BSA/AML Training Series

Lenders & Lending 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 position as lending 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
- Lending staff need different training than frontline & operations staff
    - You need to know about BSA issues affecting loan origination, etc.
- 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

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
- All types of financial transactions are subject to OFAC restrictions, including:
  - New Loans
  - Lines of credit
  - Letters of credit
  - Deposit Accounts (checking, savings, etc.)
  - Wire & ACH transfers
  - Credit Card advances
- 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

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 days of the transaction
- Reportable transactions include cash loan payments & cash loan draws

Anti-Money Laundering

- Banks are required to establish controls to monitor, identify, and report unusual and suspicious activity
- Key component of BSA program – the bank's anti-money laundering efforts
- Money laundering is the criminal act of taking illegally derived funds (or "dirty" money) & initiating a series of transactions to make the funds appear "cleaned" or look like legal funds.
- Money laundering involves cash & other vehicles to move money
- Money laundering often is a complex series of transactions where money moves across the globe

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

- Suspicious Activity Reports (SARs) are filed for unusual or suspicious activity, e.g. terrorist financing, tax evasion, elder abuse, identity theft, fraud, structuring, account take overs, 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 misrepresented information prior to and/or at loan origination
   - Customer uses fake identification documents
   - Customer provides incorrect social security numbers or different taxpayer identification numbers with variations of his or her name
   - Customer provides inconsistent signatures on collateral documents
   - Customer misrepresents occupancy status
   - Customer misrepresents income or employment
   - Customer provides false statements related to ownership of collateral interests
   - 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

Red Flags

2. Common red flags for mortgage fraud
   - Residential real estate interest taken in non-arm's length transaction –this situation is indicative of a straw buyer & involves purchase of home from a family member, friend, or employer/employee;
   - Applicant purchases another home in the same community as the existing residence without any reasonable explanation for doing so;
   - Short sale fraud or collusion
   - Misrepresented purpose for loan proceeds
   - Illegal debt elimination with the use of newly originated loan

Red Flags

3. Other Suspicious Customer Activity
   - Customer repeatedly uses a branch location that is distant from the customer's home or office without sufficient business or personal purpose
   - Loans are secured by pledged assets held by third parties unrelated to the borrower
   - Borrower requests that loan proceeds be disbursed to unrelated third party
   - Sudden large payment on defaulted loan
   - Delinquencies related to cash-secured loans, or
   - Sudden change in business or transaction activity that is inconsistent with the type of business stated by the borrower.

Red Flags – Emerging Trends

- ***Loan overpayments*** - Loan customers make large overpayments on their loans to pay them off; this activity triggers the bank to issue a refund check for the overpayment making the funds appear legitimate
- ***Bust out schemes*** – perpetrators look like regular customers; apply for credit; keep the account current while increasing the credit limits; then they rapidly increase spending & build balances; then they allow the loans to go delinquent
- ***Crowdfunding hoax*** – regular borrowers may become the targets of fraudsters who claim to work for crowdfunding platforms & charging the borrowers high fees upfront
- Loan transactions & loan repayment activity that have no apparent economic, business, or lawful purpose

BSA/AML Training Series

Lenders & Lending Staff