2021
Bank Secrecy Act
&
Anti-Money Laundering
Training

Alisha Stair, BSACS, CUDE, CCUFC, CUCE, CCUF
Member Engagement Consultant
Alisha.Stair@lscu.coop

LSCU
League of Southeastern Credit Unions & Affiliates

Goals

By the end of today's presentation, we will:

1. **Identify regulators' expectations for credit unions & staff under the BSA.**
2. **Identify required components of your BSA Compliance Program (The Pillars)**
3. **Review case studies of Credit Unions that failed BSA Compliance.**

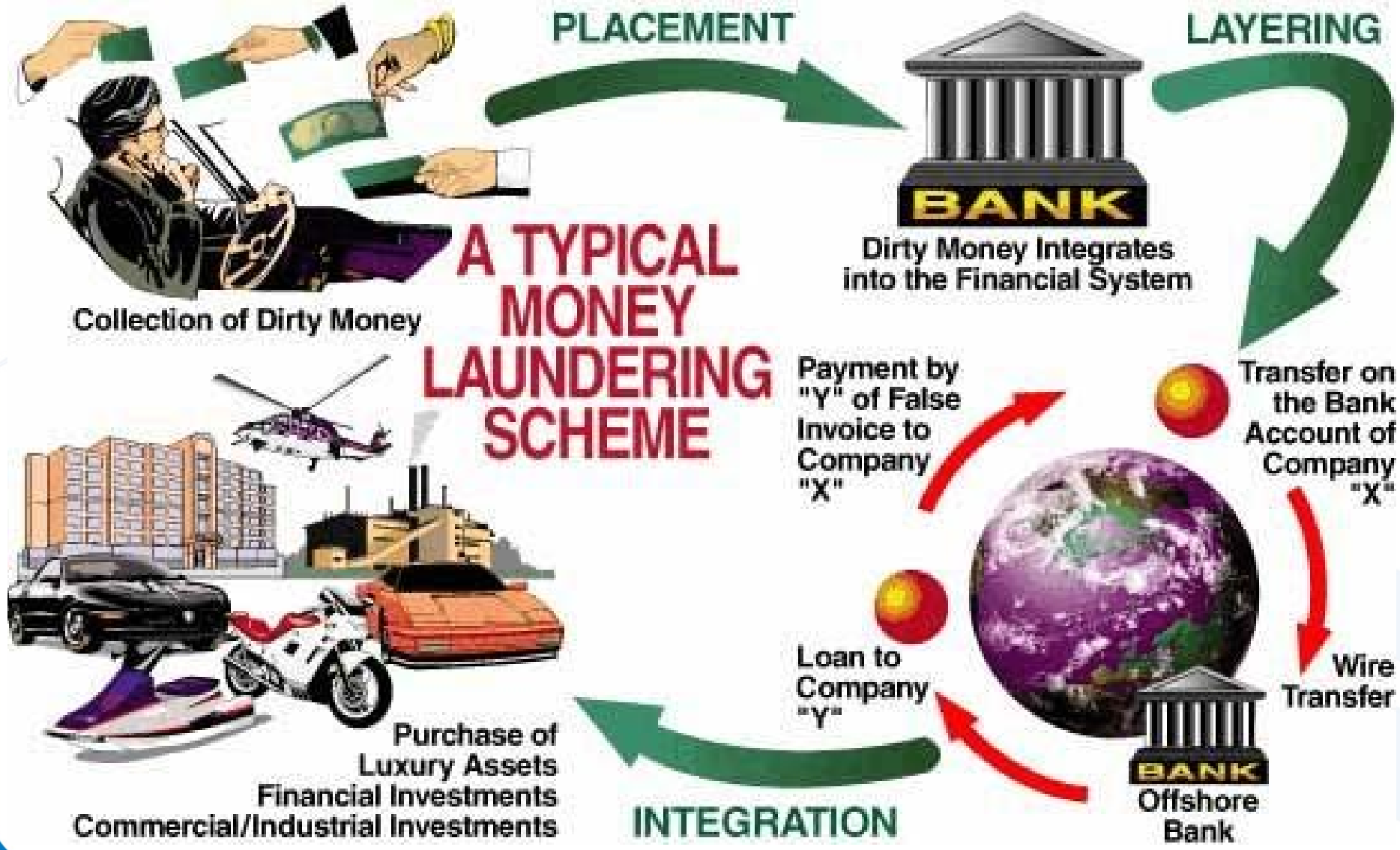
Basic Themes of BSA Compliance

1. **Analyze and Manage Risk – One size does not fit all.**
2. **Know your Members**
3. **Document Everything!**

Purpose of BSA

- **Bank Secrecy Act:** Designed to help identify the **source, volume, and movement** of currency and other monetary instruments transported or transmitted into or out of the US or deposited in financial institutions.
- Creates record keeping obligations to enable a paper trail for assisting investigations into criminal activity.
- **What is Money Laundering?**

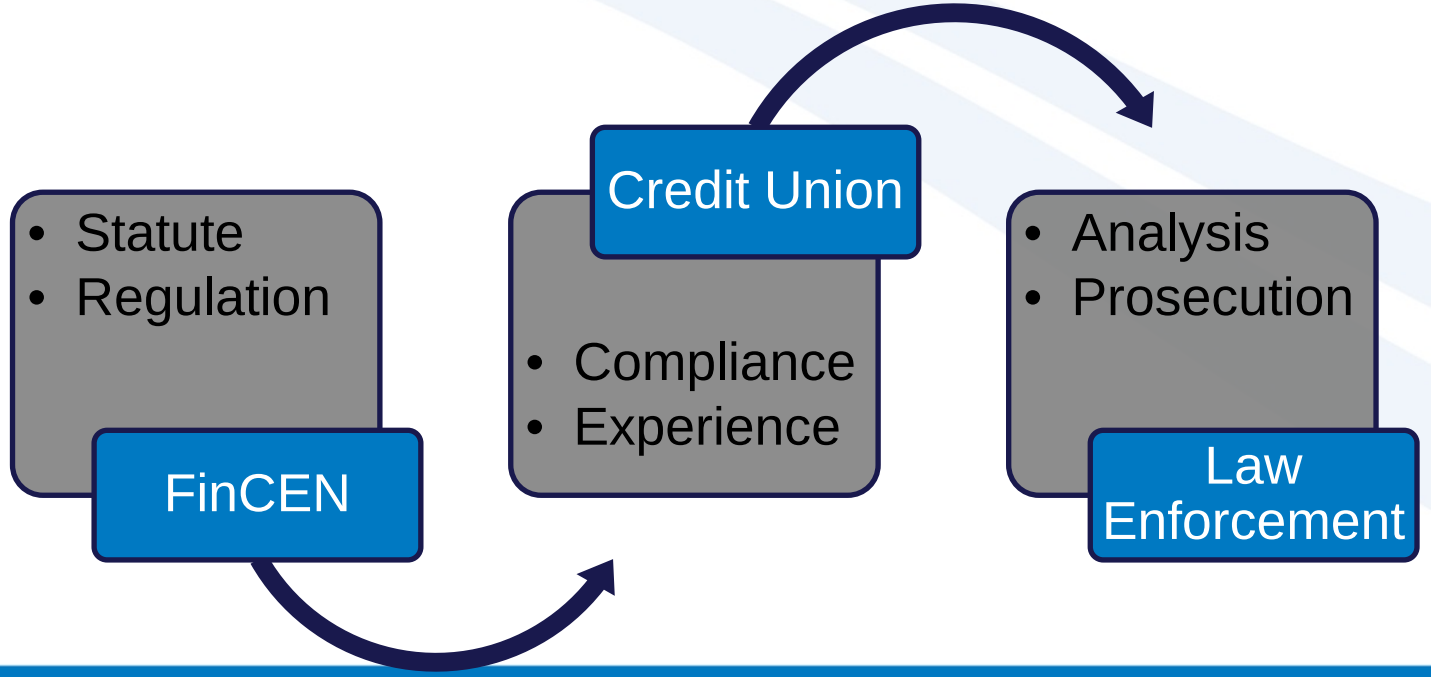
Stages of Money Laundering



FINANCIAL CRIMES ENFORCEMENT NETWORK

BSA Framework

- **The Law –** The Bank Secrecy Act and a medley of other statutes (PATRIOT Act).
- **FinCEN –** Promulgates/enforces BSA regulations & "safeguards the financial system from illicit use, combatting money laundering and promoting national security."
- **NCUA –** Enforces compliance via examination.(12 CFR Part 748)
- **Federal Law Enforcement –** Utilizes data for investigations.



Why are you here?

- **Required annual training** – *Clarified in 05-CU-09.*
- Advisory FIN-2014-A007: “This guidance was provided due to shortcomings in compliance due to a lack of involvement from institutions’ senior management….the **poor culture of compliance** which existed in part due to a **lack of leadership** to improve and strengthen organizational compliance with BSA.”

So…What is a Culture of Compliance?

Characteristics defined by FinCEN (FIN-2014-A007):

- **Leadership Should Be Engaged.**
- **Compliance Should Not Be Compromised By Revenue Interests.**
- **Information Should Be Shared Throughout the Organization.**
- **Leadership Should Provide Adequate Human and Technological Resources.**
- **The Program Should Be Effective and Tested By an Independent and Competent Party.**
- **Leadership and Staff Should Understand How Their BSA Reports are Used.**

What the BSA Exam Manual says:

The board of directors and senior management should be **informed of changes and new developments in the BSA**...they need to understand the importance of BSA/AML regulatory requirements, **the ramifications of noncompliance, and the risks posed to the credit union**…(without which)…the board of directors cannot adequately provide BSA/AML oversight.

BSA – §748.2 Procedures for Monitoring BSA Compliance (Policymaking)

a) Purpose…to **ensure that all federally insured credit unions establish and maintain procedures reasonably designed to assure and monitor compliance…**

b) Establishment of a BSA compliance program—

1. Program requirement. Each federally insured credit union **shall develop and provide for the continued administration of a program reasonably designed to assure and monitor compliance with the recordkeeping requirements…**The compliance program **must be written, approved by the credit union's board of directors, and reflected in the credit union's minutes.**
2. Member Identification Program…More Later

Pillars of BSA Compliance

1. Implement proper internal controls to ensure that your BSA program is functioning as intended;
2. Provide training for appropriate personnel, at least annually;
3. Provide adequate annual independent audit procedures;
4. Require the participation of a qualified and knowledgeable BSA officer;
5. Implement Risk Based procedures for Member Due Diligence / Beneficial Ownership Rule.

Pillar 1: Internal Controls – Responsibility

The **board of directors, acting through senior management, is ultimately responsible for ensuring that the credit union maintains an effective BSA/AML internal control structure.** The board should **create a culture of compliance** to ensure staff adherence to the credit union's BSA/AML policies, procedures, and processes. Internal controls are the policies, procedures, and processes designed to limit and control risks and to achieve compliance with the BSA. The **level of sophistication of the internal controls should be commensurate with the size, structure, risks, and complexity of the credit union.**

Pillar 1: Internal Controls - Examples

- Provide for **dual controls** to the best extent possible.
  - Ex: Employees completing the reporting forms generally should not also be responsible for the decision to file the reports.
- Provide sufficient controls and monitoring systems for timely detection and reporting of suspicious activity.
- Identify areas of high-risk and develop program to manage accordingly: **Products, Members, Branches**
- Provide adequate supervision of employees that handle currency, complete reports, grant exemptions, monitor suspicious activity, or engage in activity covered by BSA and its implementing regulations.
- Incorporate BSA compliance into job descriptions and performance evaluations, as appropriate.
- Train staff of BSA responsibilities and internal policy guidelines.
- Policy Pro is your friend!

Pillar 2 - Training

At a minimum:

- The credit union's training program must include employees whose duties involve BSA.
- Training should be tailored to the person's specific responsibilities.
- BSA/AML training should be given to new staff during orientation.
- The BSA Compliance Officer should receive periodic training that is relevant and appropriate given changes to regulatory requirements.
- Credit unions should **document** their training programs.

Pillar 3 - Audit 12 – 18 months

Independent testing should, at a minimum, include:

- An evaluation of the BSA/AML compliance program, including policies, procedures, and processes.
- A review of the credit union's risk assessment
- Appropriate risk-based transaction testing.
- An evaluation of management's efforts to resolve violations and deficiencies
- A review of staff training
- A review of the effectiveness of the suspicious activity monitoring systems.

CU AUDIT & COMPLIANCE GROUP
A Division of LEVERAGE

LSCU

Pillar 4 - Staff : BSA Officer

- The board of directors is responsible for designating & ensuring that the BSA compliance officer has **sufficient authority and resources** to administer an effective BSA/AML compliance program based on the credit union's risk profile.
  - The BSA compliance officer should be fully knowledgeable of:
    - the BSA and all related regulations
    - the credit union's products, services, etc.
- The BSA compliance officer should **regularly (monthly)** apprise the board of directors and senior management of ongoing BSA compliance.

Risk Assessment

- **Step 1**: **IDENTIFY** Risk Categories - Vary according to:
  - Products & Services: Online banking, Wires, RDC, Lending
  - Members: **MSBs**, Professional service providers, NRA accounts, cash-intensive businesses
  - Geography: High Intensity Drug Trafficking & High Intensity Financial Crime Areas (HIDTA/HIFCA)
- **Step 2**: **ANALYZE** Risk Categories & Determine Patterns using data:
  - Purpose of the account.
  - Actual or anticipated activity in the account.
  - Nature of the member's business/occupation.
  - Member's location.
  - Types of products and services used by the member.
- **Step 3: MITIGATE & MONITOR** with reports (Inactive, Large Deposit, validation) & technology (Verafin, etc.)

Example of Risk Matrix

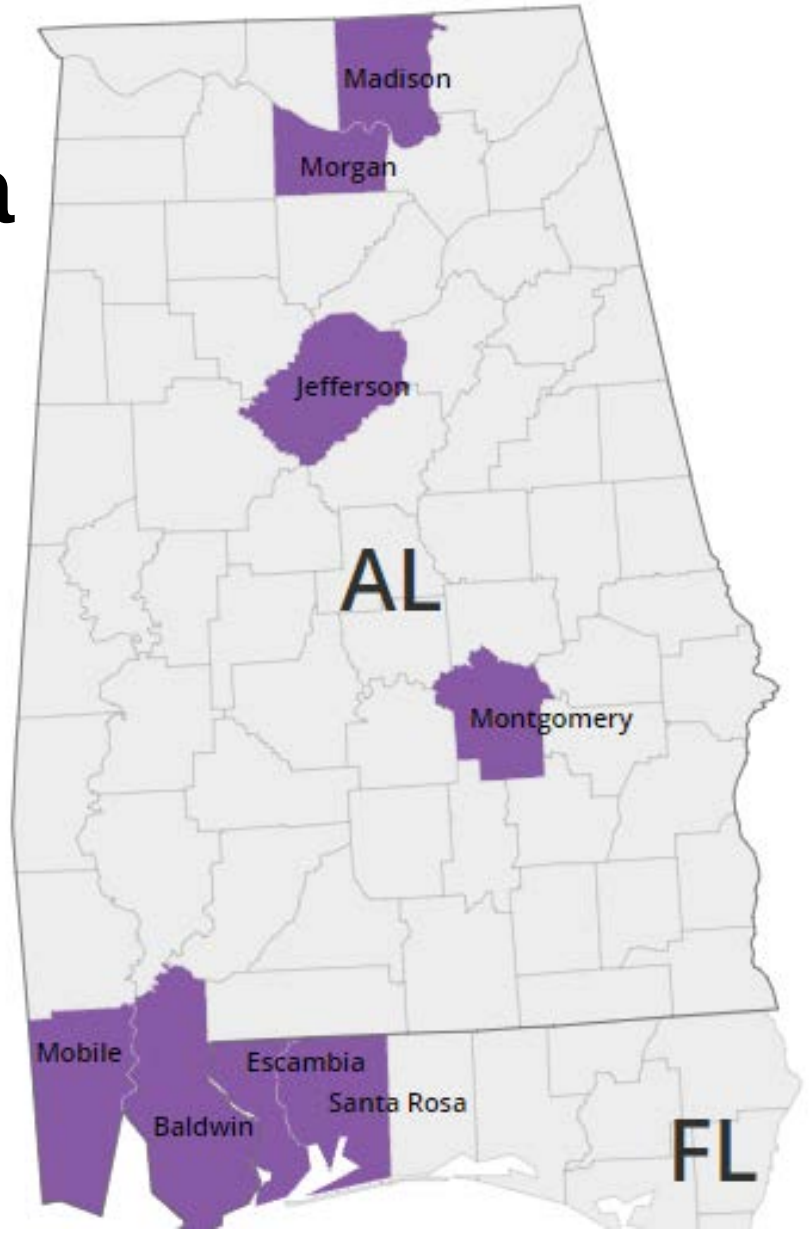
Low	Moderate	High
Stable, known customer base.	Customer base increasing due to branching, merger, or acquisition.	A large and growing customer base in a wide and diverse geographic area.
No electronic banking (e-banking) or the Web site is informational or nontransactional.	The bank is beginning e-banking and offers limited products and services.	The bank offers a wide array of e-banking products and services (e.g., account transfers, e-bill payment, or accounts opened via the Internet).
On the basis of information received from the BSA-reporting database, there are few or no large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a moderate volume of large currency or structured transactions.	On the basis of information received from the BSA-reporting database, there is a significant volume of large currency or structured transactions.
Identified a few higher-risk customers and businesses.	Identified a moderate number of higher-risk customers and businesses.	Identified a large number of higher-risk customers and businesses.

Developing the BSA Program based on the RA

Policy statements alone are not sufficient; practices must coincide with written policies and procedures. The program should:

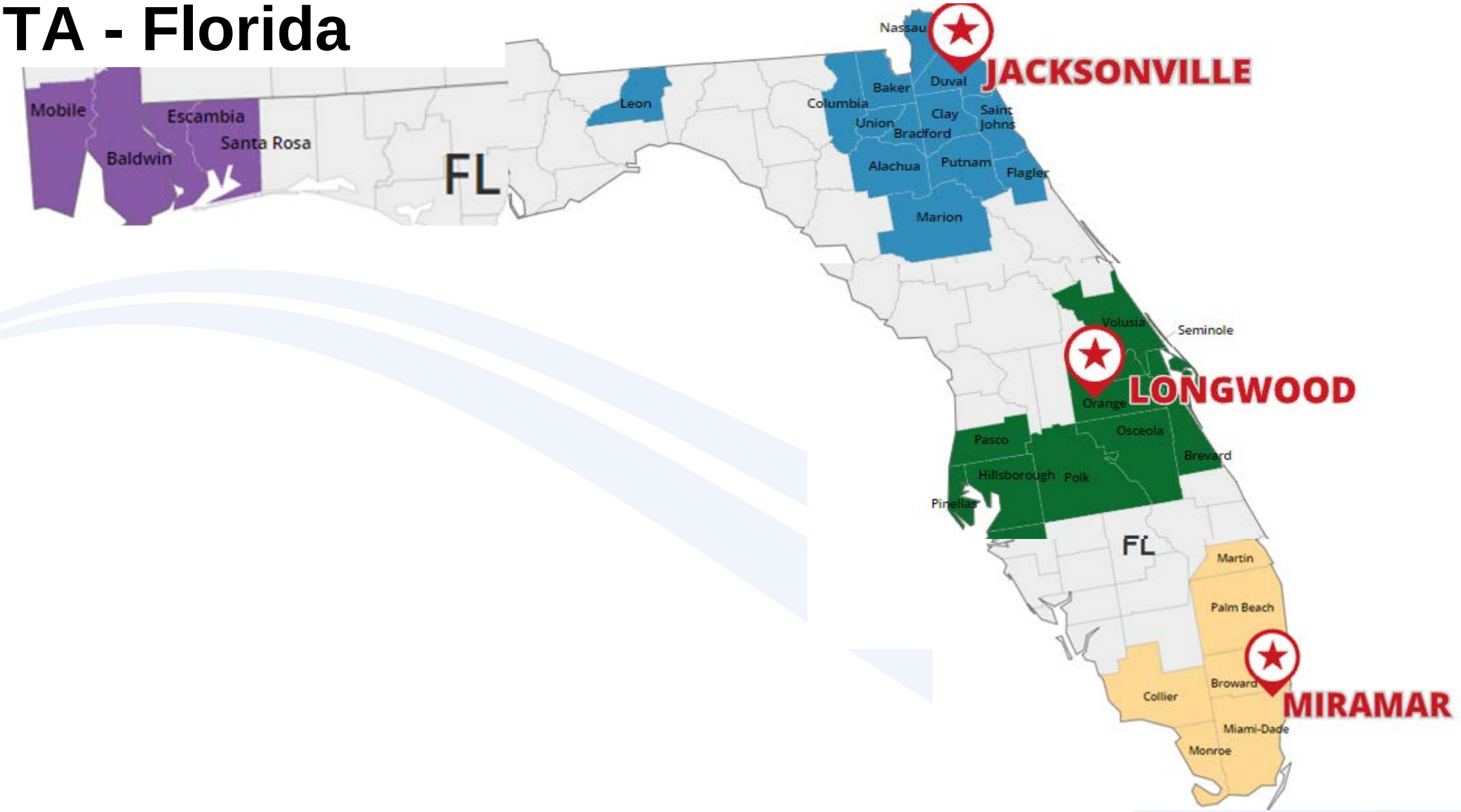
- Include policies/procedures that specifically monitor/control higher risk products, services, members, & branches.
- Identify and document the actions taken to mitigate risk.
- Evolve as new products and services are introduced or changed, expansions occur through mergers, and/or field of membership enlarges to remain credit union specific.
- Review the BSA Risk every 12 to 18 months.

HIDTA - Alabama

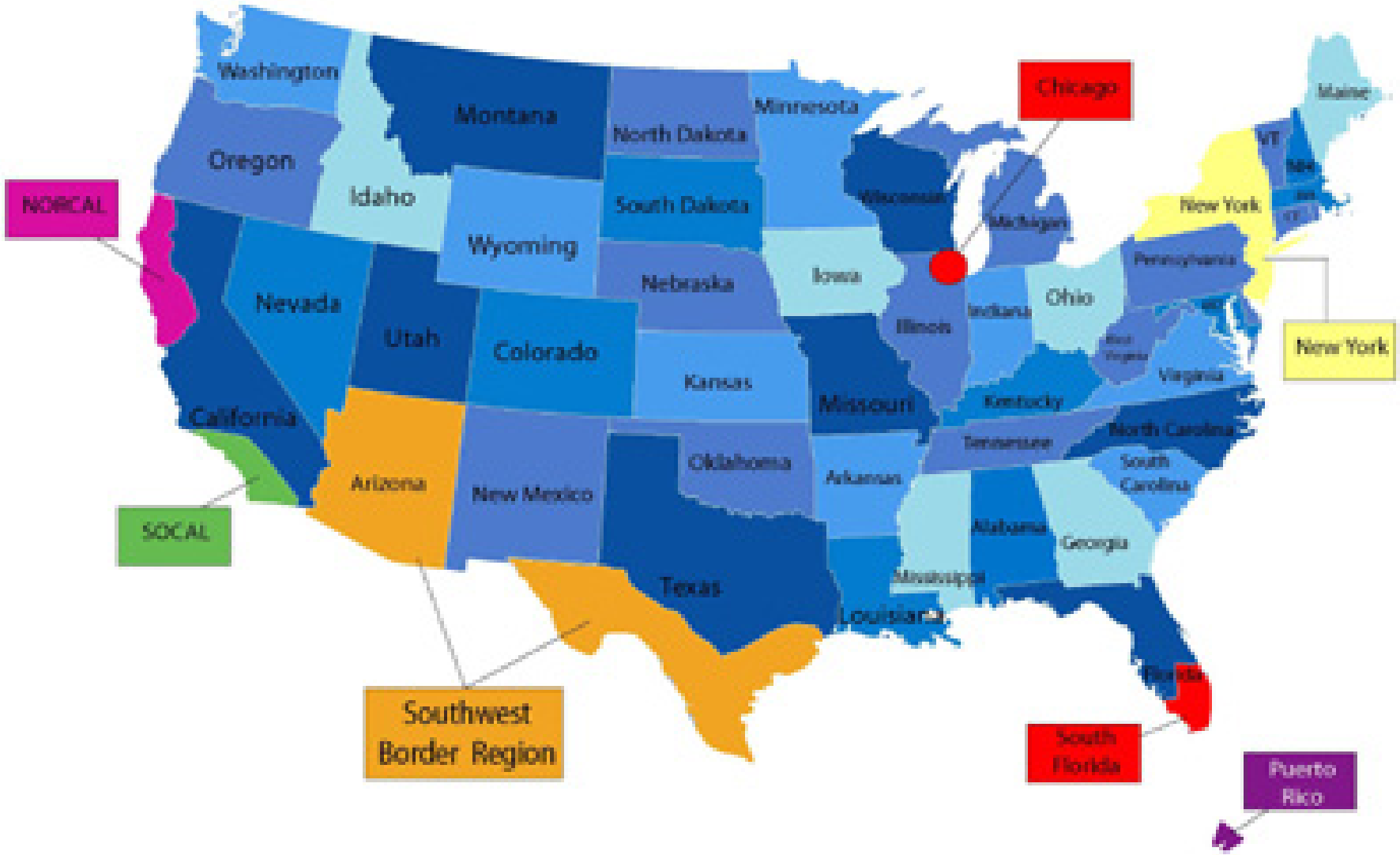


HIDTA - Georgia

HIDTA - Florida



High Intensity Financial Crimes Areas



Member Identification Program: Collect Member Information

Purpose: To enable the CU to form a reasonable belief that it knows the identity of each member.

1. Identifying Info:
    1. Name
    2. DOB for individuals.
    3. Address-PHYSICAL
    4. ID= Tax ID = SSN
2. Verifying Info:
    - Documentary - Unexpired government issued identification (photo),
        - A driver's license;
        - Passport; or
        - Military ID (criminal violation to copy)
    - Non-Documentary –
        - Information obtained from a credit bureau
        - Tax return
        - Online verification systems

Member Identification Program: Verifying Member Information

- Procedures explaining verification and non-verification. (Flowchart)
- If & when the credit union should open an account.
  - What access a “member” will have until verification, Steps for closing account upon verification failure/When to file a SAR.
- Identifying info must be kept for 5 years after the account is closed.
  - A **full description** of documents used to open account.
  - Methods used and results of verification.
  - Results of discrepancies in ID.
- Must include cross reference of ID with federal terrorist list.
- Must provide notice to applicant that credit union is requesting info to identify their ID.

What an account is and isn't

- An **"account" is a formal banking relationship to provide** or engage **in services**, dealings, or other financial transactions, and **includes a deposit account, a transaction or asset account, a credit account, or another extension of credit. An account also includes a relationship established to provide a safe deposit box or other safekeeping services or to provide cash management, custodian, or trust services.**
- **Includes renewals**
- An account does **not** include:
  - Products or services for which a formal banking relationship is not established with a person, such as check cashing, funds transfer, or the sale of a check or money order.
  - Any account that the credit union acquires. This may include single or multiple accounts as a result of a purchase of assets, acquisition, merger, or assumption of liabilities.

Currency Transaction Reports

- File Currency Transaction Report (CTR) for each transaction in currency of more than $10,000.
- Multiple currency transactions totaling more than $10,000 during any one business day are treated as a single transaction if the credit union has knowledge that they are by or on behalf of the same person.
- Aggregate weekends, ATM, and night deposit transactions (next business day).
- Must be filed within **15 calendar days** after the date of the transaction.
- Bank Secrecy Act Currency Transaction Report (BCTR)/electronic.
- **5-year record retention.**

Currency Transaction Reports

- Currency: **Coin and paper money** of the United States, or any other currency that is customarily accepted as money in the country of issue.
- This includes any aggregate transactions involving currency like:
  - Deposits & withdrawals (including IRA)
  - Loan payment
  - Purchase of CD
  - **Monetary instruments…Report even if deposited.**
  - Foreign currency exchange
  - Shared Branching
- Consolidate deposits (Cash In) and withdrawals (Cash Out) separately. Do not off-set deposits and withdrawals.

Suspicious Activity Report – Required Filing

- Criminal violations
  - involving insider abuse in any amount.
  - aggregating $5,000 or more (suspect identified).
  - aggregating $25,000 or more (suspect unknown).
- Transactions aggregating $5,000 or more, the credit union suspects:
  - May involve potential money laundering or other illegal activity.
  - Is designed to evade the BSA.
  - **Has no business or apparent lawful purpose or is not the type of transaction that the particular member would normally be expected to engage in, and the credit union knows of no reasonable explanation for the transaction.**

SAR Filing

SARs must be filed:

- **Electronically**;
- No later than **30 calendar days** from the detection of facts constituting the basis for filing, meaning *after* a meaningful investigation.
  - If no suspect is identified, the filing is extended to **60 days**.
  - Report continuing suspicious activity after 90-day review up to 120-day deadline.
- 5-year record retention.
- Board should be promptly notified of SAR filings. (Monthly)
- SARs are confidential; unauthorized disclosure of a SAR is a violation of federal law, especially to suspect member.
  - Can be shared with NCUA, law enforcement or any state regulatory authority administering a state law requiring the CU to comply.
- Do not file for robbery *(report to appropriate authorities).*
- Federal law provides a Safe Harbor.

SAR Checklist

1. Is the credit union properly e-filing all instances in which a SAR is warranted?

2. Is the report made within 30 days of discovery, or, as necessary, no later than 60 days after discovery?

3. Does the credit union file a report if it suspects that someone may be “structuring” transactions to avoid submission of a CTR?

4. Is the credit union aware that law enforcement agencies do not need a subpoena to request that the credit union provide all supporting documentation available?

5. Does the credit union report to its Board of Directors at least monthly when a SAR has been filed?

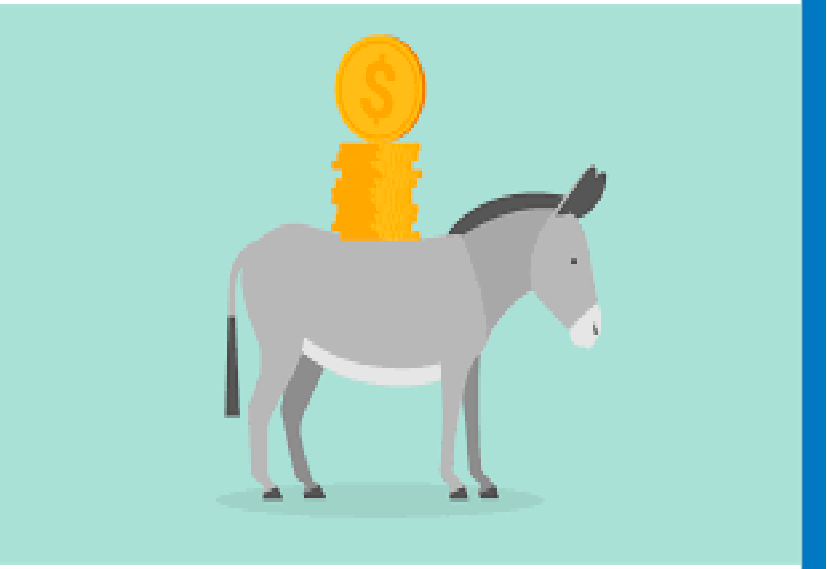
Red Flags for Suspicious Activity

- A member uses unusual or suspicious identification documents.
- A member tries to persuade an employee not to file required reports or maintain required records.
- Many fund transfers are sent in large, round dollar amounts.
- Funds are frequently sent or received via international wire transfers from or to higher-risk locations
- A member makes frequent or large transactions and has no record of past or present employment experience.
- Many small, incoming transfers are received, or deposits are made using checks and money orders. Almost immediately, all or most of the transfers or deposits are wired to another city or country in a manner inconsistent with business or history.
- A member separates a cash transaction over $10,000 into several transactions attempting to avoid the CTR reporting threshold (Structuring).
- Deposits are structured through multiple branches, or by groups of people who enter a single branch at the same time.
- A member's wire or EFT activity is unexplained, repetitive, or shows unusual patterns.
- Member conducts large deposits and withdrawals during a short time period after account opening, then subsequently closes the account or the account becomes dormant.
- An account with little activity suddenly experiences large deposit and withdrawal activity.
- When establishing a business account, member is reluctant to provide complete information about the nature and purpose, anticipated activity, or names of company officers.


MISSISSIPPI
JOSE PACHECO
3535 HWY 80 E
PEARL MS 37208

FINCEN Advisories: COVID-19 Cyber Crime & Money Mule Scams

- **(FIN-2020-A005):** Acceleration towards remote access presents opportunities for exploitation. Red flags include:
- **Targeting Remote Platforms/Processes**
  - Manipulation of documentation-spelling, blurry photos, no additional documentation, multiple logins or mismatched IPs, increased password resets
- **Phishing & Malware**
  - Unsolicited emails from untrusted sources, emails with government or industry jargon from unknown senders, links with irregular URLs
- **Business Email Compromise Schemes**
  - Emailed instructions to move payment methods from check to ACH, or a different account, transactions from healthcare sector referencing PPE.
- **(FIN-2020-A003):** Indicators of imposter & money mule scams: Virtual requests for personal info, incorrect links, multiple new account openings and money movement, low balance accounts receiving funds out of pattern.



Source: FinCEN

Monetary Instruments

- Credit unions must maintain record of monetary instruments (travelers check, cashiers check, money order, credit union checks) sold between **$3,000-$10,000 in currency**.
- Verify member or identity and record identifying info. Record of sale should include: name, date, type, serial number, amount, & identifying info. Additional information is required for non-members (if permitted).
- Multiple purchases during one business day (including different types) totaling $3,000 or more are treated as one purchase.
- Credit unions must also maintain record of funds transfers of $3,000 or more (Wire Transfer Rule).
  - Does not cover ACH or electronic. See BSA Manual for recordkeeping requirements.
- **5-year record retention**

Beneficial Owners Rule

- Must have written procedures designed to ID and verify **legal entity members** (Corp., LLC, or other entity created with Sec. of State.)
  - Does NOT include FIs, Fed or state gov't, publicly traded companies, Non-US gov't entity that **doesn't engage in commercial activities**. (Will they ever include non-profits?)
- The **procedures** must contain elements of MIP program.
  - **develop risk profile regarding member relationships & monitor activities for suspicious transactions.**
  - ID beneficial owners when **new** account is opened by:
    - Using Beneficial Owner Certification Form in Appendix A;
    - Collecting the info asked for on the Form.
  - Verification of identity consistent with the CU's MIP.
- Who are Beneficial Owners?
  - Those who own 25% or more of equity interest in a legal entity;
  - Those who control a legal entity. (CEO, CFO, President, Treasurer, etc);
  - Trusts that own 25% of entity, the beneficial owner is the trustee.
- Develop policy even if you don't serve businesses.

Beneficial Owners : Record keeping

- Credit union must establish procedures for making and maintaining a record of all info obtained under the rule.
- The record must include at least:
  - For identification: any identifying info in certification.
  - For verification: description of documents relied upon or non-documentary methods.
- Records must be retained for 5 years after the account is closed.
- Compliance date: May 11, 2018

Information Sharing - Section 314(a) of the USA PATRIOT Act (31 CFR 1010.520)

1. Credit Unions must develop policies and procedures to process requests.
2. Law Enforcement via FinCEN requests information on suspects. Credit union must have contact to receive requests.
3. Credit Union must review their current account, those active previous 12 months, or transactions with suspect for six months.
4. Credit Union has 14 days to report matches (negative response not required).
5. Credit Union should document and keep confidential its receipt, review and response. **95% of 314(a) requests have contributed to arrests/indictments**

- **Voluntary** Information Sharing — Section 314(b): PATRIOT Act (31 CFR 1010.540)

OFAC - Office of Foreign Assets Control

- Enforces sanctions on people, nations, entities.
- Credit Unions must regularly review the Specially Designated Nationals (SDN) List against membership & run applicants through OFAC list prior to account opening.
  - Also covers wire, ACH, EFT, checks & instruments, loan payments, etc.
- Credit Unions must block or reject people or entities on the list and report those transactions to OFAC within **10 business days** and annually by 9/30 as of 6/30 (*for holders of blocked property*).
  - 1-800-540-OFAC (6322) or 1-202-622-2490
- Must perform risk assessment:
  - International funds transfers.
  - Nonresident alien accounts.
  - Foreign member accounts. Etc…
- OFAC compliance pillars are essentially the same as BSA.

Member Due Diligence

- Develop policies for investigations (expectations), responsibilities, and chain of command.
- DD is an **ongoing process** tailored to the **Credit Union's risk** profile.
- Collect info on everyone to establish norms for member activity. **(Member Risk)**
  - Low-risk Members: Regularly update contact info.
  - High-risk Members: Dedicate time to review high-risk accounts. Be nosy….
- Purpose of account:
  - Source of funds and wealth;
  - Occupation or type of business
  - Financial statements
  - Where the business is organized
  - Member's place of employment
- **Document** the decision and analysis.

Case Study 1: North Dade Community Development Federal Credit Union

- FOM: Community charter – North Miami-Dade County, FL
- Employees: 5
- Assets: $4.1 million
- Serviced MSBs outside FOM, performing High Risk activities in High-Risk jurisdictions.
- 2013: MSBs transactions (90% of revenue) included:
  - $54.8 million in cash orders,
  - $1.01 billion in outgoing wires,
  - $5.3 million in returned checks,
  - $984.4 million in remote deposit capture.
- NCUA ordered C&D in 2013.

North Dade's compliance with BSA:

1. Internal Controls
   - Failed to assess money laundering and terrorist financing risks.
   - Risk assessment wasn't performed from 2009 until Nov. 2013.
   - Inadequate controls to monitor suspicious activity and 3rd party vendors.
   - 56 MSB accounts were serviced rather than the 1 vendor, without additional assessments or monitoring.
   - From 2010-13, one person accounted for 60% of business banking, they filed over 2000 CTRs, but didn't monitor the account as high risk.
   - Failed to follow policy on MSBs without licenses, continued to service MSBs.
2. BSA Officer- failed to designate.
3. Training- No record of Board or employee BSA training.
4. Audit: Had no evidence of BSA audit prior to C & D.

North Dade's compliance with BSA:

3. Member Identification Program – Failed to ID MSBs.

"By not knowing its members, North Dade was not capable of understanding their expected transactional behavior and thus was unable to appropriately monitor for suspicious activities."

4. SAR Reporting: - Filed only 15 SARs in a 3 year period.
   - Failed to file SAR after Law Enforcement seized $1.5 million from MSB owner/member.

5. Review 314(a) lists: Failed to review lists for 2 years.

FinCen Fine: $300,000

Result: Liquidiation

Case Study 2:

BETHEX FEDERAL CREDIT UNION

- FOM: low-moderate income in Bronx, NY
- Employees: 22
- Maintained internal controls to its membership since 2002.
- In 2011, began servicing MSBs, including those in high risk jurisdictions with high risk activities (wires to Middle East). Did not update internal controls.
- Relied on vendor for Due Diligence and monitoring of MSBs.

LSCU

Bethex's compliance with BSA:

1. Internal Controls
   - In 2010, Bethex processed $657 million domestic transactions.
   - In 2012, Bethex processed over $4 billion in domestic and international transactions, an increase of more than 300% with modifying its controls. **Generated high fee income.**
   - Failed to conduct risk assessment while transacting in 30 countries, some high risk.
   - Failed to perform Due Diligence – four MSBs owned by one person at one address, serviced one Mexican MSB wasn't monitored.
   - Failed to monitor suspicious activities, had insufficient staff.
2. BSA Officer
   - Failed to have BSA officer with sufficient experience, authority, and resources to ensure compliance.
   - Willfully undermined controls by sending multiple wires under policy threshold.

Bethex's compliance with BSA:

3. Audit: Ignored auditor findings.
4. Training- Inadequate

- Suspicious Activity Reporting:
  - Failed to file SARs for wires with high dollar amounts to Middle East.
  - SARs were filed late and were inadequate.

FinCen Fine: $500,000

Result: Liquidiation

Takeaways from FinCEN Enforcement Actions

1. Internal Controls:
   - Don't rely on 3rd party vendors for compliance.
     - Properly monitor & manage software.
   - Don't wire money abroad.
   - Don't service MSBs.
   - Do - Update controls annually, specifically when introducing new products and services.
2. BSA Officer- Hire sufficient and competent staff
3. Training- Annual training for Board and relevant employees.
4. Audit:
   - Independent.
   - Listen to them.

LSCU Compliance Assistance

Compliance Resources

- Access to LSCU Compliance Staff (compliance@lscu.coop) with a 24-hour or less response time to compliance questions.
- Weekly InfoSight compliance e-newsletter.
- Monthly PolicyPro newsletter.
- Quarterly Custom Performance Reports.
- Dues-supported compliance calls on timely topics.
- Compliance related training.
- Policy reviews (fee-based).
- Shared Compliance Consultant Program (fee-based).

Compliance Tools

- Found under the LSCU Compliance Tab.
  - **InfoSight:** Online compliance manual including federal and state-specific information, available 24/7.
  - **PolicyPro:** Online compliance manual and model policies customizable to your CU.
  - **ComplySight:** Provides visibility, tracking, measuring and reporting for compliance activities through a single application (fee-based).
  - **RecoveryPro:** Runs on the same platform as PolicyPro. Provides an outline of what credit unions need to create multiple business continuity plans (fee-based).

Maximizing LSCU Affiliation

COMPLIANCE AND REGULATORY SERVICES

Membership is what you make of it!

- Create a login & sign up for emails at LSCU.coop
- Utilize free tools & your LSCU Liaison!
- Follow LSCU on social media & download our app
- Connect with your *LEVERAGE* Business Development Consultant for partner recommendations
- Encourage young professionals to register for LSCU's YPG

LSCU young professionals

Southeastern Credit Union Foundation
Charity. Community. Cooperation.

LSCU Councils

LSCU

Thank you for your time and enjoy Point Clear!

Alisha Stair, BSACS
Member Engagement Consultant
LSCU & Affiliates
Email: alisha.stair@lscu.coop
Phone: 217.853.4282

LSCU
League of Southeastern Credit Unions & Affiliates