New York Law Journal
SERVING THE BENCH AND BAR SINCE 1888
WWW.NYLJ.COM
An ALM Publication
VOLUME 260—NO. 96
FRIDAY, NOVEMBER 16, 2018

Outside Counsel

So You Want to Join a Bank Board? Ask About AML Risk Oversight

By **Matthew L. Biben**

In the first half of 2018, financial regulators around the world imposed more than $1.7 billion in fines related to anti-money laundering (AML) compliance failures, nearly matching 2017's annual total of $2 billion. More than $1 billion of that $1.7 billion originated from enforcement actions by U.S. regulators and prosecutors. If you have been asked to join the board of directors of a financial institution, you should be asking yourself two questions: "What do I need to know in order to effectively oversee and hold management accountable for complying with AML laws and regulations?" and "What questions should I be asking management and the chief compliance officer (CCO) about the company's AML policies and U.S. sanctions programs?"

What Do I Need to Know?

While you may already know the basic requirements of AML regulations, such as the requirement to file currency transactions reports (CTRs) and suspicious activity reports (SARs), it's worth taking a look at the Federal Financial Institutions Examination Council Bank Secrecy Act/Anti-Money Laundering Examination Manual (the FFIEC Manual). Originally created as a guide for bank examiners carrying out Bank Secrecy Act (BSA) and Office of Foreign Assets Control (OFAC) examinations, the FFIEC Manual provides an excellent overview of AML compliance program requirements, BSA/AML risks and risk management expectations.

> Upon arrival at any financial firm, you should receive at least summary data that reflects the overall health of the company's AML compliance program, including key risk indicator reports.

What Questions Should I Be Asking?

Upon arrival at any financial firm, you should receive at least summary data that reflects the overall health of the company's AML compliance program, including key risk indicator reports. As with other issues tracked by the board, there is often a balance between getting too little and too much information. For years, the Office of the Comptroller of the Currency (OCC) has published a "Director's Toolkit," which includes documents such as "Detecting Red Flags in Board Reports—a Guide for Directors," and "Internal Controls—a Guide for Directors." These publications offer specific AML-related questions for directors to consider and ask, and are worth reviewing.

That said, since there are several key AML issues that have been the subject of recent AML enforcement actions, we suggest directors ask the following questions of management and the CCO about the company's AML policies and U.S. sanctions programs:

Do we have a written AML risk assessment? Risk assessments should first measure inherent risk, which is

MATTHEW L. BIBEN *is a litigation partner and co-leader of the banking industry group at Debevoise & Plimpton.*

the risk that an activity would pose if no controls or other mitigating factors were in place. A residual risk rating should be assigned after controls are taken into account. The assessment should be candid and self-critical, such that reading one is an eye-opening experience. This is especially true for assessments describing the inherent risks of doing business in a high-risk jurisdiction or providing high-risk financial services. (Think: processing transactions for money transmitters along the Mexican-U.S. border, providing international private bank accounts to politicians in Latin America or correspondent accounts to banks in Latvia, or services to cryptocurrency trade). Small institutions might not have formal written assessments, but they still need to engage in and document the assessment process. In conversations with senior management, resist their inclination to discuss their controls or other mitigating factors until the inherent risks are thoughtfully considered and vetted.

Do we have uncorrected supervisory issues contained in written agreements, enforcement actions or matters requiring attention (MRAs)? Large fines and enforcement actions for AML deficiencies can be levied by criminal law enforcement agencies during investigations that turn relatively quickly from focusing on the crimes of money launderers to the failures of compliance departments. But most enforcement actions are brought by regulators for uncorrected deficiencies previously cited by them during routine exams. While overseeing and holding management accountable for fixing these problems, beware of solutions involving technology upgrades that might prove to be unfeasible—in two years and too late to avoid further regulatory action. Ask for regular updates and drill down on milestones that could be at risk.

Do we have uncorrected AML deficiencies identified by outside consultants? Senior managers and compliance officers occasionally retain outside experts to review the firm's AML compliance program. Such ad hoc reviews are often triggered by unfavorable audit or exam findings, pending enforcement actions or management's desire to proactively find and address problems. Recent AML enforcement actions have highlighted the risks to financial institutions receiving such assessments when they have not acted on them to fix documented AML deficiencies, or have withheld them from regulators who have asked to see such reports. If the BSA compliance officer is new to the firm, ask her or him to check the files for reports commissioned and left behind by the former BSA compliance officer.

Outside of the compliance department, which other employees receive AML training? How is the training list vetted? To whom and how often do employees report suspicious activity? Financial institutions must ensure that appropriate personnel are trained in applicable aspects of the BSA. As a director, you will receive training that is most likely tailored to your role of providing oversight, approving BSA/AML policies, and ensuring that management is providing sufficient BSA/AML resources. But the answer to the questions "Who else is receiving this type of training," "Who has reviewed the training list?" and "How often are they identifying and reporting activity," will provide considerable insight into the firm's culture of compliance. Is compliance with AML regulations viewed as a company-wide responsibility? If so, who is getting the training and are there measurable results?

Do we receive and analyze consumer and fraud complaints? Are there any ongoing government investigations concerning fraud by or through the company? These two questions should result in an important conversation with management about possible fraud occurring at or through the institution, such as internet-based scams resulting in victims sending numerous but relatively small dollar transactions through the institution. For years, regulators were slow to treat fraud detection and reporting as an AML requirement, but criminal prosecutors eventually stepped in to offer clarification—in the form of prosecutions and large fines—for firms failing to detect, report and stop such transactions.

What are our SAR volumes and how do they stand relative to our peers, based on industry benchmarking and FinCEN statistics? Disclosures of specific SAR filings outside of the filing institution are prohibited, but AML compliance officers should have a good sense of how their SAR volumes compare to other institutions. Small institutions, in particular, seem prone to under-reporting. This is often a result of several factors including lack of experience, misconceptions about the level of suspicion required to file a SAR and the effects

of reporting a particular client. *Note:* a review of the past 35 years of BSA enforcement trends quickly confirms that the risks of under-filing far outweigh the risks of over-filing.

How often does the BSA officer present to the board? The board of directors must designate a qualified individual to serve as the BSA Compliance Officer. The BSA Officer is responsible for ensuring that the designated individual has sufficient authority and resources (monetary, physical, and personnel) to administer an effective AML compliance program.

Given the increasing legal and practical requirements placed on a board by AML and OFAC regulations, it may be worth considering whether to designate a committee of the board to sit as a compliance committee to review these and other compliance issues.

The BSA compliance officer must regularly apprise the board and senior management of ongoing compliance with the BSA, including the reporting of SARs filed with FinCEN. The ability of the BSA compliance officer to speak openly with the board about AML compliance issues, particular the resources needed to address potential program deficiencies, is an important indicator of the program's health.

Are there sufficient AML and Audit staff members who are competent and knowledgeable to manage current and proposed business activities? What are the employee attrition rates for these departments? Small institutions often hire AML and Audit staff members who lack sufficient expertise and who may also find it difficult to identify when and where additional resources are needed. But all institutions, large and small, are occasionally hit with significant increases in investigative caseloads which can lead to employee attrition and the loss of important institutional knowledge. Sufficiency of resources is a dynamic exercise that needs to be monitored in light of changing business mix and regulatory expectations.

Do we have any compliance alert or case backlogs? While this may be related to the previous question about staffing, it calls for a much more objective answer, and the existence of a significant compliance backlog can be the equivalent of a "canary in a coal mine" problem for a financial institution. Regulators allow for occasional late SAR filings but, when the number of late SAR filings increase, they can quickly conclude the existence of a systemic failure warranting supervisory action.

Regarding U.S. sanctions screening—what have we missed (either individual transactions that we failed to block or reject, or whole groups of transactions)? OFAC requirements are separate and distinct from the BSA, but both OFAC and the BSA share a common national security goal. For this reason, regulators and many financial institutions view compliance with OFAC sanctions as related to BSA compliance obligations. In general, the regulations administered by OFAC require financial institutions to block accounts and other property of specified countries, entities, and individuals; or prohibit or reject unlicensed trade and financial transactions with specified countries, entities, and individuals. True hits in this area happen, as do "misses"—the failure to block or reject prohibited accounts or transactions that might, upon review by OFAC, expose the company to significant fines. Asking what transaction the institution has "missed" during a given period (e.g., the most recent two-year period) is also a good starting point to understanding the institution's customer base and risk profile.

Given the increasing legal and practical requirements placed on a board by AML and OFAC regulations, it may be worth considering whether to designate a committee of the board to sit as a compliance committee to review these and other compliance issues. Regardless of whether a subcommittee on behalf of the full board, or the full board, owns these responsibilities, it's important that the right questions be asked about the AML program. As boards increasingly focus on monitoring the spectrum of risk, including new risks like cyber, it's as important as ever to keep risk oversight of AML compliance top of mind.