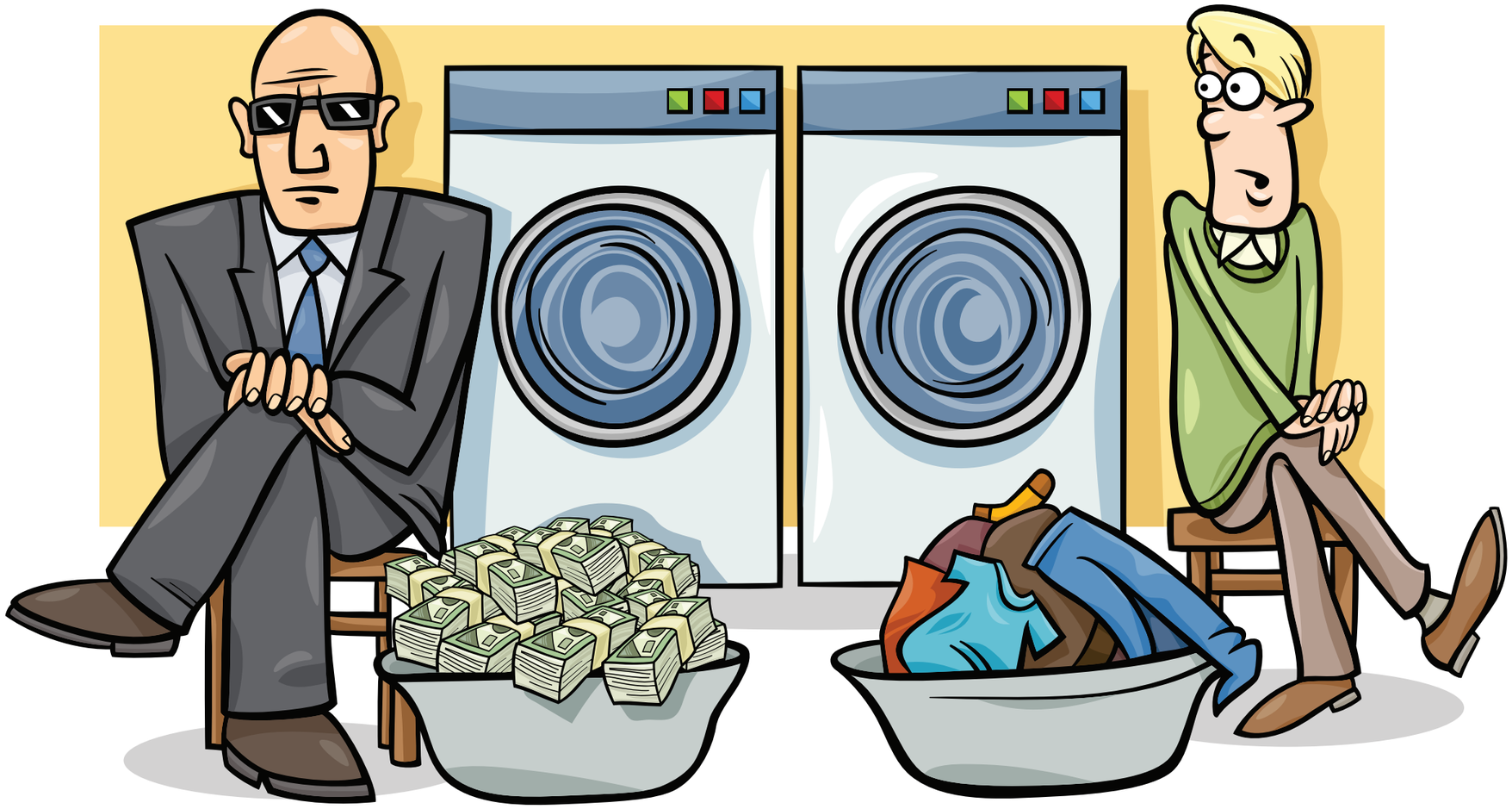

COMMON AML COMPLIANCE PROBLEMS

AND WAYS TO AVOID THEM

SHUTTERSTOCK, INC.

BY JEFFREY F. INGBER

BANKS[1] OF ALL types expend vast amounts of staff resources, money, and management attention to ensure an appropriate anti-money laundering (AML) and sanctions compliance program.

Yet they continue to find themselves subject to serious supervisory findings, private and public enforcement actions, record-breaking levels of fines and monetary settlements for violations, and curtailment of plans for expansion. In 2014 alone, supervisors and law enforcement agencies levied monetary settlements for money laundering, sanctions, and tax evasion in excess of $13.4 billion.[2]

There are reasons for this that extend beyond a bank's control, including ever-rising supervisory expectations, sensitivity to AML matters in a world rife with terrorism, and the complexity of newer requirements such as Ukraine- and Russia-related sanctions. Nonetheless, banks and other financial institutions continue to make their own fundamental mistakes in the AML arena. Below is a summary of 10 key mistakes and some ways to avoid them.

IN SOME SENSE, PREPARING FOR AN AML EXAM IS LIKE STUDYING FOR A TEST THAT YOU'VE BEEN GIVEN THE ANSWERS TO, BECAUSE THE FFIEC'S BSA/AML MANUAL NOTES WHAT SUPERVISORS WILL FOCUS ON: THE "PILLARS" OF AML COMPLIANCE.

1. Insufficiently Linking the AML Compliance Program to the Firm's AML Risk Assessment

In some sense, preparing for an AML exam is like studying for a test that you've been given the answers to, because the FFIEC's BSA/AML manual notes what supervisors will focus on: the "pillars" of AML compliance.

Of the four traditional pillars, the one most likely to generate a "matter requiring attention" (MRA), other findings, or some type of enforcement action is the requirement for an adequate system of internal controls. Internal controls is a broad concept that requires policies, procedures, and processes to ensure a multitude of things, including the ability to readily identify and mitigate higher-risk operations as well as the timely detection and reporting of suspicious activity.

Banks often are tagged with an improper internal controls process because they fail to maintain the foundation on which it must be built: an assessment of the inherent AML risks that flow from their products, services, customers, delivery methods, and geographic markets, and the controls needed to mitigate those risks. For example, greater controls must be in place if a bank 1) has a customer base that includes foreign entities or politically exposed persons (PEP); 2) services other financial intermediaries such as third-party payment processors, money service businesses, or foreign correspondents; or 3) offers high-risk products such as prepaid cards or remote deposit capture. And the efficacy of those controls must be assessed by key risk indicators and other metrics and data.

A DYNAMIC AML COMPLIANCE PROGRAM IS ONE THAT CONTINUALLY RECONSIDERS ITS RISK STRUCTURE TO ADDRESS ANY GAPS PRESENTED BY ADDITIONAL BUSINESS OR ENVIRONMENTAL CHANGES THAT CAN CREATE NEW OR HEIGHTENED RISKS.

Similarly, each of the other three pillars cannot be appropriately addressed unless it is properly risk based. The risk assessment should inform and complement the expertise of BSA/AML officers as well as the staffing and technology resources they command.

Training for the approved AML compliance program must be tailored to relevant risks, as opposed to being overly generic, and regularly updated to match evolving regulatory requirements. In particular, training provided to the lines of business should be detailed and relevant to the mix of products and services offered. For example, professionals involved in onboarding new customers should be well versed in the associated AML risks and the institution's standards for new customer acceptance.

The focus of independent testing of the AML compliance program by independent compliance and internal audit must flow from an understanding of the AML risk assessment that leads to higher frequency and intensity of testing for the greatest risks. (Conversely, while the independent testing requirement is expected to be applied on a risk-prioritized basis, a bank also is expected to be able to demonstrate that its full AML compliance program has been subjected to testing.)

Customer due diligence (CDD), which links a bank's know-your-customer program with its monitoring and reporting of suspicious activity and which always has been integral to an effective AML compliance program, now effectively has been elevated to "fifth pillar" status. The FFIEC manual makes clear that a bank's CDD program must be commensurate with its AML risk profile. A sound AML customer risk assessment should 1) collect sufficient information on a customer to determine its AML risk (for example, create an expectation of transactional activity); 2) develop an accurate and complete customer profile using the information collected; and 3) implement criteria to prompt enhanced due diligence (EDD), either due to the customer type or prompted by red flags generated from transaction-monitoring activity.

2. Inadequately Addressing Beneficial Ownership

Concerns regarding beneficial ownership (a concept that includes both legal ownership and effective control) have taken center stage in the AML compliance world. As the Financial Action Task Force has stated, knowing beneficial ownership allows banks to better judge whether a corporate client is a money-laundering risk and enables law enforcement to more easily "follow the money."

In July 2014, the Financial Crimes Enforcement Network (FinCEN) issued a long-awaited proposed rule (not yet final) requiring banks to collect and maintain information on individuals who hold 25% or more of an interest in a customer or who otherwise control the customer.

It can be challenging to look through layers of legal ownership, particularly for entities such as shell companies, trusts, partnerships, and special-purpose vehicles. Historically, compliance officers have implemented procedures that require navigating through a multitude of corporate registries, Internet pages, and public databases (such as the S.E.C.'s EDGAR). While they may appear comprehensive, these time-consuming searches often prove unproductive.

Banks must continue to up their game in this area. Customers, especially those rated "high risk," must be required to periodically provide meaningful information about changes in beneficial ownership. Banks should consider increasingly targeted searches using the most advanced database solutions for screening against PEP, sanctions, or enforcement lists, as well as outsourcing to intelligence services that can provide information not publicly available. And all the information gathered by a bank to determine beneficial ownership should be assimilated into its overall CDD knowledge base.

3. Treating AML Compliance as a Static Exercise

A common mistake is to set up (often with assistance from consultants who then disappear along with their knowledge base) a "state of the art" CDD or automated monitoring program and then gradually neglect it—essentially treating AML compliance as a static exercise revisited only sporadically.

A dynamic AML compliance program is one that continually reconsiders its risk structure to address any gaps presented by additional business or environmental changes that can create new or heightened risks. For example, if a bank has recently implemented a major new product or platform (such as mobile payments or expanded online account openings), the consequent risks should be reflected in an updated assessment and controls framework. This includes supplementing customer profiles and reevaluating and recalibrating the data input, thresholds, and rules underlying automated monitoring systems to ensure they continue to make sense for the types of transactions the bank is trying to identify and control. And a robust AML compliance program requires a dynamic chief AML compliance officer, one who is plugged into the ongoing evolution of the bank.

4. Placing the Burden on Supervisors

If an institution is under an enforcement action or has received an MRA or other findings from a supervisor, it is important that these deficiencies be addressed promptly and thoroughly. Often, however, that's the bulk of what an institution is expected to do between scheduled exams, under the assumption that the path to keeping a supervisor happy is to focus on its specific criticisms.

This "managing to supervisory expectations" approach has the effect of placing the burden on the supervisor to oversee a bank's AML compliance program. No one knows an institution and its AML risks better than its own management and staff. Plus, supervisory requirements and expectations change constantly. Rather than waiting for supervisors to identify improvement needs, all three lines of defense should be proactive in updating their respective responsibilities within the AML program.

Meanwhile, because no compliance program is foolproof, those overseeing it must maintain strong, effective working relationships with supervisors—ones that facilitate disclosure of major problems and avoid unpleasant surprises. Proactively managing relationships with supervisors will help safeguard the bank's reputation and regulatory risk profile.

However, opening the kimono is only appropriate up to a point. Disclosure to a supervisor does not replace prevention, the prompt remediation of issues, or the application of sufficient resources and focus to AML matters. And when an institution discloses a weakness to a supervisor, it should be prepared to also provide a pragmatic solution, one that mitigates any gap in controls (for example, an interim compensating control, such as a manual solution until an automated tool is implemented).

5. Forgetting That Less May Be More

As business expansion and changing external circumstances raise AML risk, a bank is required to continuously increase expense, resources, and focus. Not to mention that some AML risks are difficult to mitigate even under the best of circumstances.

Business growth also creates inherent conflicts. For example, if a bank enters a high-risk jurisdiction, there is incentive to allocate an inappropriate risk score to it, which may lead to not applying EDD and stricter monitoring measures. This is a critical misstep, as supervisors expect strong EDD measures to be in place for accounts that are not low or medium risk. In general, adding high-risk customers places pressure on relationship managers to understate the AML risks they present. A good practice in this regard is for the AML officers to define the attributes of a high-risk customer and grant secondary approval to the front-line business professionals.

As AML risks rise, potential de-risking through business reduction must be added to the arsenal—specifically, not taking on, or eliminating, certain high-risk products, services, markets, and client relationships not deemed "core." As the bank performs ongoing AML assessments of its lines of business, a part of the evaluation should be to determine if their design and risks continue to fit with the capabilities of the bank's overall AML program. And in this vein, a bank should be inherently skeptical of the wisdom of taking on accounts closed by other banks per their own de-risking program.

6. Overreacting to AML Risk

Now let me contradict myself a bit. The recent trend by banks to close accounts deemed high risk, such as foreign embassies, correspondent banks, and money-transfer businesses, has provoked a pushback from regulators. In a March 2015 speech, Comptroller of the Currency Thomas J. Curry stated that "the OCC does not encourage banks to terminate customer relationships without a careful analysis of the risks presented by that customer and the bank's ability to manage those risks." His speech followed FinCEN guidance, which was issued in November 2014 out of concern that banks had begun to "indiscriminately" terminate money service business (MSB) accounts or refuse to open them, and referenced FinCEN's expectation that banks "serve the MSB industry while meeting their BSA obligations."

Thus, a Catch-22 situation has developed requiring that an institution that's actively de-risking document a clear and specific rationale for terminating established client relationships. A smart approach to a balanced de-risking process is to craft a detailed AML risk appetite statement that explains and justifies such actions as part of an overall business strategy and provides guidance as to which risks the bank believes can be appropriately controlled.

7. Not Carefully Assessing Payment Processors

With good reason, supervisors are increasingly sensitive to the services banks provide to payment processors, which themselves service a variety of merchant accounts. Payment processors often are not subject to BSA/AML regulatory requirements and can be lax in performing due diligence on their own clients' identities and business practices.

Banks must ensure that they can monitor and understand the nature and source of the transactions processed through an account established for a payment processor and that the processor itself has an adequate customer-approval program. Ways to assess the risks associated with

A SOUND AML PROGRAM CANNOT EXIST UNLESS IT IS SUPPORTED BY AND REFLECTIVE OF AN OVERALL STRONG CULTURE OF COMPLIANCE, ONE THAT DOES NOT ALLOW FOR THE COMPROMISE OF POLICIES, PROCEDURES, AND PROCESSES FOR BUSINESS GAIN.

such bank accounts include conducting extensive background checks, requiring the processor to identify its major customers, determining the adequacy of its due diligence standards for accepting new merchants, reviewing databases to check whether the processor and its principal owners and operators have been subject to law enforcement actions, and monitoring for indicators of fraudulent activity.

8. Failing to Keep Good Records

As examiners will tell you, it doesn't count unless appropriately documented. Common mistakes and omissions in recordkeeping and documentation include the following:

- Policies and procedures that do not reflect current practice or that do not indicate the person(s) currently responsible for implementing them.
- Training records that are not up-to-date or do not provide evidence that those required to take the training have completed it.
- Lack of clear records in regard to resolution of FinCEN 314(a) reviews and false OFAC positives.
- Lack of complete work papers evidencing the scope of independent testing, as well as a lack of documentation demonstrating that findings were communicated to senior management and the board of directors.
- Failure to have an agreement that specifies how third parties used for CIP reviews and OFAC checks will perform these activities.

Maintaining comprehensive customer due diligence files also is a key, particularly for high-risk customers. As an example, for a money service business, the file should contain the following information at a minimum: 1) confirmation of the MSB's up-to-date registration with FinCEN (if required); 2) confirmation of compliance with state licensing requirements; 3) a listing of which agencies examine the MSB for AML compliance (for example, the IRS, state banking departments, etc.); 4) evidence of review of the customer's agents, both foreign and domestic; and 5) the evaluation conducted of the customer's BSA/AML program.

9. Not Ensuring a Culture of Compliance

A sound AML program cannot exist unless it is supported by and reflective of an overall strong culture of compliance, one that does not allow for the compromise of policies, procedures, and processes for business gain. Supervisors have increasingly come to expect boards of directors and senior management to send a clear message to all staff members and third-party representatives of the bank that reputation and ethical behavior are critical and to communicate their expectations for how this is best done.

It's vital that this "tone from the top" not be conveyed only statically through corporate documents such as a code of conduct, mission statement, or a reputational risk policy. Rather, senior managers must actively engage with staff in ways that ensure everyone understands the ethical requirement as a guide to day-to-day conduct—thereby strengthening the "tone at the middle." Such communication should be two-way, with an escalation process in place that facilitates the flow of information from staff up to senior managers.

Boards and senior management, working closely with their HR departments, also are expected to demonstrate their use of incentives to reinforce culture. Decisions about bonuses, promotions, performance ratings, and so on must be formally and sufficiently tied to consideration of how well individuals adhere to the stated compliance culture.

As noted in an August 2014 FinCEN Advisory, another key to ensuring a strong AML compliance culture is that "relevant information from the various departments within the organization is shared with compliance staff to further BSA/AML efforts." This statement underscores the criticality of the three lines of defense working in coordination to identify, understand, and address AML issues.

10. Insufficient Tender Loving Care for U.S. Affiliates

For years, foreign banking organizations (FBOs) have engaged in activities in the U.S. through a variety of organizational structures. Scrutiny of them will increase, post Dodd-Frank, as a result of the intermediate holding company rules designed to help ensure enhanced capital, adequate liquidity, and other prudential standards. FBOs also must be mindful of the need to ensure the compliance strength of their U.S. affiliates. In the past, as demonstrated by various enforcement actions, many foreign head offices have neglected their U.S. regulatory and statutory obligations.

One key is to establish an organizational and reporting structure with appropriate checks and balances. It's a mistake to have U.S. independent compliance staff report solely to business management, as this presents potential conflicts of interest that could hinder effective BSA/AML compliance. An appropriate level of independence should be maintained by providing U.S. compliance staff with a reporting line to the global corporate compliance function and ensuring they are actively involved in all matters affecting AML risk, including adherence to U.S. AML requirements.

Conversely, it's also a mistake to have U.S. compliance staff report to global compliance staff without some type of matrix reporting relationship to the U.S. business. The business owns all risks, including those related to AML, and understands them best. The business also appreciates the nuances of U.S. laws and regulations. Thus, the organizational structure must facilitate U.S. compliance staff working closely with the business to identify and address domestic AML issues.

To avoid problems with U.S. supervisors, the FBO's head office must demonstrate that it serves as a source of compliance strength for its U.S. affiliates by providing sufficient resources and management focus, granting authority to the U.S. AML head to act promptly and decisively on U.S. issues, and ensuring accountability on the part of the business lines. To do all this, the head office must receive a sufficient flow of information relating to U.S. operations and have a thorough understanding of the BSA/AML risk and control environment governing U.S. operations.

Managing a bank's AML compliance program requires not just sufficient resources, expertise, and commitment, but also proactive, knowledgeable management and a staff organized, authorized, and incentivized to properly address the most sensitive issues of the day. A well-balanced combination of quantitative and qualitative tools is critical to AML compliance success. ®

Jeffrey F. Ingber, an industry consultant, has held senior management positions at Citibank, the Depository Trust & Clearing Corporation, and the Federal Reserve Bank of New York. He can be reached at jingber@gmail.com or www.jeffingber.com.

Notes

1. As used here, "bank" is intended broadly to mean banking organizations—that is, financial holding companies, bank holding companies, savings and loan holding companies, and banks.
2. See ACAMS, Annual Enforcement Action Survey, 2015 (available at http://info.moneylaundering.com/enforcement-action-2015.asp).