BSA/AML Training Series

BSA Officers & Staff

Why does this matter?

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

Agenda

- Principles of BSA/AML
- Your role in BSA/AML program success
- BSA/AML issues with which banks struggle
- Emerging industry trends
- Program updates
- Enforcement Actions

BSA/AML Program

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

BSA Compliance Officer

- Appointed by the Board
- Knows & understands BSA and AML regulations
- Understands bank's products and services
- Has direct line of communication with the Board of Directors and Senior Management

Internal Controls

- Policies / Procedures / Controls
- Type of controls depends on the size & scale of bank
- Includes BSA/AML Risk Assessment
  - Products, services, customer base, bank's geographic locations, & implemented internal controls
- BSA Officer should inform the Board of Directors & Senior Management of BSA compliance initiatives, deficiencies, & corrective actions
- Examples of internal controls - identify cash transactions greater than $10,000; check for potential OFAC matches; monitor transaction activity for suspicious behavior

Training

- No proper training = Potential money laundering or terrorist financing risk
- Tailored to employees' specific responsibilities
  - For example – BSA/AML training for Lenders will look different than BSA/AML training for Tellers
- Cover – internal policies, procedures, monitoring systems, and any changes
- Some employees may require more frequent training (than once a year)
- Document all training and employee attendance

Independent Audit

- Verification of whether:
  - the BSA compliance program works well; and
  - the BSA compliance program complies with the law
- Conducted by either:
  - Bank's Internal Audit department
  - Outside auditors or consultants; or
  - Other qualified independent third party
- Sound practice to conduct an independent audit every 12-18 months
- Should reflect the bank's BSA/AML risk profile
- Audit results must be reported to the Board of Directors or to a designated Board committee

Risk Assessment

- Assists in identifying BSA/AML risk profile for your bank
- Rely on the Risk Assessment to design & implement controls to mitigate inherent risk
- Identify specific risk categories within bank
- Biggest risk categories – customers, products & services, and geography
- Quantify the categories (e.g. number of customers, number & location of branches, etc.)
- Update annually or as your bank's risk changes

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
- Have multiple deposits occurred in different branches? – A SAR may need to be considered
- Reportable transactions
  - Currency deposits
  - Currency withdrawals
  - Currency exchanges
  - Other Payments & Transfers in cash
  - Aggregate multiple transactions

Currency Transaction Reporting (continued)

- Cash transactions are 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 the 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.

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 is between $3,000 and $10,000, inclusive
- 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
  - Maintain records on a purchase form, a central log, or within a deposit platform system

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

Funds 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

Intermediary 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

Beneficiary 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

Originating 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

Funds Transfers – Record Retention

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

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) 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
- Procedures should outline how bank will address recurring SAR filings, escalation process, & account closure
- Report overall SAR activity to the Board of Directors

Suspicious Activity Processes

- Five key components of suspicious activity monitoring and reporting systems:
  - Identification of unusual activity
  - Alert management
  - SAR decision making
  - SAR completion & filing
  - Monitoring & SAR filing on continuing activity
- Interdependent components & should be successfully implemented
- Breakdown in one or more of the components may adversely affect SAR reporting and BSA compliance

Suspicious Activity Processes - Identification

- To identify potential money laundering & terrorist financing activity, look for red flags or unusual/suspicious behaviors
- Identification channels include:
  - Employees identify activity/behavior during daily operations
  - Law enforcement submits inquiries and requests (e.g. 314(a) requests)
  - Regulator issued advisories
  - Transaction monitoring processes

Suspicious Activity Processes – Alert Management

- Alert management – the processes used to investigate & evaluate identified unusual activity
  - Have an escalation process, so employees can refer identified unusual activity from all business lines
- Investigative staff needs access to internal & external tools to allow them to properly research the activity
  - For example – core account systems, account information, CDD & EDD information
- Once the unusual activity has been analyzed, make a decision whether or not to file a SAR & document that decision

Suspicious Activity Processes – Alert Management

- 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 Processes – SAR Filing

- File complete & accurate SARs
- Sufficiently describe the reported activity & include the basis for filing
- SARs must be filed electronically through the BSA E-Filing System
- File SARs timely:
  - 30 calendar days from the date of the initial detection of facts that form a basis for filing
  - If no suspect can be identified, you have 60 days to file a SAR
- The 30 day clock does not start to tick until a review is conducted & the bank makes a determination that the transaction is suspicious

Suspicious Activity Processes – Continuing SARs

- If suspicious activity continues after you file a SAR, the continuing activity must be shared with law enforcement by filing continuing activity SARs
- Filed after a 90 day review with the filing deadline of 120 calendar days after the date of the previously filed SAR
- Example:
  - Original SAR filed on July 16, 2016
  - Suspicious activity continues
  - Continuing SAR must be filed by November 13, 2016
- Of course, banks may file continuing SARs earlier than the 120 day deadline

Suspicious Activity Processes – Continuing SARs

- Develop & implement policies, procedures & processes to address issues identified as the result of repeat SAR filings
- In your policies and procedures include:
  - Review by senior management and/or legal staff (e.g. BSA officer or SAR committee);
  - Criteria for when analysis of the overall customer relationship is necessary;
  - Criteria for whether and when to close an account; and
  - Criteria for when to notify law enforcement, if appropriate.

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 staff 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
- Assess your bank's exposure to potential OFAC violations and mitigate that liability

Office of Foreign Assets Control (OFAC)

- All types of financial transactions are subject to OFAC restrictions, including:
  - Deposit Accounts (checking, savings, etc.)
  - Loans
  - Lines of credit
  - Letters of credit
  - Safe Deposit Boxes
  - Wire & ACH transfers
  - Currency Exchanges
  - Purchase of monetary instruments
  - Trust Accounts
  - Credit Cards
- Ensure OFAC procedures outline when & how the bank screens 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

OFAC – Compliance Program

- BSA/AML Examination Manual strongly encourages banks to establish & maintain a written OFAC compliance program, based on the bank's OFAC risk profile
- Effective OFAC compliance program includes internal controls to:
  - Identify suspect accounts & transactions, and
  - Reporting blocked & rejected transactions

OFAC – Compliance Program

- OFAC compliance program should address the following:
  - Identify high-risk business areas and potential sanction exposure for your bank;
  - Provide appropriate internal controls for screening, reporting, recordkeeping, due diligence, and regular updates to the program;
  - Include OFAC in independent audits for compliance;
  - Designate a bank employee for OFAC compliance (this generally is the same person who is also the BSA officer for a bank);
  - Create and implement training programs.

Information Sharing – 314(a)

- Section 314(a) addresses information sharing between law enforcement/FinCEN and 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)

Section 311 Special Measures

- Secretary of the Treasury may require domestic financial institutions to take special measures against foreign jurisdictions, foreign financial institutions, classes of international transactions, types of accounts of primary money laundering concern
- First through Fifth Special Measure – see pages 138 & 139 of the BSA/AML Examination Manual for more detailed requirements of each special measure
- See https://www.fincen.gov/statutes_regs/patriot/section311.html for current Section 311 Special Measures
- Develop, document, & implement appropriate procedures to address Section 311 special measures

Virtual Currency

- Virtual currency (digital currency) is a medium of exchange on the internet & is not authorized or adopted by the United States government.
- Variety of different virtual currencies used, most commonly known is Bitcoin;
- FinCEN guidance (FIN-2013-G001) clarified how the BSA regulations apply to "convertible virtual currency;"
- 2014 BSA/AML Examination Manual – BSA requirements & supervisory expectations for providing banking services to administrators or exchangers of virtual currencies are the same as for money transmitters
- Blockchain – public ledger or distributed database of transactions in electronic form; allows for an anonymous exchange of assets

Third-Party Payment Processors

- Third-Party Payment Processors provide payment-processing services to merchants & other business entities;
- Use their bank accounts to conduct payment processing for their customers;
- Processors may deposit remotely created checks on behalf of their clients, or process ACH transactions
- Bank has no direct relationship with the processor's clients, yet processors may serve international & high risk businesses
- 3rd-Party Payment Processors may expose the bank to illegal transactions, money laundering, and fraud risk because the processors are not subject to BSA/AML requirements

Rewards-based Crowdfunding

- Method to pool funds relying on internet campaigns to solicit contributions/donations from a large number of individuals;
- Campaign creator does not know most of the contributors;
- Goal is to raise money for a specific business venture, personal cause, or project;
- Most beneficiaries of crowdfunding are legitimate, however crowdfunding can be abused;
- SARs must be filed on unusual/suspicious transactions involving crowdfunding funds

Funnel Account Activity

- ***Funnel account*** – individual or business account that receives multiple cash deposits, often in amounts below the cash reporting threshold, in one geographic area, and from which the deposited funds are almost immediately withdrawn in a different geographic area;
- Smaller national or regional banks are also affected:
  - Bank branches located in different geographic areas, esp. near international borders
- Have a process to identify these types of transactions & file SARs as necessary
- For more details on Funnel Accounts & Trade-Based Money Laundering, see FinCEN Advisory FIN-2014-A005.

Marijuana Banking

- Marijuana use still illegal under federal laws;
- "Cole Memo" includes 8 Department of Justice marijuana enforcement priorities
- FinCEN guidance (FIN-2014-G001) clarified customer due diligence expectations and reporting requirements for those financial institutions providing services to marijuana businesses;
- Deciding whether to provide banking services to marijuana businesses?
  - Understand federal and state law
  - Understand FinCEN's guidance
  - Understand the structure & workings of the business you will bank
  - Understand the potential issues you may face from your regulators and/or federal law enforcement

Customer De-Risking

- De-risking refers to banks closing accounts of clients considered "high-risk" and exiting these relationships;
- Banks also are exiting higher risk products and markets to reduce their exposure to potential financial crime;
- Banks are concerned about BSA compliance risks associated with the high-risk relationships;
- Examples of de-risked clients – money service businesses, embassies, nonprofit organizations, etc.
- Regulators have not provided a clear message regarding de-risking;
- Consider the question of de-risking from a strategic point of view at the Board level & fully document decision in Board meeting minutes

CIP and Prepaid Cards

Type of Card	Who Loads Funds	Customer
General Purpose	Reloadable	Cardholder
General Purpose	Not Reloadable	3rd Party Program Manager
Payroll Cards	Employer is the only person that may deposit funds into the account	Employer/Accountholder
Payroll Cards	Employee is able to access credit through the card or add funds to the card outside of the employer	Employee/Cardholder
Government Benefit Cards	Only the government agency can load funds	No CIP required
Government Benefit Cards	The beneficiary/cardholder can load funds and/or access credit	Beneficiary/Cardholder
Health Benefit Cards (FSAs & HRAs)	Only employer loads funds	Employer/Accountholder
Health Benefit Cards (HSAs)	Established by employee; employee or employer may load funds	Employee/Cardholder

CIP and Prepaid Cards

- For additional information on CIP requirements and their application to Prepaid Cards, see https://www.fdic.gov/news/news/financial/2016/fil16021a.pdf
- You can also read the ICBA summary of the rule, here: https://www.icba.org/files/ICBASites/PDFs/SummaryofCIPGuidancePrepaidCards5-4-16.pdf

Customer Due Diligence Final Rule

- Bank must know the identity of the individuals who own or control the business (beneficial owners)
- Must identify & verify the identity of the beneficial owners of all legal entity customers at account opening
- Must maintain records of beneficial ownership
- Must monitor & maintain updated customer information to identify suspicious activity
- Must comply with the requirements by May 11, 2018
- Must obtain beneficial ownership information for existing customers, IF, during regular monitoring the bank detects information relevant to reevaluating the risk of the existing customer
- Determination of beneficial owner based on two-prong test:
  - ***Ownership Prong*** – owns 25% or more of the equity interests of the company
  - ***Control Prong*** – has significant responsibility to control, manage, or direct the company

Customer Due Diligence Final Rule

- Final rule also amends AML program requirements, with banks required to:
  - Establish risk-based procedures for conducting ongoing due diligence
  - Develop customer risk profiles
  - Implement ongoing monitoring to identify and report suspicious activity, and
  - Based on risk, update customer information
- Read the final rule here: https://www.gpo.gov/fdsys/pkg/FR-2016-05-11/pdf/2016-10567.pdf

Updated BSA/AML Examination Manual

- Revised BSA/AML Examination Manual released in December 2014
- Revised version clarifies supervisory expectations & regulatory changes since the last update to the manual in 2010
- Significant revisions made in the following sections:
  - Suspicious Activity Reporting
  - Currency Transaction Reporting
  - Automated Clearing House Transactions
  - Prepaid Access
  - 3rd Party Payment Processors
- Review the updated Manual and make changes to your BSA/AML policies and procedures, as needed, based on your bank's risk profile.
- Access the updated BSA/AML Examination Manual here: https://www.ffiec.gov/bsa_aml_infobase/documents/bsa_aml_man_2014.pdf

BSA/AML Training Series

BSA Officers & Staff