BSA/AML Training Series

Frontline & Operations Staff

Why does this matter?

- Serious consequences for non-compliance:
  - Enforcement actions
  - Civil Money Penalties (CMPs)
  - Bank charter revocation

Today's Objectives

- Overview of BSA/AML requirements
- Four pillars of BSA/AML Program
- BSA/AML requirements applicable to your role as frontline & operations staff
- Red Flags to watch out for in your daily work

Four Pillars

- Designated BSA Compliance Officer
- Internal Policies, Procedures, & Controls
- Training (annual and on-going)
- Independent Testing & Audit

BSA Officer

- Appointed by the Board
- Responsible for managing the BSA/AML compliance program
- Contact your BSA/AML officer with any questions about BSA/AML processes, procedures, and policies

Internal Controls

- Internal controls are the policies, procedures, and controls designed to address BSA/AML risks at your bank
  - Internal controls are developed & implemented to comply with BSA laws & requirements
- Internal controls will depend on size, products, services, and geographic area of the bank, and as a result they will look different at different banks
- Examples of internal controls – identify cash transactions greater than $10,000; check for potential OFAC matches; monitor transaction activity for suspicious behavior

Training

- Training tailored to employee's specific responsibilities
- Frontline & operations staff need different training than lending staff
  - You need to know about BSA issues affecting account opening, deposits, withdrawals, ACH, wires, & other deposit and operational areas
- Training must occur at least annually, but many banks provide ongoing BSA training

Independent Audit

- Audit verifies whether the bank's BSA program is effective and compliant with BSA & AML laws and regulations
- Can be conducted by internal audit, outside auditors, consultants, or other qualified independent third parties
- Reflects the bank's BSA/AML risk profile

BSA/AML Requirements

- Customer Identification Program
- Customer Due Diligence & Enhanced Due Diligence Procedures
- Currency Transaction Reporting & Exempt Customers
- Monetary Instrument Record Keeping
- Suspicious Activity Reporting
- OFAC screening & monitoring
- Information sharing practices under sections 314(a) and 314(b), and
- Record Retention.

Customer Identification Program

- CIP required under section 326 of the USA PATRIOT Act
- Written CIP program required based on the bank's size & risk profile, and applies to all new customers
- Banks to form a reasonable belief as to the customer's true identity
- Minimum information required:
  - Name,
  - DOB (for individuals),
  - Address (no P.O. boxes), &
  - Identification number (e.g. SSN, EIN, etc.)
- Verify the identity of each customer
- Check OFAC
- Notice to customer – describing bank's identification requirements
- Opening a new customer account without the required CIP information results in a CIP error or violation.

Customer Due Diligence

- Allows the bank to understand the customer's expected transactional activity
- Allows the bank to determine the expected profile and risk rating of customer
- Forms a basis for determination whether transaction activity is normal or unusual for that customer
- Customer Due Diligence applies to all customers
- Starting on May 11, 2018 banks will be required to identify & verify the identity of the beneficial owners of all legal entity customers at the time a new account is opened

Enhanced Due Diligence

- Enhanced Due Diligence applies to customers identified as posing higher money laundering or terrorist financing risk
- For these customers, gather additional information at account opening:
  - Purpose of account, source of funds, type of business or occupation, expected activity & volume (cash deposits & withdrawals, wires & international wires), etc.
- Ongoing monitoring process – customer account profiles must be current and monitoring efforts should be based on risk

Currency Transaction Reporting

- Must file Currency Transaction Reports for transactions in excess of $10,000 (in cash or coin)
- If multiple transactions aggregate to over $10,000 in a day – file a CTR
- CTRs must be filed electronically within 15 calendar days of the transaction
- Reportable transactions
  - Currency deposits
  - Currency withdrawals
  - Currency exchanges
  - Other Payments & Transfers in cash
  - Aggregate multiple transactions
- Have multiple deposits occurred in different branches? – A SAR may need to be considered, so notify your BSA Officer

Currency Transaction Reporting (continued)

- Cash transactions must be aggregated
- Armored Car Service (ACS) – controls to determine on whose behalf ACS is acting (e.g. bank's, customer's, 3rd party's)
- Name of Armored Car Service employee is not required by FinCEN
- See FIN-2014-R010 – Application of FinCEN Regulations to Currency Transporters, Including Armored Car Services

Currency Transaction Reporting (continued)

- ***Commonly-owned businesses*** – if the bank has information that separately incorporated businesses are not operating independent of each other or their common owner, CTR aggregation is required
- ***Example***:
  - Abby Jones owns 2 businesses – A & B, with separate tax ID numbers
  - Both businesses frequently conduct large cash transactions
  - Funds from Business A are used to routinely cover payroll at Business B

In this example, the activity indicates Business A and Business B may overlap their transaction activity and the bank would be required to aggregate cash transactions of both businesses onto one CTR for filing purposes.

Structuring

- Breaking up of currency transactions to evade BSA reporting requirements
- If thresholds are met – should be reporting as a suspicious transaction
- Structuring is per-se illegal – even if the currency has been legally obtained, if structuring occurs, it should be reported on a SAR
- Most common illegal activity occurring at banks
- When structuring occurs, you should file a SAR, or a CTR *and* a SAR, as applicable.

Structuring (continued)

Example 1 – A customer comes into the bank to deposit $11,000 in cash. As you start gathering the needed information to file a currency transaction report, the customer states that he does not have time for all of this and decides to only deposit $9,000.

This is structuring. A currency transaction report would not be filed in this situation. Remember, the transaction must be over $10,000 in cash for filing a CTR. However, because this is overt structuring, a suspicious activity report would need to be filed.

Structuring (continued)

Example 2 – A customer withdraws $8,000 in cash at Branch A. Then immediately thereafter, drives over to Branch B and withdraws additional $5,000. The aggregated cash transaction is $13,000. What do you do?

A currency transaction report must be filed because the aggregated cash withdrawal exceeds the filing threshold. This smells like intentionally structured withdrawal activity – the customer drove to two different branches to withdraw the cash. A suspicious activity report would also need to be filed unless information could be identified that indicated a legal and legitimate reason for the consecutive cash withdrawals.

Currency Transaction Reporting - Exemptions

Phase I exemptions

- Banks
- Departments & agencies of the U.S. government
- Departments & agencies of State government
- Political subdivisions
- Listed corporations whose common stock is listed on NYSE, AMEX, or NASDAQ
- Subsidiaries of listed corporations

Franchises are private & do not fall under Phase I exemption

Currency Transaction Reporting - Exemptions

Phase II exemptions

- Non-listed businesses that meet the following criteria:
  - Maintained a transaction account at the bank for at least 2 months
  - Frequently engages in transactions in currency exceeding $10,000
  - Is incorporated or organized under the laws of the U.S. or a State, and
  - Is not identified as an ineligible entity by federal agencies
- Examples of non-listed businesses that cannot be exempted:
  - Purchase or sale of motor vehicles of any kind, vessels, aircraft, farm equipment, etc.
  - Pawn brokerage
  - Real estate brokerage,
  - Title insurance companies.
- Sole proprietors – eligible for exemption if account is used only for business purposes & they satisfy the same Phase II criteria as other exempt business customers

Monetary Instrument Record Keeping

- Monetary instruments include – cashier's checks, money orders, traveler's checks, foreign drafts
- Verify identity of monetary instrument purchasers when purchase value falls between $3,000 and $10,000
- Contemporaneous purchases of the same or different types of instruments totaling $3,000 or more must be treated as one purchase
- Records of sales must be maintained

Monetary Instrument Record Keeping

Accountholder

- Name of Purchaser
- Date of Purchase
- Type of Instrument purchased (e.g. cashier's check)
- Serial number of each instrument purchased
- Dollar amount of each instrument
- Identification verification

Non-Accountholder

- Name & Address of Purchaser
- Social Security Number or Alien ID Number
- Date of Birth
- Date of Purchase
- Type of instrument purchased
- Serial number of each instrument purchased
- Dollar amount of each instrument
- Verification of name & address of purchaser

Monetary Instrument Record Keeping

Red Flags for Sales of Monetary Instruments

- Sales of sequentially numbered monetary instruments;
- Sales of monetary instruments to the same purchaser or to different purchasers made payable to the same remitter;
- Money instrument purchases by noncustomers;
- Common purchasers, payees, addresses, sequentially numbered purchases, and unusual symbols
- Customer purchases a number of cashier's checks, money orders, or traveler's checks for large amounts under a specific threshold
- Monetary instruments deposited by mail are numbered sequentially or have unusual symbols or stamps on them

Fund Transfers

- Allow to quickly transfer funds
- Attractive method to hide the source of funds
- Banks must collect & retain some information for funds transfers of $3,000 or more
- Recordkeeping requirements differ based on whether the bank is an originator, intermediary, or the beneficiary bank

Fund Transfers – Record Keeping Requirements

Originating Bank

- Name & address of originator
- Amount of payment order
- Date of payment order
- Any payment instructions
- Identity of the beneficiary's institution
- As many of the following items as are received with the payment order:
  - Name & address of beneficiary
  - Account number of the beneficiary
  - Any other identifier of the beneficiary
- Records required for non-customers:
  - Name & address of person placing the transfer order
  - Identification Type (if in person)
  - Identification Number (if in person)
  - TIN, Alien Identification Number, or note that none was available

Intermediary Bank

- Name & account number of transmittor
- Address of transmittor
- Amount of transmittal order
- Date of transmittal order
- Identity of the recipient's institution
- As many of the following items as are received with the transmittal order:
  - Name & address of the recipient
  - Account number of the recipient
  - Any other specific identifier of the recipient
- Either name & address or the numerical identifier of the tranmittor's financial institution

Beneficiary Bank

- If proceeds delivered in person – must verify the identity of the person receiving the proceeds:
  - Name & address
  - Type of document reviewed
  - Number of the identification document
  - The person's TIN, or Alien Identification Number, or passport number & issuing country, or a note that none was available
- If proceeds not delivered in person:
  - Retain a copy of the check/instrument used to disburse the funds; or
  - Record the information on the check/instrument; and
  - Record the name & address of the person to whom the check/instrument was sent

Fund Transfers – Record Retention

- Records must be retained for 5 years
- Must be retrievable by name
- If existing customer, must be retrievable by account number

Office of Foreign Assets Control (OFAC)

- OFAC – part of the U.S. Department of the Treasury
- Administers & enforces economic & trade sanctions based on U.S. foreign policy objectives & national security goals against targeted:
  - Foreign countries & regimes;
  - Individuals;
  - Entities; and
  - Practices
- OFAC requirements apply to all U.S. persons
- Your bank has its own set of OFAC policies & controls addressing the procedures you must follow to complete OFAC searches.

Office of Foreign Assets Control (OFAC)

- OFAC is a strict liability law – if a bank facilitates a transaction for a person/entity on the OFAC list, the bank will be in violation of OFAC laws & sanctions
- OFAC procedures & controls are based on the bank's risk profile

Office of Foreign Assets Control (OFAC)

- All types of financial transactions are subject to OFAC restrictions, including:
  - Deposit Accounts (checking, savings, etc.)
  - Safe Deposit Boxes
  - Wire & ACH transfers
  - Currency Exchanges
  - Purchase of monetary instruments
  - Trust Accounts
  - Credit Cards
- Refer to your bank's OFAC procedures for direction on when & how to screen for potential OFAC matches

OFAC – Blocked Transactions

- If OFAC true match – bank must either block or reject the transaction
- Transactions to be blocked:
  - Made by or on behalf of a blocked individual or entity
  - Made to or go through a blocked entity, or
  - Made in connection with a transaction in which a blocked individual or entity has an interest.
- File blocking report:
  - within 10 business days of the occurrence of a blocked transaction, and
  - Annually by September 30th reporting on assets blocked as of June 30th of that year.
- Place blocked funds/assets in a separate blocked account
- Keep a full record of blocked property, including blocked transactions:
  - For the period the property is blocked, and
  - 5 years after the date the property is unblocked

OFAC – Prohibited Transactions

- Transactions may be prohibited, but no blockable interest exists
- Don't accept the transaction (reject it), but there is no need to block the asset
- Report rejected transactions to OFAC within 10 business days of when the transaction occurred
- No annual reporting of rejected transaction is required
- Keep full record of each rejected transaction for 5 years of when the transaction occurred

Information Sharing – 314(a)

- Section 314(a) addresses information sharing between law enforcement & financial institutions
- Law enforcement agencies may request FinCEN to solicit information from banks
- Conduct a one-time search of bank records to identify accounts or transactions for an individual or entity included in FinCEN's request
- Banks must implement policies, procedures, and processes for responding to 314(a) requests accurately & timely
  - Within 14 days from FinCEN request
- Information in FinCEN 314(a) requests is strictly confidential
- Keep documentation that all required searches were performed
- Based on feedback from law enforcement, 95% of 314(a) requests have contributed to arrests or indictments

Information Sharing – 314(b)

- Banks may request to share information with other banks under section 314(b)
- Banks who want to share, must first certify to FinCEN that they will do so according to 314(b) requirements
- Information about SAR filings cannot be discussed under the auspices of 314(b)

Money Laundering

- ***Placement*** – placing illegal money into a financial institution like your bank; placement occurs through deposits of cash, purchase of monetary instruments, or structuring deposits into an account;
- ***Layering*** – occurs when a fraudster attempts to separate the funds from the illegal activity by moving the money around & through the financial system.
  - Examples of activity: funds transfers, withdrawals from one bank & deposits into another bank, purchase & negotiations of monetary instruments, etc.
- ***Integration*** – the ultimate goal of fraudsters; illegal funds appear to be fully integrated into the mainstream financial system; laundered funds are ready to be disbursed back to the fraudster or criminal.

Suspicious Activity Monitoring

- Monitoring, identifying, and reporting suspicious activity are regulatory requirements
- Suspicious Activity Reports (SARs) are filed for unusual or suspicious activity, e.g. terrorist financing, tax evasion, elder abuse, identity theft, fraud, structuring, account takeovers, human trafficking and smuggling, funnel account activity, and many more.
- Not investigating a crime, just notifying authorities of account activity and explaining why that activity is unusual or suspicious.
- Reporting of activity is important because it may provide a link for law enforcement to solve an ongoing crime.

Suspicious Activity Monitoring

- Suspicious Activity Reports (SARs) must be filed for the following transactions:
  - Transactions that involve insider abuse in any amount;
  - Transactions aggregating $5,000 or more when a suspect can be identified; and
  - Transactions aggregating $25,000 or more regardless of a potential suspect.
- SAR can be filed for transactions that aggregate to less than the listed amounts
- Speak with your bank's BSA Officer to discuss your bank's policies & procedures

Red Flags

1. Customers provide insufficient or suspicious information when opening accounts, purchasing monetary instruments, etc.

- Customer uses fake, unusual, or suspicious documents
- Customer uses different taxpayer identification numbers with variations of his or her name
- Business customer does not want to provide complete information about the nature and purpose of its business, anticipated account activity, names of its officers and directors, or business location
- Two or more customers use similar identification documents

Red Flags

2. Efforts to avoid reporting or recordkeeping requirements – this may be structuring, and as we discussed above, structuring is per se illegal and you should refer any incident to your BSA officer or a designated person

- Customer is reluctant to provide information needed to file a mandatory report
- Customer tries to persuade bank employee not to file required reports, such as a Currency Transaction Report
- Business or customer asks to be exempted from reporting or recordkeeping requirements
- Customer accesses a safe deposit box after completing a transaction involving a large withdrawal of currency, or accesses a safe deposit box before making currency deposits in structured amounts to evade CTR filing requirements
- Customer is reluctant to provide identification when purchasing monetary instruments in recordable amounts (be especially aware of nonaccount holders who want to purchase monetary instruments but don't want to provide the required information)

Red Flags

3. Activity inconsistent with the customer's business

- Retail business has dramatically different patterns of cash deposits from similar businesses in the same area
- Unusual funds transfers occurring between related accounts
- Unusual funds transfers occurring between unrelated accounts (may be same owner)
- Goods or services purchased by business customer do not match the customer's stated line of business
- Sudden change in transaction activity inconsistent with type of business

Red Flags

4. Funds Transfer Red Flags

- Numerous funds transfers sent in large, round dollar amounts
- Funds transfers occur to/from financial secrecy havens or to/from higher-risk geographic locations without a business reason or when the activity is out of norm for the customer's business type or transaction history
- Small incoming funds transfers are received and almost immediately most are wired to another bank or country (inconsistent with business and/or transaction history)
- Funds transfer activity is unexplained, repetitive, or shows unusual patterns

Red Flags

5. Automated Clearing House Transactions (ACH)

- Multiple layers to third-party service providers that appear to be unnecessarily involved in transactions
- Unusually high number of transactions initiated over the Internet or by phone
- Monitor third-party service providers with history of violating ACH network rules or generating illegal transactions

Red Flags

6. Other Suspicious Customer Activity

- Customer repeatedly uses a branch location that is located far from the customer's home or office without sufficient business or personal purpose
- Customer opens an account and conducts large and frequent deposits and withdrawals during a short period of time, then closes the account or the account becomes dormant
- Multiple debit cards associated with an account
- Customer makes frequent or large transactions, but has no record of past or present employment

Case Scenario

You get an email from what appears to be a President of a business customer. In the email, the customer requests that a wire be sent to a vendor in a foreign country. The customer also writes that he will be unavailable for the next 24 hours and all communication must be done over email. What do you do? Do you become suspicious?

SARs & Red Flags

- Find more information about money laundering and terrorist financing red flags on the Financial Crimes Enforcement Network website: https://www.fincen.gov/
- SAR filings are CONFIDENTIAL!

BSA/AML Training Series

Frontline & Operations Staff