



Bank Secrecy Act/Anti-Money Laundering for Board Members

Michigan Credit Union League
July 10, 2009

Robert Zalewski
CUcorp Compliance Consultant
Robert.Zalewski@CUcorp.com
1-800-262-6285 ext. 493

Overview of Presentation

- Background and Purpose of BSA/AML
 - Identifying Illegal Transactions
- BSA/AML Program Requirements
- Bank Secrecy Act Risk Assessment
- Bank Secrecy Act Policy
- Bank Secrecy Act Reporting Requirements
- Member Identification Program & Monitoring
- OFAC
- USA Patriot Act



Background and Purpose of Bank Secrecy Act

BSA/AML Background

Purpose:

- To help identify the source, volume and movement of currency and other monetary instruments transported or transmitted into or out of the U.S. or deposited into financial institutions.
- To aid in the investigation of money laundering, tax evasion, international terrorism and other criminal activity.

Identifying Illegal Transactions

Money Laundering

- The criminal practice of processing “dirty” money through a series of transactions in order to “clean” the funds so that they appear to be proceeds from legal activities.
- May not involve currency (cash) at every stage of the laundering process.
- Generally involves three independent steps (that can occur at the same time).

Identifying Illegal Transactions

Terrorist Financing

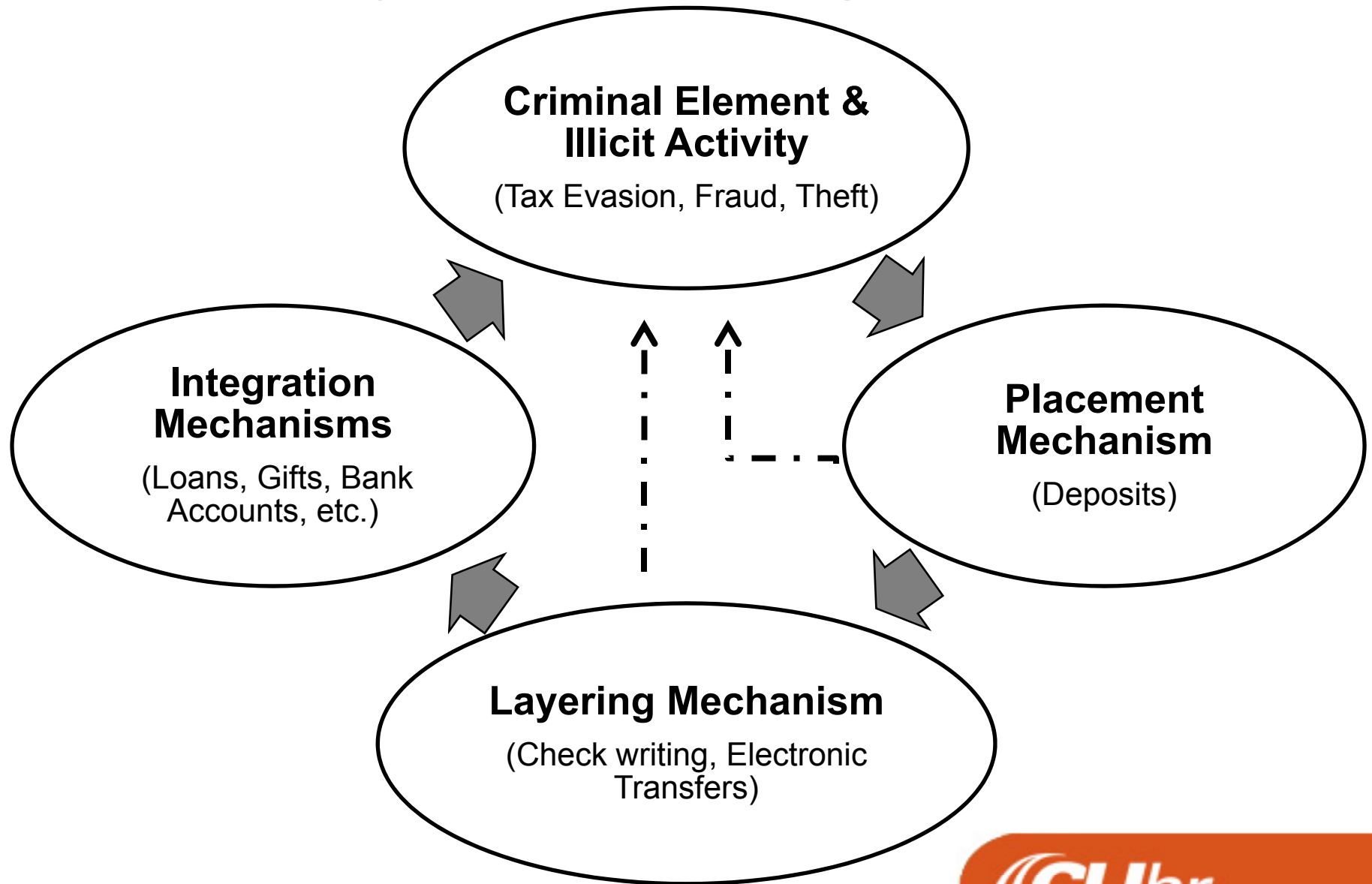
- Activities are often funded through legitimate sources.
 - Charitable donations
 - Business ownership
 - Personal employment
- Money laundering is often a component.
 - Structured deposits or withdrawals
 - Purchases of monetary instruments, or stored value cards
 - Wire transfers

Identifying Illegal Transactions

Money Laundering

- Placement: Structuring currency deposits in amounts to evade reporting requirements, or commingling currency deposits of legal and illegal activities.
- Layering: Moving funds around the financial system, often in a complex series of transactions.
- Integration: Creating the appearance of legality through additional transactions. Examples: the purchase and resale of real estate or other assets.

Money Laundering Example





Bank Secrecy Act/Anti-Money Laundering Program

Risk Based Program Requirements

BSA/AML Program

- Examiner will look determine if the credit union has an effective program for BSA/AML compliance.
- Policies, procedures, internal controls, training, and audit process will be evaluated.
- Must be written, approved by the board of directors annually, and noted in the board minutes.
- Risk assessment will be completed by examiners if one is not available for review.

Penalties for BSA Violations

- Credit unions
 - Cease and Desist Order
 - Loss of charter (criminal and civil).
 - Criminal money penalties up to the greater of \$1 million or twice the value of the transaction.
 - Civil money penalties.

Penalties for BSA Violations (cont.)

- Individuals
 - Removal and bar from banking (criminal and civil).
 - Criminal fine of up to \$250,000, five years in prison, or both for willful violations of the BSA and for structuring transactions to evade BSA reporting requirements.
 - Criminal fine of up to \$500,000, ten years in prison, or both for violating BSA and any other U.S. law or engaging in a pattern of criminal activity.
 - Civil money penalties.



Bank Secrecy Act Risk Assessment

BSA Risk Assessment

- The risk assessment, identifies the risk for each of the following:
 - Products & services;
 - Members; and
 - Geographic locations.
- Assessments must change as new products and services are introduced, strategic plans change, or field of membership changes.
- Ongoing updating required.

Risk Assessment Considerations

- What types of products and services does the credit union offer?
- Who is using them?
- Where is the potential exposure to money laundering?
- What steps have been taken to mitigate risk?

BSA Risk Assessment Considerations

Federal Financial Institution Examination Council has developed an Examination Manual to ensure consistent evaluation of BSA/AML Compliance Programs.

- BSA/AML Risks are in Appendix J
- Office of Foreign Assets Control are in Appendix M

BSA/AML Risk Assessment Factors

Membership

Low	Moderate	High
Stable, known membership base.	Membership base increasing due to branching, merger, or acquisition.	A large and growing membership base in a wide and diverse geographic area.

BSA/AML Risk Assessment Factors

Products Offered – Electronic Banking

Low	Moderate	High
No electronic banking (e-banking) or the web site is informational or non-transactional.	The credit union is beginning e-banking and offers limited products and services.	The credit union offers a wide array of e-banking products and services (i.e., account transfers, <u>e-bill payment</u> , or accounts opened via the Internet).

BSA/AML Risk Assessment Factors

Large Currency/Structured Transactions

Low	Moderate	High
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.

BSA/AML Risk Assessment Factors

Membership – High Risk Customers/Businesses

Low	Moderate	High
Identified a few high-risk customers and businesses.	Identified a moderate number of high-risk customers and businesses.	Identified a large number of high-risk customers and businesses.

BSA/AML Risk Assessment Factors

International Relationships

Low	Moderate	High
Few international accounts or very low volume of currency activity in the accounts.	Moderate level of international accounts with unexplained currency activity.	Large number of international accounts with unexplained currency activity.

BSA/AML Risk Assessment Factors

Funds Transfers

Low	Moderate	High
A limited number of funds transfers for members, non-members, limited third-party transactions, and no foreign funds transfers.	A moderate number of funds transfers. A few international funds transfers from personal or business accounts with typically low-risk countries.	A large number of non-member funds transfer transactions and payable upon proper identification (PUPID) transactions. Frequent funds from personal or business accounts to or from high-risk jurisdictions, and financial secrecy havens or jurisdictions.

BSA/AML Risk Assessment Factors

Geographic Locations Served

Low	Moderate	High
The credit union is not located in a High Intensity Drug Trafficking Area (HIDTA) or High Intensity Financial Crime Area (HIFCA). No fund transfers or account relationships involve HIDTAs or HIFCAs..	The credit union is located in an HIDTA or an HIFCA. Credit union has some fund transfers or account relationships that involve HIDTAs or HIFCAs.	Credit union is located in an HIDTA and an HIFCA. A large number of fund transfers or account relationships involve HIDTAs or HIFCAs.

BSA/AML Risk Assessment Factors

Geographic Locations Served

Low	Moderate	High
No transactions with high-risk geographic locations.	Minimal transactions with high-risk geographic locations.	Significant volume of transactions with high-risk geographic locations.

Risk Assessment – Geographic Location

- Domestic high-risk geographic locations include:
 - High Intensity Drug Trafficking Areas (HIDTAs)
 - <http://www.whitehousedrugpolicy.gov/hidta/>
 - High Intensity Financial Crime Areas (HIFCAs)
 - www.irs.gov/compliance/enforcement/article/0,,id=107488,00.html#hifca
 - http://www.fincen.gov/le_hifcadesign.html
- Michigan HIDTA counties:
 - Wayne, Macomb, Oakland, Washtenaw, Genessee, Kent, Kalamazoo, Allegan and Van Buren

BSA/AML Risk Assessment Factors

Key Personnel and Frontline Personnel Turnover

Low	Moderate	High
Low turnover of key personnel or frontline personnel (i.e., customer service representatives, tellers, or other branch personnel).	Low turnover of key personnel, but frontline personnel in branches may have changed.	High turnover, especially in key personnel positions.

BSA/AML Risk Assessment Factors

Products and Services Offered

Low	Moderate	High
The credit union offers limited or no private banking services or trust and asset management products or services.	The credit union offers limited domestic private banking services or trust and asset management products or services over which the CU has investment discretion. Strategic plan may be to increase trust business.	The credit union offers significant domestic and international private banking or trust and asset management products or services. Private banking or trust and asset management services are growing.

Risk Assessment Summary

Risk Factor [Product/ Service; Members; Geographic Location]	Degree of Risk (low, med., high)	Areas of Concern	Risk Controls

Risk Assessment Summary

Risk Factor	Degree of Risk	Areas of Concern	Risk Controls
Membership	Medium	Customer base increasing due to a new branch opening.	<ol style="list-style-type: none">1. Strong MIP Program2. Strong Customer Due Diligence Procedures3. Processing system combines cash transactions.4. Reports monitored daily.5. Ongoing BSA Training of all staff and Board.



Bank Secrecy Act Policy

Policy Provisions

- Board of directors ultimately responsible for ensuring the credit union has an effective BSA/AML program.
- Policy requirements include (not all inclusive):
 - Periodically updating the risk assessment.
 - Informing board of compliance initiatives and deficiencies, actions taken and SARs filed.
 - Designate a BSA/AML compliance officer.
 - Establish a Member Identification Program.
 - Provide for timely updates in response to changes in regulations.
 - Establishment of an annual training program.

Independent Testing

- BSA/AML program needs to be independently reviewed by the internal audit department, outside auditors, or other qualified independent parties.
- Report to the board.
- Risk-based, covering all of the credit union's activities.
- Should, at a minimum, include the following:
 - An evaluation of the overall integrity and effectiveness of the BSA/AML compliance program, including policies, procedures and practices.
 - A review of the credit union's risk assessment for reasonableness, given the credit union's risk profile.



Bank Secrecy Act Reporting Requirements

Reporting Requirements

- Suspicious Activity Reports (SARs)
 - SARs are Secret!
- Currency Transaction Reports (CTRs)
- Currency Transaction Report Exemptions

Suspicious Activity Reports

The statement of the Bank Secrecy Act Advisory Group on unauthorized disclosure of information from Bank Secrecy Act Suspicious Activity Reports follows:

The unauthorized disclosure of Suspicious Activity Reports is not only a violation of federal criminal law, but it undermines the very purpose for which the suspicious activity reporting system was created - the protection of our financial system through the prevention, detection, and prosecution of financial crimes and terrorist financing. The unauthorized disclosure of Suspicious Activity Reports can compromise the national security of the United States as well as threaten the safety and security of those institutions and individuals who file such reports.

8/14/04

SAR Filing – Clearly Defined

Credit unions are required to file a SAR with respect to the following types of financial losses:

- Criminal violations involving insider abuse in any amount.
- Criminal violations aggregating \$5,000 or more when a suspect can be identified.
- Criminal violations aggregating \$25,000 or more regardless of a potential suspect.

SAR Filing

Money Laundering & Terrorist Financing

See FFIEC BSA Exam Manual Appendix F: Money Laundering and Terrorist Financing “Red Flags”

- Members not willing to provide full information
- Funds transfers & ACH activity (what to look for)
- Activity inconsistent with a Member’s Business
- Lending Activity
- Employee Activity
- Trade Finance

SAR Filing

Structuring Transactions

See FFIEC BSA Exam Manual Appendix G: Structuring

Definition:

“a person structures a transaction if that person, acting alone, or in conjunction with, or on behalf of, other persons, conducts or attempts to conduct one or more transactions in currency in any amount, at one or more financial institutions, on one or more days, in any manner, for the purpose of evading the [CTR filing requirements].”

Suspicious Activity Report Policy & Procedures

Policies and procedures need to address:

- Completing, filing and retaining SARs and their supporting documentation;
- Reviewing and evaluating the transaction activity of subjects included in law enforcement requests (i.e. subpoenas, section 314(a) requests, and National Security Letters); and.
- Reporting SARs to the board of directors, or a committee thereof, and senior management.

Suspicious Activity Reports – Timing

- SARs must be filed no later than 30 calendar days from the date of the initial detection of the suspicious activity (60 calendar days if no suspect can be identified).
- For financial institutions wanting to report suspicious transactions that ***may relate to terrorist activity***. Financial institutions should immediately report any imminent threat to local-area law enforcement officials.
- Board of directors must be notified that SARs have been filed.

Suspicious Activity Reports (record retention)

- Must retain copies of SARs and supporting documentation for 5 years from the date of the report.
 - “Supporting documentation” refers to all documents or records that assisted the credit union in making the determination to file a SAR.
 - Must provide all documentation supporting the filing of a SAR upon request to FinCEN, an appropriate law enforcement agency, and/or a supervisory agency.

Suspicious Activity Reports

Continuing Activity on an account with Suspicious Activity

- File a SAR at least every 90 days.
- Policies and procedures should include the following:
 - Review by senior management and legal staff (i.e., BSA compliance officer or SAR committee).
 - Criteria for when to close the account.
 - Criteria for when to notify law enforcement, if applicable.
- If a law enforcement agency requests keeping an account opened, the credit union should ask for the request in writing.

Suspicious Activity Reports - Safe Harbor

- Credit union directors, officers, employees and agents that reports a suspicious transaction to the appropriate authorities are granted a safe harbor from any civil liability under any law or regulation.
- This safe harbor applies to SARs filed within the required reporting thresholds as well as those filed voluntarily on any activity below the threshold.

Suspicious Activity Reports - Secrecy

- No disclosure to anyone involved in the transaction that a SAR has been filed.
 - May ONLY inform FinCEN, law enforcement or federal banking agencies.
 - Notify FinCEN and regulator regarding requests to disclose.
- No requirement to investigate or confirm the underlying crime.
- Use of the “Other” category should be limited to situations that cannot be broadly identified.

Currency Transaction Reports

- Must be filed for each deposit, withdrawal, payment, transfer or other transaction involving currency (cash) of ***more than*** \$10,000.
- Multiple transactions by or on behalf of one person in one business day: consolidate the transactions and report them as one if the total exceeds \$10,000.
- Must be filed within 15 days after the date of the transaction (25 days if filed magnetically or electronically).

Currency Transaction Reports

- Be aware of structured transactions designed to avoid CTR reporting.
- Management should ensure that the credit union has an adequate system to monitor accounts to detect currency transactions that when combined exceed \$10,000.
- Must verify and record the following in the report:
 - Member's name, address, account number and social security number (or tax identification number).

Currency Transaction Reports

- If a report is inaccurate or incomplete, you may be fined \$500. If there is a pattern of negligent violations, the fines can be higher.
- Backfiling - If the credit union has failed to file CTRs on reportable transactions:
 - Begin to file them; and
 - Contact the IRS Detroit Computing Center to find out whether the backfiling of unreported transactions is necessary.
- Keep CTRs for 5 years from the date of the report.

Currency Transaction Report Exemptions

- Credit unions may exempt certain members from currency transaction reporting.
- Must file a the Designation of Exempt Person form with the Internal Revenue Service (IRS)
- Two types of exemptions:
 - Phase I
 - Phase II

CTR Exemptions - Update

Financial Crimes Enforcement Network (FinCEN) rules change effective January 5, 2009.

- Depository institutions will no longer be required to review annually or make a designation of exempt person (DOEP) filing for customers who are other depository institutions, U.S. or State governments, or entities acting with governmental authority.
- Depository institutions will be able to designate an otherwise eligible non-listed company or a payroll customer after either two months time (previously twelve months) or after conducting a risk-based analysis.

CTR Exemptions – Update (continued)

- Definition of “frequent” transactions will be changed to five transactions per year instead of the current eight.
- Depository institutions will no longer be required to biennially renew a designation of exempt person filing for otherwise eligible Phase II customers, but an annual review of these customers must still be conducted.
- Depository institutions will no longer be required to record and report a change of control in a designated non-listed or payroll customer.

Currency Transaction Reports

Phase I Exemptions

These exemptions are for those members or entities that are financial institutions, government entities, or publicly traded.

- Categories:
 - Companies traded on NYSE or NASDAQ..
 - Subsidiaries of companies traded on NYSE or NASDAQ. (at least 51% of common stock must be owned by the listed entity).
- Exemptions need to be confirmed annually.

Currency Transaction Report Phase II Exemptions

Businesses that would frequently be filing a CTR, but that has a legitimate purpose for the transactions.

Credit Union will need to document that:

- The business has maintained a transaction account at the exempting credit union for at least 2 months;
- Frequently (at least 5) engages in currency transactions with the credit union in excess of \$10,000; and
- Is legally incorporated or organized under the laws of the U.S. or a state,.

Currency Transaction Reports Exemptions

Ineligible Businesses

Certain businesses are ***ineligible*** for treatment as an exempt non-listed business. Examples of ineligible businesses include (see the Fincen guidance):

- Car dealers (and dealers of all motor vehicles including vessels, aircraft, farm equipment or mobile homes.)
- Businesses practicing law, accounting or medicine.
- Investment advisors.
- Real estate brokerage and title insurance companies.
- Trade unions.
- Auctioneers, & pawn brokers.
- Any other business specified by FinCEN.



Member Identification Program and Ongoing Monitoring

Member Identification Program

Member Verification

- Must be written, approved by the board and incorporated in the compliance program.
- The MIP must contain risk-based procedures for verifying the identity of the member within a reasonable time after the account is opened.
- Must verify enough information to form a reasonable belief that it knows the true identity of the member.
- Procedures must describe when it will use documents, non-documentary methods, or a combination of both.

Member Identification Program

Documentary Methods

- Procedures must set forth minimum acceptable documentation.
- Individuals
 - Encouraged to review more than one document
 - Unexpired government-issued form of identification
- “Persons” other than individuals (corp., partnership or trust)
 - Certified articles of incorporation
 - Unexpired government-issued business license
 - Partnership agreement
 - Trust instrument
 - Identification of signatories, sole proprietor or partners - ONLY when identity cannot be obtained using either method

Member Due Diligence Program

- Member Due Diligence (MDD) Program
 - Begins with verifying the member's identity and assessing the risks associated with that member.
 - Enables the prediction of the types of transactions in which a member is likely to engage.
 - Assists in determining when transactions are potentially suspicious.
 - Should include an enhanced MDD for high-risk members and ongoing due diligence of that member base.

Member Due Diligence Program

- Credit unions should monitor its lower-risk members through regular suspicious activity monitoring and MDD processes.
 - If there is a potential change in the member's risk profile, management should reassess the member's risk rating and follow established policies and procedures for maintaining or changing member risk ratings.
- Periodic risk-based monitoring of the member relationship to determine whether there are any substantive changes to the original information.

Member Due Diligence Program

- For high-risk members, the credit union should consider obtaining, both at account opening and throughout the relationship, the following information:
 - Purpose of the account.
 - Source of funds and wealth.
 - Beneficial owners of the account, if any.
 - Member's (or beneficial owner's) occupation or type of business.

Member Due Diligence

FFIEC Examination Procedures specifically address the following type of businesses (not all inclusive):

- Non-bank financial institutions (e.g., money services businesses; casinos; brokers/dealers in securities; and dealers in precious metals, stones, or jewels).
- Deposit brokers.
- Cash-intensive businesses (e.g., convenience stores, restaurants, retail stores, liquor stores, cigarette distributors).
- Non-governmental organizations and charities.
- Professional service providers (e.g., attorneys, accountants, doctors, or real estate brokers).



Office of Foreign Assets Control (OFAC) Compliance

OFAC

- An office of the U.S. Treasury that administers and enforces economic and trade sanctions based on U.S. foreign policy and national security goals.
- Requirements are separate and distinct from the BSA, but they share a common national security goal.
- OFAC regulations require the following:
 - Block accounts and other property of specified countries, entities and individuals.
 - Prohibit or reject trade and financial transactions with specified countries, entities and individuals.
 - Reporting blocked transactions to OFAC.

OFAC – Policy and Procedures

- Policies and procedures need to ensure that the credit union does not enter into transactions with individuals or organizations that are on the Specially Designated Nationals List.
- OFAC Compliance Program needs to be risk based.
- OFAC Risk Assessment considerations are similar to BSA/AML risk considerations.
 - FFIEC BSA/AML Examination Manual, Appendix M – OFAC Procedures

OFAC – Blocked Transactions

- Financial institutions must block transactions that are:
 - By or on behalf of a blocked individual or entity;
 - Are to or through a blocked entity; or
 - Are in connection with a transaction in which a blocked individual or entity has an interest.

OFAC – Prohibited Transactions

- Prohibited transactions with no blockable interest in the transaction (i.e., transaction should not even be accepted).
- In these cases, the transaction is simply rejected.
- Examples: transfers between Specially Designated Nationals or Blocked Persons (SDNs).



USA Patriot Act

Information Sharing

- Sections 314(a) and (b) of the USA PATRIOT Act.
- Two types of information sharing:
 - Between the law enforcement and financial institutions [314(a)]; and
 - Between financial institutions [314(b)].
- Policies, procedures and processes should cover how to respond to 314(a) requests and for sharing and receiving under 314(b).

Information Sharing 314(a) Requests

- Between the Credit Union and Law Enforcement
 - FinCEN may require a credit union to search its records to determine whether it maintains or has maintained accounts for, or engaged in transactions with a specified person, entity or organization.
 - Must search accounts maintained during the last 12 months, and transactions conducted outside of an account by or on behalf of a named suspect during the preceding 6 months.
 - Must report to FinCEN within 14 days, unless the request specifies otherwise.
 - Only report that there is a match.
 - No need for negative responses.

Information Sharing 314(a) Requests (cont.)

- Requests should not be the sole basis for filing SARs.
 - May be relevant and, if filed, confidential information must be kept off of the form (ex: grand jury subpoenas).
- **Must be kept confidential.**
- May provide match information over FinCen's Web site.

Information Sharing

314(a) Requests (cont.)

- Document that required searches were performed.
 - Can be done by photocopying the cover page of the request with a sign-off that the records were checked, the date of the search and the search results.
 - Retain copy of the form resulting in positive matches, along with the supporting documentation.
- Requests may be mailed, posted on FinCEN's secure Web site or faxed.
- If third party is handling search, ensure confidentiality.

Thank You!

Robert Zalewski

CUcorp Compliance Consultant

Robert.Zalewski@CUcorp.com

1-800-262-6285 ext. 493

(248) 925-8131