A Deep Dive Into Bank Secrecy Act

JUNE 19, 2025

PRESENTED BY

Lindsey Becker, CRCM – Senior Manager Internal Audit

NACUSAC 2025 Conference

DoerenMayhew

"Doeren Mayhew" is the brand name under which Doeren Mayhew Assurance and Doeren Mayhew Advisors, LLC and its subsidiary entities provide professional services. Doeren Mayhew Assurance and Doeren Mayhew Advisors, LLC (and its subsidiary entities) practice as an alternative practice structure in accordance with the AICPA Code of Professional Conduct and applicable law, regulations and professional standards. Doeren Mayhew Assurance is a licensed independent CPA firm that provides attest services to its clients, and Doeren Mayhew Advisors, LLC and its subsidiary entities provide tax and business consulting services to their clients. Doeren Mayhew Advisors, LLC and its subsidiary entities are not licensed CPA firms.

Introduction

The Bank Secrecy Act (BSA) and related laws and regulations require financial institutions to take reasonable steps to verify the identity of their customers, monitor and report certain currency, suspicious, and foreign transactions, which requires financial institutions to maintain records providing a paper trail that law enforcement can utilize and provides for penalties for individuals and entities attempting to avoid those requirements.

Common acronyms

AML	Anti-money laundering	FinCEN	Financial Crimes Enforcement Network
BSA	Bank Secrecy Act	OFAC	Office of Foreign Assets Control
CDD	Customer due diligence	SAR	Suspicious Activity Report
CIP	Customer identification program	BO	Beneficial ownership
CTR	Currency Transaction Report	MRB	Marijuana-related business
CTRE	CTR exemption	MSV	Money services business
FFIEC	Federal Financial Institutions Examination Council	POATM	Privately-owned ATM

Today’s discussion topics

- Five Pillars of a BSA/AML compliance program
- Overview
- BSA/AML software data validation review
- FinCEN 2024 Proposed Rule, updated fines for 2025, potential penalties
- Top BSA Violations and penalties
- SAR filings for certain cyber events

Five Pillars of a BSA/AML compliance program

1. System of internal controls to assure ongoing compliance
2. Independent testing for compliance
3. Designation of individual(s) responsible for coordinating and monitoring day-to-day compliance
4. Training for appropriate personnel
5. Risk-based procedures for conducting ongoing MDD/CDD
    - Understanding the relationship to develop a risk profile
    - Conducting ongoing monitoring to identify and report suspicious transactions, maintaining and updating member information

Lack of compliance in any one of these areas is likely to cause a failure in the BSA/AML program compliance requirements and result in an enforcement action.

Overview

- Internal controls
  - Solid policies, procedures and processes that correspond to credit union's size, complexity and organizational structure
- Board and management oversight
  - Appoint qualified independent BSA officer
  - Obtain audit report findings and steps to remediate timely
  - Obtain reports from BSA officer on SAR fillings and report on resource deficiencies
- Training
  - Develop annual BSA/AML training program and deliver to appropriate personal

Fines/penalties were noted in these areas during 2024 and many credit unions had to create a new training program that tailored training each respective area

Overview

- Compliance resources
  - Sufficient financial and personnel resources, including adequate software
- Risk assessment
  - BSA/AML/OFAC compliance program should be risk-based and identify risk categories that incorporate a credit union's products, services, members and geographic locations. Inherent risk – Controls – Residual risk
  - Living document that should be updated as changes take place within the credit union (new product or service, mergers and acquisitions) or as laws and rules change to monitor for risk exposure.
  - Needs to be reviewed and approved at least annually by the Board.

Overview

- MDD/CDD – Know your member
  - Objective is to enable a credit union to understand the nature and purpose of member relationships, including understanding the types of transactions in which a member is likely to engage.
- SAR
  - Effective monitoring program in place to monitor for suspicious activity
    - Identification or alert of unusual activity. May include employee identification, law enforcement inquiries, other referrals, and transaction and surveillance monitoring system output.
    - Managing alerts.
    - SAR decision making.
    - SAR completion and filing.
    - Monitoring and SAR filing on continuing suspicious activity.

Overview

- CTR
  - Monitor to ensure compliance with FinCEN for cash transactions over $10,000.
- 314(a) & 314(b)
  - Ensure credit union is signed up to receive 314(a) requests from FinCEN. If the credit union participates in optional 314(b), required documentation is maintained.
- OFAC
  - Compliance with OFAC sanctions means credit unions must monitor, block, and report financial transactions linked to individuals or entities subject to these sanctions. The Board should receive regular reports from the BSA Officer regarding OFAC compliance. Any matches need to be reported within 10 business days.

OFAC – New Retention Guidance

In March 2025 – US Department of the Treasury's Office of Foreign Assets Control (OFAC) issued a Final Rule:

- Extends the recordkeeping requirements
- Extends retention period from 5 years to 10 years
- Effective March 12, 2025
- All financial institutions must now retain the following for 10 years:
  - Blocked or rejected transactions
  - Member due diligence – know your member
  - Licenses and authorizations
  - Internal compliance reviews

OFAC – New Retention Guidance

Compliance Program Adjustments

Recordkeeping systems – Credit Unions must update their system to store sanctions-related records for 10 years

Policy updates – compliance manuals and procedures must reflect new retention timeline

OFAC Risk Assessment – must reflect new retention timeline

Overview

- BSA/AML/OFAC independent audit
  - Required every 12-18 months with the results being provided to the Board.
- AML
  - Controls to reduce the risk of money laundering

BSA/AML software data validation review

- Automated monitoring systems
  - Rule-based systems that apply transaction parameters, scenarios, and filters that are tailored to each credit union.
  - Test periodically to ensure they are working effectively.
- Review assesses if:
  - Data from core system and other third-party vendors is timely and accurately transferred to the BSA/AML software for data analysis.
  - Software parameters/settings related to suspicious activity monitoring are adequate to facilitate compliance within BSA/AML regulatory reporting requirements.

FinCEN Rule, proposed June 28, 2024

- Requires financial institutions to establish, implement and maintain effective, risk-based, and reasonably designed AML/Countering the Financing of Terrorism (CFT) programs with certain minimum components, including a mandatory risk assessment process.
- Require financial institutions to review government-wide AML/CFT priorities and incorporate them, as appropriate, into risk-based programs, as well as provide for certain technical changes to program requirements.
- Promote clarity and consistency across FinCEN's program rules for different types of financial institutions.

Money Service Businesses (MSBs)

- Credit Unions are seeing an increase in MSBs seeking accounts
- If maintaining account relationships with or considering offering accounts to MSBs, the BSA compliance program must include effective policies, procedures and processes to mitigate the associated risks:
  - Properly identify member accounts as MSBs
  - Assess potential risk posed by the member relationship
  - Conduct adequate and ongoing due diligence of the MSB relationship
  - Ensure MSB accounts are appropriately included in the suspicious activity monitoring and reporting systems

Money Service Businesses (MSBs)

- Cash-intensive businesses are conducting legitimate business; however, some aspects of these businesses may be susceptible to money laundering or terrorist financing. Common examples include, but are not limited to, the following:
  - Convenience stores
  - Restaurants
  - Retail stores
  - Liquor stores
  - Cigarette distributors
  - Privately owned automated teller machines (ATM)
  - Vending machine operators

Privately Owned ATMs

- ATMs not owned by a regulated financial institution
- Often associated with cash-intensive businesses (i.e., convenience stores, bars, restaurants, grocery stores, check cashing establishments)
- Credit Union should identify all POATMs and conduct periodic onsite visits, annual due diligence, and inquire on the source of funds used to replenish the ATM

Marijuana Related Businesses (MRB)

- Credit Unions across the country continue to bank money from MRBs - Deposits and Loans
- They are allowed to bank as long as the requirements set out by FinCEN are followed, meaning all transactions are reported to the government
- Credit Unions are exploring; however, they're worried about the large amounts of cash walking in the door. Often times armored car services are arranged to transport cash directly to the Federal Reserve Bank.

Marijuana Related Businesses (MRB)

- Many key risk factors to be considered
- Ability to complete the enhanced compliance required and key partner or vendor relationships can be difficult
- Often times Credit Unions have to hire additional staff for the increased scrutiny
- Even for credit unions that have decided not to bank marijuana money, they need to make sure no existing members are quietly funneling marijuana through their accounts
- Credit Unions should have a policy indicating if it chooses to offer accounts for MRBs

Updated monetary penalties for 2025

- FinCEN adjusted its civil monetary penalties (CMPs) to account for inflation, effective January 17, 2025
  - Penalties for failing to file SARs, CTRs, or not maintaining proper record-keeping have increased
  - Maximum CMPs for violating BSA requirements now exceed $1 million

2025 penalty adjustments

TABLE 1 TO § 1010.821—PENALTY ADJUSTMENT TABLE

U.S. Code citation	Civil monetary penalty description	Penalties as last amended by statute	Maximum penalty amounts or range of minimum and maximum penalty amounts for penalties assessed on or after January 17, 2025
12 U.S.C. 1829b(j)	Relating to Recordkeeping Violations for Funds Transfers.	$10,000	$26,262
12 U.S.C. 1955	Willful or Grossly Negligent Recordkeeping Violations.	10,000	26,262
31 U.S.C. 5318(k)(3)(C)	Failure to Terminate Correspondent Relationship with Foreign Bank.	10,000	17,765
31 U.S.C. 5321(a)(1)	General Civil Penalty Provision for Willful Violations of Bank Secrecy Act Requirements.	25,000 –100,000	71,545 –286,184
31 U.S.C. 5321(a)(5)(B)(i)	Foreign Financial Agency Transaction—Non-Willful Violation of Transaction.	10,000	16,536
31 U.S.C. 5321(a)(5)(C)(i)(I).	Foreign Financial Agency Transaction—Willful Violation of Transaction.	100,000	165,353
31 U.S.C. 5321(a)(6)(A)	Negligent Violation by Financial Institution or Non-Financial Trade or Business.	500	1,430
31 U.S.C. 5321(a)(6)(B)	Pattern of Negligent Activity by Financial Institution or Non-Financial Trade or Business.	50,000	111,308
31 U.S.C. 5321(a)(7)	Violation of Certain Due Diligence Requirements, Prohibition on Correspondent Accounts for Shell Banks, and Special Measures.	1,000,000	1,776,364
31 U.S.C. 5330(e)	Civil Penalty for Failure to Register as Money Transmitting Business.	5,000	10,556
31 U.S.C. 5336(h)(3)(A)(i)	Civil Penalty for Beneficial Ownership Information Reporting Violation.	500	606
31 U.S.C. 5336(h)(3)(B)(i)	Civil Penalty for Unauthorized Disclosure or Use of Beneficial Ownership Information.	500	606

Potential fines for violating OFAC

- Can be substantial
- Criminal penalties include
  - Fines ranging from $50,000 to $10,000,000

    and
  - Imprisonment ranging from 10- to 30-years for willful violations
- Civil penalties
  - $250,000 or twice the amount of each underlying transaction to $1,075,000 for each violation

Top BSA violations of 2024

According to a 2024 review of BSA/AML enforcement actions **regulators** cited failures across the **five pillars** of a compliant BSA/AML program:

1. Failure to File Suspicious Activity Reports (SARs)

- Credit unions were cited for **delays or failures in filing SARs**, especially in cases involving unusual cash transactions or suspected fraud.
- In one case, a **former BSA officer** at a credit union was fined **$100,000** for multiple failures to file SARs and maintain proper documentation

Top BSA Violations of 2024

2. Inadequate Customer Due Diligence (CDD)

- Examiners found that some Credit Unions did not properly **risk-rate members** or update member profiles based on transaction behavior.
- This led to **missed red flags** in high-risk accounts, including those involving money service businesses (MSBs).

3. Weak Internal Controls

- Several institutions lacked **automated transaction monitoring systems**, relying instead on manual reviews that were inconsistent or incomplete.
- Some Credit Unions had **outdated BSA/AML policies** that did not reflect current regulatory expectations.

Top BSA Violations of 2024

4. Insufficient Training and Oversight

- BSA training was found to be **infrequent or not role-specific**, leading to staff being unaware of red flags or reporting obligations.
- In some cases, the **BSA Officer role was not clearly defined**, or the officer lacked sufficient authority or resources.

5. Failure to Conduct Independent Testing

- Some Credit Unions failed to conduct **annual independent BSA audits**, or the audits were too limited in scope to be effective.

TD Bank Violations & Penalties

- $3 billion penalty
- Largest bank in history to plead guilty to violating BSA
  - 10th biggest bank in US and 2nd in Canada
- Largest BSA penalty ever
- Next largest penalty was against Wells Fargo, with a $1 billion fine in 2018
- Rare – limit placed on asset growth
  - Bank had intended to expand further in the U.S.

TD Bank Violations & Penalties

- 92% of TD Bank's transactions went unmonitored between January 2018 and April 2024
- Failed to monitor $18.3 trillion in customer activity over a 6-year period
- Despite significant internal red flags, the bank did not identify its own employees were conspiring to launder tens of millions of dollars to Colombia until law enforcement arrested them
- One money laundering network moved more than $470 million through the bank's U.S. branches, bribing employees with more than $57,000 in gift cards to ensure employees would keep processing their transactions

TD Bank Violations and Penalties

- Between March 2021 and March 2023, a high-risk jewelry business moved nearly $120 million through shell accounts before TDB reported the activity.
- In another scheme, several money laundering networks deposited funds in the US and quickly withdrew those funds using ATMs in Colombia.
  - Five employees helped by issued dozens of ATM cards for the launderers, aiding in the laundering of around $39 million.
- TDB instructed stores to stop filing unusual transaction reports on certain suspicious customers

TD Bank violations and penalties

- TDB became the bank of choice for multiple money laundering organizations and criminal actors and processed hundreds of millions of dollars in money laundering transactions.
- Employees said their AML failures made it “convenient” for criminals
- Principal Deputy Assistant Attorney General Nicole M. Argentieri: “U.S. financial institutions are the first line of defense against money laundering and illicit finance. When they participate in crime rather than prevent it, we will not hesitate to hold them accountable to the fullest extent of the law.”

Brinks 2025 Case

- Landmark enforcement action by FINCEN in February 2025
- First time the agency penalized an armored car company for violations of the Bank Secrecy Act
- Penalty Amount $37 Million
- Violations:
  - Failure to register as a Money Service Business (MSB)
  - Failure to implement an effective AML program
  - Failure to file Suspicious Activity Reports (SARs)
- Moved hundreds of millions of dollars in bulk currency across the US Mexico border on behalf of high-risk clients, including a Mexican currency exchanger that later plead guilty to BSA Violations
- Lacked controls to detect and report suspicious activity exposing US to money laundering/narcotics trafficking

SAR filing for certain cyber events

- Occurrences of ATM jackpotting are increasing nationwide
  - In one Wisconsin theft, the suspect(s) installed a malicious hard drive resulting in one ATM releasing between $60,000 and $100,000 in cash
- If the action is reported to the appropriate law enforcement agency, no SAR is required to be filed for robberies or burglaries.
  - ATM jackpotting can be argued as a form of robbery; no SAR required if reported correctly
- Another New York Credit Union was a victim of jackpotting on nearly 20 ATMs resulting in $1 million loss in stolen cash due to these malicious hard drives attached to ATM machines
- Look for attached items, damage, open/unlocked ATMs

SAR Filing for Certain Cyber-Events

- However: in FIN-2016-A005, FinCEN defines a “Cyber-Event” as "An attempt to compromise or gain unauthorized electronic access to electronic systems, services, resources, or information."
- Generally, ATM jackpotting fits these broad definitions of both cyber-event and cyber-enabled crime
- Financial institutions can choose to not file a SAR for ATM jackpotting if it was considered a robbery / burglary, and it reported properly otherwise
- Most risk-averse choice would be to file one anyway based on FinCEN’s definition of a Cyber-Event – and it is better to over-file than under-file.

Questions?

Lindsey Becker, CRCM
Internal Audit and Compliance
Senior Manager
Cell: (810) 210-4446
Email: becker@doeren.com

Thank you