BANK SECRECY ACT / ANTI-MONEY LAUNDERING (BSA/AML) COMPLIANCE

March 11, 2012
Shawn Wolbert
MCUL & Affiliates
Overview of Presentation

- BSA Acronyms
- Purpose
- Pre-Exam Review
- Compliance Program
  - Risk Assessment
  - Internal Controls
    - Monitoring
    - Reporting
    - Recordkeeping
  - Independent Testing
- Compliance Officer
- Training
- Customer Identification (CIP)
- Information Sharing
- Penalties for Non-Compliance
- OFAC
BSA/AML Acronyms

• **BSA/AML** – Bank Secrecy Act/Anti-Money Laundering

• **FFIEC** – Federal Financial Institutions Examination Council
  – Prescribes uniform BSA principles, standards
  – Provides report forms for the federal examination of financial institutions
  – Makes recommendations to promote uniformity in the supervision of financial institutions
  – Provides the BSA/AML Examination Manual
BSA/AML Acronyms

• **FinCEN** – Financial Crimes Enforcement Network
  – Bureau of the U.S. Treasury that administers the BSA
  – Issues regulations, provides guidance, supports examination functions

• **OFAC** - Office of Foreign Assets Control
  – Division of the U.S. Treasury that administers and enforces U.S. economic trade sanctions
BSA/AML Purpose

• 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
Why BSA Board Training?

• FFIEC BSA/AML Manual:
  – “While the board of directors may not require the same degree of training as banking operations personnel, they need to understand the importance of BSA/AML regulatory requirements, the ramifications of noncompliance, and the risks posed” to the credit union

• Board training must provide for a general understanding of the BSA
Pre-Exam Review

• Review of BSA database reporting information
  – Inconsistencies between credit union records and reporting databases
• Review of prior exam and management’s responses to previously identified BSA violations
• Review of correspondence between the credit union and FinCEN or the IRS Detroit Computing Center
  – Whether management has taken corrective action
Pre-Exam Review

• Contact management and BSA compliance officer
  – BSA/AML compliance program, management structure and risk assessment
  – Suspicious activity monitoring and reporting system
  – Level and extent of automated BSA/AML systems
COMPLIANCE PROGRAM

Every credit union must have a written compliance program that is tailored to its level of risk.
Compliance Program

• Directors are responsible for ensuring that their credit unions have a written BSA compliance program that is tailored to its level of risk
  – Written policies, procedures and processes

• Must be written, approved by the board of directors and noted in the board minutes
Compliance Program

• Made up of the following:
  – Risk Assessment
  – Internal Controls
  – Independent Testing
  – Designation of BSA/AML Compliance Officer
  – Training
  – Customer (Member) Identification Program (CIP)
RISK ASSESSMENT

The risk assessment will determine the policies, procedures and processes for BSA/AML compliance
Risk Assessment

Risk Assessment Link to the BSA/AML Compliance Program

Risk Assessment
- Identify & Measure Risk:
  - Products
  - Services
  - Customers
  - Geographies

Internal Controls
- Develop Applicable:
  - Policies
  - Procedures
  - Systems
  - Controls

Result

Risk-Based BSA Compliance Program
- Internal Controls
- Audit
- BSA Compliance Officer
- Training
Risk Assessment

• The risk assessment, though the use of a Risk Matrix, should identify and measure the degree of risk for each of the following:
  – Products & services;
  – Members; and
  – Geographic locations
• Identify steps that have been taken to mitigate risk
• Should evolve as new products and services are introduced or changed, expansions occur through mergers, and/or field of membership enlarges
• Recommended every 12 to 18 months
Risk Assessment – Risk Matrix

• Product/Service; Members; Geographic Location
• Degree of Risk (low, medium, high)
• Areas of Concern
• Risk Controls
Risk Assessment – Products and Services

• 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?
Risk Assessment - Members

• Who does your credit union serve?
• What services do they use?
• What is their source of funds?
• Where are they located?
Risk Assessment – Geographic Location

• High-risk locations can be foreign or domestic.
• Domestic high-risk geographic locations include:
  – High Intensity Drug Trafficking Areas (HIDTAs)
  – High Intensity Financial Crime Areas (HIFCAs)
    • [www.irs.gov/compliance/enforcement/article/0,,id=107488,00.html#hifca](http://www.irs.gov/compliance/enforcement/article/0,,id=107488,00.html#hifca)
    • [http://www.fincen.gov/le_hifcadesign.html](http://www.fincen.gov/le_hifcadesign.html)
• Michigan HIDTA counties:
  – Wayne, Macomb, Oakland, Washtenaw, Genesee, Kent, Kalamazoo, Allegan and Van Buren
INTERNAL CONTROLS

Written policies, procedures and practices must be designed to limit and control risks, and to achieve compliance with the BSA.
Internal Controls

• Made up of the credit union’s:
  – Monitoring
  – Reporting
    • Currency Transaction Reports (CTRs)
      – CTR Exemptions
    • Suspicious Activity Reports (SARs)
  – Recordkeeping
Internal Controls

• Board ultimately responsible for ensuring the credit union has an effective internal control structure

• Policies, procedures and processes should be in place to monitor and identify unusual activity

• The level of monitoring is dictated by the credit union’s risk assessment, with an emphasis on high-risk products, services, members and geographic locations
Internal Controls - Monitoring

• Monitoring systems typically include:
  – Employee identification or referrals;
  – Manual systems;
  – Automated systems; or
  – Any combination

• Member Due Diligence Program
Internal Controls – Monitoring 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
  – Keep current member information
Internal Controls - Reporting

- BSA requires financial institutions to file the following reports with the Financial Crimes Enforcement Network (FinCEN):
  - Currency Transaction Reports (CTRs)
    - CTR Exemption Forms (if applicable)
  - Suspicious Activity Reports (SARs)
CURRENCY TRANSACTION REPORTS

Examiner will assess compliance with the statutory and regulatory requirements for large currency transaction reporting
Internal Controls - Reporting
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
- May be fined up to $10,000 per day for each CTR not filed
Internal Controls - Reporting Currency Transaction Reports

• Examples of reportable transactions:
  – Denomination exchanges, IRAs, loan payments, ATM transactions, purchases of certificates of deposit, deposits and withdrawals, funds transfers paid in currency, and monetary instrument purchases

• Management should ensure that the credit union has an adequate system to:
  – Aggregate currency transactions throughout the credit union; and
  – Appropriately report currency transactions subject to the BSA requirement
CTR Exemptions

• Credit unions may exempt certain types of members from currency transaction reporting

• Must file a Designation of Exempt Person form with the Internal Revenue Service (IRS)

• Two types of exemptions (Phase I and Phase II)

• **Must begin filing electronically on March 31, 2013**
  
  – For those unable to meet this deadline, FinCEN will consider, based upon certain limited hardship exceptions, specific requests to file the most current paper forms for up to one year past the mandatory electronic filing deadline
CTR – Entities Ineligible for Exemption

Certain businesses are **ineligible** for treatment as an exempt non-listed business:

- Serving as a financial institution or as agents of one (of any type)
- Purchasing or selling motor vehicles of any kind, vessels, aircraft, farm equipment or mobile homes
- Practicing law, accounting or medicine
- Auctioning of goods
- Chartering or operation of ships, buses or aircraft.
- Operation of a pawn brokerage
- Engaging in gaming (other than licensed pari-mutuel betting at race tracks)
CTR – Entities Ineligible for Exemption

- Engaging in gaming (other than licensed pari-mutuel betting at race tracks)
- Engaging in investment advisory services or investment banking services
- Operating a real estate brokerage
- Operating in title insurance activities and real estate closings
- Engaging in trade union activities
- Engaging in any other activity that may, from time to time, be specified by FinCEN

• A business that engages in multiple business activities – must have no more than 50% of its gross revenues per year are derived from one or more of the ineligible activities listed
Currency Transaction Reports
Exemption Safe Harbor

• Safe harbor from civil penalties for the failure to file a CTR for transactions in currency by an exempt person, unless the credit union knowingly provides false or incomplete information, or has reason to believe that the member does not qualify as an exempt member
  – Safe harbor does NOT apply to the filing of suspicious activity reports (SARs). The credit union must still retain records of funds transferred, or records in connection with the sale of monetary instruments to that person
 Examiner will assess policies, procedures, processes and overall compliance with statutory and regulatory requirements for monitoring, detecting and reporting suspicious activities
Internal Controls – Reporting SAR

• Credit unions are **required** to file a SAR with respect to the following:
  – 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
Internal Controls – Reporting SARs

– Transactions conducted or attempted by, at or through a credit union aggregating $5,000 or more, of the credit union knows, suspects or has reason to suspect that the transaction:
  • May involve potential money laundering or other illegal activity
  • Is designed to evade the BSA or its implementing regulations
  • 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
Internal Controls – Reporting SARs

• 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
• Board must be notified that SARs have been filed
• Must begin filing electronically on March 31, 2013
  – For those unable to meet this deadline, FinCEN will consider, based upon certain limited hardship exceptions, specific requests to file the most current paper forms for up to one year past the mandatory electronic filing deadline.
Internal Controls – Reporting SARs

• Examiners will look to the credit union’s overall decision-making process, not individual SAR decisions
• Individual SARs may be reviewed to determine the overall effectiveness of the SAR monitoring, reporting and decision-making process
• Failure to file a SAR will not be criticized unless the failure is significant or accompanied by evidence of bad faith
• Documenting SAR decisions is recommended
Internal Controls – Reporting SARs

• Must retain copies of SARs and supporting documentation for 5 years from the date of the report

• NO disclosure to anyone involved in the transaction that a SAR has been filed
  – May inform FinCEN, law enforcement or federal banking agencies
  – May share the SAR, or any information that would reveal the existence of the SAR, with an affiliate, provided the affiliate is subject to a SAR regulation
SAR 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, regardless of whether such reports are filed pursuant to the SAR instructions
  – This safe harbor applies to SARs filed within the required reporting thresholds as well as those filed voluntarily on any activity below the threshold
Internal Controls – Recordkeeping

• Funds Transfers of $3,000 or above
  – Originating credit union
  – Intermediary institution
  – Beneficiary’s institution

• Money instrument sales between $3,000 and $10,000

• Records of both must be retained for 5 years
INDEPENDENT TESTING

Examiner will obtain and evaluate the supporting documents of the independent testing of the credit union’s BSA/AML compliance program.
Independent Testing

• Should be conducted by the internal audit department, outside auditors, or other qualified \textit{independent} parties – at least every 12 to 18 months
• Results reported to the board
• Risk-based, covering all of the credit union’s activities
  – Program effectiveness
  – Risk assessment evaluation
  – Personnel knowledge and adherence
BSA COMPLIANCE OFFICER(S)

Board must designate a qualified employee(s) to serve as the BSA compliance officer
BSA Compliance Officer(s)

• Must be appointed (NCUA Part 748.2)
• Responsible for management of the credit union’s BSA compliance program
• Board must ensure the BSA compliance officer(s) has the sufficient authority and resources to administer the compliance program
• Line of communication should allow the BSA compliance officer(s) to regularly apprise the board and senior management of ongoing BSA compliance
TRAINING

All appropriate personnel must be trained in the applicable aspects of the BSA
Training

• All staff whose duties require knowledge of the BSA, tailored to their specific responsibilities
• Should be ongoing, as regulations and staff change
• Should include regulatory requirements and the credit union’s internal policies, procedures and processes
• Inform board and senior management of changes to the BSA and the implementing regulations
• Document training program
  – Materials, dates and attendance records
Training

• The following elements should be included in the training program and materials:
  – The importance the board of directors and senior management place on ongoing education, training and compliance
  – Employee accountability for ensuring BSA compliance
  – Comprehensiveness of training, considering specific risks of individual business lines
  – Training of personnel from all applicable areas of the credit union
  – Penalties for non-compliance
CUSTOMER/MEMBER IDENTIFICATION PROGRAM (CIP/MIP)

The compliance program must include a written CIP/MIP for all members who open an account after October 1, 2003
Customer Identification Program

• Must be written, approved by the board and incorporated in the compliance program

• Must include:
  – Account opening procedures that specify the identifying information obtained from each member; and
  – Reasonable and practical risk-based procedures for verifying the identity of each member
  – Comparison of identity with government lists

• Must retain the identifying information for 5 years after the account is closed
  – Not required to make and retain copies of photocopies, but if this is done, security must be ensured
INFORMATION SHARING

Examiner will assess compliance with the statutory and regulatory requirements for information sharing
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)]
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 during the past 12 months (or 6 months if there is a transaction where no account is involved)
  – Must report to FinCEN within 14 days, unless the request specifies otherwise

• Sent out once every 2 weeks via secure website

• Must be kept confidential
Information Sharing - 314(b) Requests

- Between financial institutions
- An FI must notify FinCEN of its intent to engage in information sharing, and that it has established and will maintain adequate procedures to protect the information
- A notice to share information is effective for one year
- Should ensure that the other FI or association has filed its required FinCEN notice
- Cannot share SARs or SAR filing information
  - If request relates to a transaction subject to a SAR, disclose only the transaction and member information requested
Information Sharing – National Security Letters (NSLs)

• Written investigative demands that may be issued by the local Federal Bureau of Investigation (FBI) and other federal government authorities to obtain financial records from financial institutions

• Highly confidential – examiners will not review
  – Policies and procedures should be in place to process and maintain confidentiality of NSLs
  – SARs should not include their existence

• Questions regarding NSLs should be directed to the local FBI office
Penalties for BSA Violations

• Credit unions
  – Cease and Desist Order (see “Interagency Guidance”)
  – 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

- 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
Examiner will review the credit union’s OFAC risk assessment and audit to determine the extent to which an OFAC review is necessary during the BSA examination.
OFAC

• 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 unlicensed trade and financial transactions with specified countries, entities and individuals
  – Reporting blocked and prohibited transactions to OFAC
OFAC – Blocked Transactions

• Must block those 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

• When requested to make a funds transfer that falls into one of these categories, execute the order and place the funds into a blocked account
  – Cannot be canceled or amended after it is received by a U.S. financial institution unless authorized by OFAC
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)
OFAC - Reporting

• Blocked transactions – within 10 days of the occurrence, and annually by September 30 (for those blocked as of June 30)
• Prohibited transactions – within 10 days of the occurrence
• Must keep full and accurate record of each blocked and rejected transaction for 5 years after the date of the transaction
• For blocked property, records must be retained for 5 years after the property is unblocked
OFAC Program (Recommended)

- Risk assessment
- Internal controls
  - How transactions will be flagged and reviewed
  - Defining criteria for comparing names to OFAC list
  - How it will be determined which hits are valid or false (investigation)
  - Reassessment of OFAC filtering system
  - Prevention of transactions until comparison is made
  - Updating the OFAC list
  - Process used to block and reject transactions
  - Managing blocked accounts
OFAC Program (Recommended)

- Reporting transactions, blocked accounts and prohibited transactions.
- Maintaining licensing information.

• Independent testing (at least annually)
• Responsible individual
• Training
Resources

- MCUL: [www.mcul.org](http://www.mcul.org) (InfoSight)
- NCUA: [www.ncua.gov](http://www.ncua.gov)
- CUNA: [www.cuna.org](http://www.cuna.org)
- NASCUS: [www.nascus.org](http://www.nascus.org)
- FinCEN: [www.fincen.gov](http://www.fincen.gov)
- IRS Detroit Computing Center: (800) 800-2877
- FinCEN’s Financial Institutions Terrorist Hotline to report terrorist activity against the U.S.: 1-866-556-3974
- FBI: [www.fbi.gov](http://www.fbi.gov)
- OFAC: [www.treas.gov/ofac](http://www.treas.gov/ofac)