAR lookback will be an operational lift, but banks should incorporate insights gained from the exercise to enhance their programs and train staff.</p>

Conclusions

In essence, financial institutions should study and leverage recent consent orders as a roadmap for how to build or remediate their BSA/AML programs. Successfully navigating this regulatory environment requires proactive measures and long-term investments in people, processes, and systems. As discussed above, key areas of focus should be:

- Ensuring the BSA/AML compliance team, including the BSAO, are competent and adequately resourced and independent of management.
- Staffing boards with experienced and engaged independent board members.
- Designing a written CDD and EDD program that enables accurate development of client risk profiles and effective leveraging of that information in the transaction monitoring process.

- Maintaining an effective suspicious activity monitoring and reporting program for both clients and third-party relationships.
- Thoroughly understanding and mitigating the risks posed by third-party relationships by incorporating BSA/AML and OFAC risk assessments into any third-party risk management program and conducting regular reviews of the BSA/AML compliance programs of third parties.
- Ensuring the accuracy, completeness, and governance of compliance and other applicable data.

Banks facing potential enforcement actions need to quickly deploy their time and resources toward remediation and anticipate that the process will be both operationally and financially burdensome. Regulators are requiring that deficiencies be addressed immediately or within short time frames, which will take resources away from business-as-usual activities. Where resources are limited, banks need to seek credible and credentialed outside assistance, both to support implementation and to signal to the regulators that they are serious about fixing the identified issues. Banks should not wait for formal action to develop action plans and begin remediation, especially where policies, procedures, and processes require enhancements.

Note: Treliant offers specialized expertise and tailored solutions to address this heightened regulatory landscape. Our team includes former practitioners, regulators, and advisors who can help banks navigate complex compliance requirements, identify vulnerabilities, and implement effective remediation strategies.

**Rawan Abdelrazek**

Rawan Abdelrazek, Managing Director with Treliant's Financial Crimes and Fraud Solutions team, is a seasoned financial services executive with extensive experience in program buildouts, compliance, remediation, digital assets/cryptocurrency, strategic change, operational management, and government leadership. She has a solid track record in compliance and program remediation for adherence to the Bank Secrecy Act and Anti-Money Laundering rules (BSA/AML).

rabelrazek@treliant.com

**Kari Trautvetter**

Kari Trautvetter, a manager at Treliant, has over four years of experience and advises clients worldwide on anti-money laundering (AML) matters and other aspects of compliance programs. She has experience across a broad range of compliance-related projects, including fraud investigations, AML compliance, cryptocurrency regulatory compliance, sanctions review, and related litigation.

ktrautvetter@treliant.com