BSA/AML/OFAC
Regulatory Expectations of Bank Boards of Directors:
Protect your bank and the financial system.
It's a big job. Severe penalties for non-compliance.

Focus on what's important

April 00, 2019
Bank Secrecy Act (BSA) - Office of Foreign Asset Control (OFAC) Anti-Money Laundering (AML)
2019 Board of Directors Training Session – [redacted]

Focus on what's important

NOTE TO VIEWERS
<u>This is a 20 minute presentation</u>. The presenter will address only the "headlines."
However, there's plenty of information here than should be carefully considered later.

Questions are always welcome,
Except I will probably be shot if I go overtime.
However, I'll be completely out of breath, so being shot won't be that big a deal.

April 00, 2019
Bank Secrecy Act (BSA) - Office of Foreign Asset Control (OFAC) Anti-Money Laundering (AML)
2019 Board of Directors Training Session – [redacted]

FOCUS ON THESE FIVE IMPORTANT THINGS:

1. Implement and continually update BSA/AML and OFAC risk assessment

2. A written BSA/AML/OFAC policy and procedure describing how compliance will be achieved and maintained
    - •A system of internal controls to ensure ongoing compliance.
    - •Independent testing of BSA/AML compliance.
    - •Designate an individual or individuals responsible for managing BSA compliance (BSA compliance officer).
    - •Training for appropriate personnel.
3. Develop a robust , tailored to your bank, continually updated
    - •Customer Information Profile (CIP) procedure
    - •Customer Due Diligence (CDD) procedure
    - •Enhanced Due Diligence (EDD) procedure for high risk customers
4. Focus on Suspicious Activity Monitoring and Reporting

The Regulation's Expectation

The Bank Secrecy Act (and AML, OFAC) is intended to safeguard the U.S. financial system and the financial institutions that make up that system from the abuses of financial crime, including money laundering, terrorist financing, and other illicit financial transactions.

Money laundering and terrorist financing are financial crimes with potentially devastating social and financial effects.

Regulation Describes Board Responsibilities

The board of directors is responsible for approving the BSA/AML compliance program and for overseeing the structure and management of the bank's BSA/AML/OFAC compliance function.

The board is responsible for setting an appropriate culture of BSA/AML compliance, establishing clear policies regarding the management of key BSA/AML risks, and ensuring that these policies are adhered to in practice.

The board should ensure that senior management is fully capable, qualified, and properly motivated to manage the BSA/AML compliance risks arising from the organization's business activities in a manner that is consistent with the board's expectations.

The board should ensure that the BSA/AML compliance function has an appropriately prominent status within the organization.

Senior management … and senior compliance personnel within the individual business lines should have the appropriate authority, independence, and access to personnel and information within the organization, and appropriate resources to conduct their activities effectively.

The board should ensure that its views about the importance of BSA/AML compliance are understood and communicated across all levels of the banking organization.

The board also should ensure that senior management has established appropriate incentives to integrate BSA/AML compliance objectives into management goals and compensation structure across the organization, and that corrective actions, including disciplinary measures, if appropriate, are taken when serious BSA/AML compliance failures are identified.

Criminal Penalties for Money Laundering, Terrorist Financing, and Violations of the BSA Penalties for money laundering and terrorist financing can be severe.

Civil Penalties for Violations of the BSA

The federal banking agencies and FinCEN, respectively, can bring **civil money penalty actions** for violations of the BSA.

Moreover, in addition to criminal and civil money penalty actions taken against them, **individuals may be removed from banking** for a violation of the AML laws as long as the violation was not inadvertent or unintentional. All of these actions are publicly available.

Criminal Penalties for Violation of Money Laundering, Terrorist Financing and the BSA

A person convicted of money laundering can face **up to 20 years in prison and a fine of up to $500,000**.

Any property involved in a transaction or traceable to the proceeds of the criminal activity, including property such as loan collateral, personal property, and, under certain conditions, entire bank accounts (even if some of the money in the account is legitimate), **may be subject to forfeiture.**

The U.S. Department of Justice may bring criminal actions for money laundering that may include criminal fines, imprisonment, and forfeiture actions. In addition, **banks risk losing their charters, and bank employees risk being removed and barred from banking**.

A person, including a bank employee, **willfully violating the BSA** or its implementing regulations **is subject to a criminal fine of up to $250,000 or five years in prison, or both**. **A person who commits such a violation while violating another U.S. law, or engaging in a pattern of criminal activity, is subject to a fine of up to $500,000 or ten years in prison, or both.**

A bank that violates certain BSA provisions, faces **criminal money penalties up to the greater of $1 million or twice the value of the transaction**.

First take away:
BSA AML and OFAC are at their core reporting and monitoring regulations.

Second take away:
the regulations have a detailed set of rules that govern how the data is used

- what data is collected,
- how it is reported
- how it is maintained
- how it is monitored and
- how it is updated
- how the bank acts on the collected data

A bank and its board of directors will be judged on how well they manage and act upon the reporting process.

Most prevalent ways banks get into BSA trouble:

- *Failure to file SARs and/or Follow Up SARs*
- *Failure to file CTRs and similar reporting*
- *Egregious failure to file other reports*
- *Failure to develop customer and bank risk profile*

- *Failure to have a written compliance program*
- *Failure to implement frequent, meaningful internal training*

- *Failure to have an independent audit*
- *Failure to have qualified BSA management*

- *Failure to grant independence to BSA management*

- *Failure to develop, implement and maintain BSA/AML/OFAC risk assessments.*

You are required by BSA/AML/OFAC regulations to file these 12 reports on a pre-defined scheduled or as an event occurs.

- Suspicious Activity Reporting
- Currency Transaction Reporting
- Currency Transaction Reporting Exemptions
- Information Sharing
- Purchase and Sale of Monetary Instruments Recordkeeping
- Funds Transfers Recordkeeping
- Foreign Correspondent Account Recordkeeping, Reporting and Due Diligence
- Private Banking Due Diligence Program (Non-U.S. Persons)
- Special Measures
- Foreign Bank and Financial Accounts Reporting
- International Transportation of Currency or Monetary Instruments Reporting
- Office of Foreign Assets Control

- Correspondent Accounts (Domestic)
- Correspondent Accounts (Foreign)
- Bulk Shipments of Currency
- U.S. Dollar Drafts
- Payable Through Accounts
- Pouch Activities
- Electronic Banking
- Funds Transfers
- Automated Clearing House Transactions
- Prepaid Access
- Third-Party Payment Processors
- Purchase and Sale of Monetary Instruments
- Brokered Deposits
- Privately Owned Automated Teller Machines
- Nondeposit Investment Products
- Insurance
- Concentration Accounts
- Lending Activities
- Trade Finance Activites
- Private Banking
- Trust and Asset Management Services
- Geographic locations of your customers
- In/Out of your market
- In/Out of the US
- Nonresident Aliens and Foreign Individuals
- Politically Exposed Persons
- Embassy, Foreign Consulate, and Foreign Mission Accounts
- Non-Bank Financial Institutions
- Professional Service Providers
- Non-Governmental Organizations and Charities
- Business Entities (Domestic and Foreign)
- Cash-Intensive Businesses

You are required to (1) know about and (2) monitor customers who are included in this list. More reports. More risk evaluation.

Focus on what's important

Implement a BSA/AML Risk assessment

Implement a BSA/AML risk assessment. Determine whether the bank has included all risk areas, including any new products, services, or customers, entities, and geographic locations. Determine whether the bank's process for periodically reviewing and updating its BSA/AML risk assessment is adequate.

Factors to develop a risk assessment:

- Purpose of the account.
- Actual or anticipated activity in the account.
- Nature of the customer's business/occupation.
- Customer's location.
- Types of products and services used by the customer.

If the bank has not developed a risk assessment, or if the risk assessment is inadequate, the examiner must complete a risk assessment.

Examiners should document and discuss the bank's BSA/AML risk profile and any identified deficiencies in the bank's BSA/AML risk assessment process with bank management.

Implement an OFAC risk assessment.

The OFAC risk assessment should consider the various types of products, services, customers, entities, transactions, and geographic locations in which the bank is engaged, including those that are processed by, through, or to the bank to identify potential OFAC exposure.

Have in place independent testing of its OFAC compliance program.

Review correspondence received from OFAC and, as needed, the civil penalties area on OFAC's Web site to determine whether the bank had any warning letters, fines, or penalties imposed by OFAC since the most recent examination.

Review correspondence between the bank and OFAC (e.g., periodic reporting of prohibited transactions and, if applicable, annual OFAC reports on blocked property).

Minimum Content of a BSA/AML/OFAC Compliance Program:

A written BSA/AML/OFAC policy and procedure describing how compliance will be achieved and maintained

•A system of internal controls to ensure ongoing compliance.

•Independent testing of BSA/AML compliance.

•Designate an individual or individuals responsible for managing BSA compliance (BSA compliance officer).

•Training for appropriate personnel.

BSA/AML/OFAC
Minimum Standard for Customer Information Profile (CIP)

The CIP must contain account-opening procedures detailing the identifying information that must be obtained from each customer. At a minimum, the bank must obtain the following identifying information from each customer before opening the account:

- Name.
- Date of birth for individuals.
- Physical Address
- Valid Photo ID
- Name of Beneficial Owner(s) for qualified legal entities
- In case a new account opened by a customer that is not an individual, the bank will obtain information about individuals with authority or control over such accounts, including signatories, in order to verify the customer's identity.

The CIP must include procedures for determining whether the customer appears on any federal government list of known or suspected terrorists or terrorist organizations.

Customer Due Diligence (CDD) supports monitoring of customer activity by establishing a baseline of “expected customer behavior.” Helps the bank identify suspicious activity.

CDD also forms the basis a Risk Profile.

Customer Due Diligence (CDD)

In accordance with regulatory requirements, all banks must develop and implement appropriate risk-based procedures for conducting ongoing customer due diligence, including, but not limited to:

At a minimum, the bank must establish risk-based CDD procedures that:

- Enable the bank to understand the nature and purpose of the customer relationship in order to develop a customer risk profile.
- Enable the bank to conduct ongoing monitoring
  - for the purpose of identifying and reporting suspicious transactions and,
  - on a risk basis, to maintain and update customer information, including information regarding the beneficial owner(s) of legal entity customers.

In addition, the bank’s risk-based CDD policies, procedures, and processes should:

- Be commensurate with the bank’s BSA/AML risk profile, with increased focus on higher risk customers.
- Contain a clear statement of management’s and staff’s responsibilities, including procedures, authority, and responsibility for reviewing and approving changes to a customer’s risk profile, as applicable.
- Provide standards for conducting and documenting analysis associated with the due diligence process, including guidance for resolving issues when insufficient or inaccurate information is obtained.

Higher Risk Profile Customers

Customers that pose higher money laundering or terrorist financing risks, (*i.e.,*higher risk profile customers), present increased risk exposure to banks.

As a result, due diligence policies, procedures, and processes should define what additional customer information will be collected, perhaps on a continuing basis, on the customer risk profile and the specific risks posed. This is known as Enhanced Due Diligence (EDD.)

The bank needs to understand different levels of risk:

A business customer who lives in Memphis (next to your Blossom office) with a money market account.

VS

An attorney practice with five lawyers (three of whom live in Nashville) with offices in Atlanta, Jacksonville as well as Knoxville, which has a Cash Management Account with ACH and Remote Deposit Capture

Based on the customer risk profile, the bank may consider obtaining, at account opening (and throughout the relationship), more customer information in order to understand the nature and purpose of the customer relationship, such as:

- Source of funds and wealth.
- Occupation or type of business (of customer or other individuals with ownership or control over the account).
- Financial statements for business customers.
- Location where the business customer is organized and where they maintain their principal place of business.
- Proximity of the customer's residence, place of employment, or place of business to the bank.
- Description of the business customer's primary trade area, whether transactions are expected to be domestic or international, and the expected volumes of such transactions.
- Description of the business operations, such as total sales, the volume of currency transactions, and information about major customers and suppliers.

Performing an appropriate level of ongoing due diligence that is commensurate with the customer's risk profile is especially critical in understanding the customer's transactions in order to assist the bank in determining when transactions are potentially suspicious. This determination is necessary for a suspicious activity monitoring system that helps to mitigate the bank's compliance and money laundering risks.

Customer Profile Work Sheet for some "potentially higher risk accounts"

Ongoing Monitoring of the Customer Relationship

The requirement for ongoing monitoring of the customer relationship reflects existing practices established to identify and report suspicious transactions and, on a risk basis, to maintain and update customer information.

Therefore, the bank's CDD program must include risk-based procedures

- for performing ongoing monitoring of the customer relationship, on a risk basis,
- to maintain and update customer information, including beneficial ownership information of legal entity customers.

The process is risk-driven. Should the bank become aware as a result of its ongoing monitoring that customer information, including beneficial ownership information, has materially changed, it should update the customer information accordingly.

What monitoring is looking for:

1. **Most common reason monitoring bells get triggered**:

Transactions or other activity that are inconsistent with the bank's understanding of the nature and purpose of the customer relationship or with the customer risk profile.

2. **Other reasons alarms go off:**

- Significant and unexplained changes in account activity
- Changes in employment or business operation
- Changes in ownership of a business entity
- Red flags identified through suspicious activity monitoring
- Receipt of law enforcement inquiries and requests such as criminal subpoenas, National Security Letters (NSL), and section 314(a) requests
- Results of negative media search programs
- Length of time since customer information was gathered and the customer risk profile assessed

Suspicious Activity Reports (SARs)

Suspicious activity reporting forms the cornerstone of the BSA reporting system. It is critical to the United States' ability to utilize financial information to combat terrorism, terrorist financing, money laundering, and other financial crimes.

Banks should recognize that the quality of SAR content is critical to the adequacy and effectiveness of the suspicious activity reporting system.

Banks, bank holding companies, and their subsidiaries are required by federal regulations to file a SAR with respect to:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating $5,000 or more when a suspect can be identified.
- Criminal violations aggregating $25,000 or more regardless of a potential suspect.
- Transactions conducted or attempted by, at, or through the bank (or an affiliate) and aggregating $5,000 or more, if the bank or affiliate knows, suspects, or has reason to suspect that the transaction:
  - May involve potential money laundering or other illegal activity (e.g., terrorism financing). Is designed to evade the BSA or its implementing regulations.
  - Has no business or apparent lawful purpose or is not the type of transaction that the particular customer would normally be expected to engage in, and the bank knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

Immediate Release
September 23, 2013
WASHINGTON, DC – The Financial Crimes Enforcement Network (FinCEN) today announced the assessment of a $37.5 million civil money penalty against TD Bank, N.A. for failure to file suspicious activity reports related to the massive Ponzi scheme orchestrated by Florida attorney Scott Rothstein. The Office of the Comptroller of the Currency also announced the assessment of a concurrent $37.5 million penalty against the Bank for related violations. Additionally, the Securities and Exchange Commission has assessed a separate $15 million penalty against the Bank for related securities violations.

A transaction includes

- a deposit;
- a withdrawal;
- a transfer between accounts;
- an exchange of currency;
- an extension of credit;
- a purchase or sale of any stock, bond, certificate of deposit, or other monetary instrument or investment security;
- or any other payment, transfer, or delivery by, through, or to a bank.

Identification of Unusual Activity
How the Examiner evaluates a bank's SAR Reporting process

Review the bank's policies, procedures, and processes for identifying, researching, and reporting suspicious activity. Determine whether they include the following:

- Lines of communication for the referral of unusual activity to appropriate personnel.
- Designation of individual(s) responsible for identifying, researching, and reporting suspicious activities.
- Monitoring systems used to identify unusual activity.
- Procedure to file and/or decline to file SAR
- Review documentation supporting reporting or not filing
- Procedures for reviewing and evaluating the transaction activity of subjects included in law enforcement requests or National Security Letters (NSLs)) for suspicious activity. NSLs are highly confidential documents; as such, examiners will not review or sample specific NSLs. Instead, examiners should evaluate the policies, procedures, and processes for:
    - Responding to NSLs.
    - Evaluating the account of the target for suspicious activity.
    - Filing SARs, if necessary.
    - Handling account closures.

BSA/AML/OFAC
Regulatory Expectations of Bank Boards of Directors:

Protect your bank and the financial system.
It's a big job. Severe penalties for non-compliance.
Focus on what's important

Let's summarize: The Five Most Important Things a Director Needs to Know about BSA/AML/OFAC

1. **Implement and continually update BSA/AML and OFAC risk assessment**

2. **A written BSA/AML/OFAC policy and procedure describing how compliance will be achieved and maintained**
   - **A system of internal controls to ensure ongoing compliance.**
   - **Independent testing of BSA/AML compliance.**
   - **Designate an individual or individuals responsible for managing BSA compliance (BSA compliance officer).**
   - **Training for appropriate personnel.**
3. **Develop a robust , tailored to your bank, continually updated**
   - **Customer Information Profile (CIP) procedure**
   - **Customer Due Diligence (CDD) procedure**
   - **Enhanced Due Diligence (EDD) procedure for high risk customers**
4. **Focus on Suspicious Activity Monitoring and Reporting**

BSA/AML/OFAC
Regulatory Expectations of Bank Boards of Directors:

Protect your bank and the financial system.
It's a big job. Severe penalties for non-compliance.
Focus on what's important

Whew! That was a lung-breaker.

Thank You for Your Time and Attention.

Any Questions?