



MDIDC
Credit Union Association

BANK SECRECY ACT COMPLIANCE TRAINING FOR VOLUNTEERS

Annual Meeting and Convention

June 4, 2018

ABOUT THIS PROGRAM TODAY

- This program is intended to assist credit union volunteers in complying with BSA/AML, and to further provide guidance and resource information.
- It includes general information that covers the Bank Secrecy Act, and related Anti-Money Laundering requirements.



THE BANK SECRECY ACT

The *Bank Secrecy Act* (BSA), also known as the Financial Record-keeping and Reporting of Currency and Foreign Transactions Act of 1970, was enacted to help in the investigation of money laundering, tax evasion and other criminal activity.



THE BANK SECRECY ACT

The *Bank Secrecy Act* is a combination of various statutes that require financial institutions to obtain and retain certain records, as well as report certain financial transactions to the federal government. Statutes included are the Money Laundering Control Act, Anti-Drug Abuse Act, Currency and Foreign Transactions Reporting Act, and Title III of the USA PATRIOT Act.



THE BANK SECRECY ACT

The *Bank Secrecy Act* and related federal and state law requirements are a critical component of credit union operations. As the first line of defense for financial crimes, credit unions play an important role in minimizing fraud, money laundering, terrorist financing, and other financial crimes.

COMPLIANCE WITH BSA/AML IS DIFFICULT

- What makes compliance with BSA/AML difficult?
- What are some of the biggest challenges facing your credit union?
 1. Training requirements
 2. Understanding BSA/AML risks
 3. BSA/AML program development
 4. Monitoring account activity
 5. OFAC and FinCEN requirements
- What will make compliance with BSA/AML easier?



FOUR MAJOR CHALLENGES COMPLIANCE PROFESSIONALS ARE FACING

1) Enforcement actions and fines for BSA/AML violations

- Fear of enforcement actions/fines is the biggest challenge
- Various forms: civil money penalties, cease & desist orders, charter revocation, & criminal penalties
- Actions can be devastating, as credit unions may not be able to bounce back from the loss



MAJOR CHALLENGES

2) Additional risks to the credit union

- Reputational risk: Adverse publicity regarding business practices and associations
- Operational risk: Losses resulting from inadequate internal processes or systems, or from external events
- Legal risk: Potential lawsuits, adverse judgments, fines and penalties, unenforceable contracts



MAJOR CHALLENGES

3) Growing AML costs

- The money spent on AML programs continues to sky rocket
- Various fines and settlements are being imposed on financial institutions
- Financial institutions are shelling out big bucks for the fear of becoming the next Bethex FCU



MAJOR CHALLENGES

4) Constant changes

- If there is one constant in the BSA/AML industry, it is the prevalence of change
- Changes in regulatory requirements, as well as the way criminals launder money and finance terrorism
- Credit unions face an uphill battle ensuring their AML programs are both sufficient and sustainable as a result of the various compliance challenges



CRITICAL ELEMENTS

Five Pillars of BSA/AML Compliance

- Training for appropriate personnel
- Designated individual responsible
- System of internal controls to ensure compliance
- Risk-based, ongoing customer due diligence
- Independent testing



TRAINING

- All appropriate personnel must be trained in applicable aspects of the BSA
- At a minimum, the training program must provide training to those whose duties require knowledge of the BSA
- Should be tailored to fit specific responsibilities
- Should be ongoing, and documented
- The BSA compliance officer should be trained in all aspects of the BSA as well as the activities and overall BSA/AML risk profile of the credit union



INDIVIDUAL RESPONSIBLE

- BSA Compliance Officer
 1. Designated by the Board of Directors
 2. Coordinates and manages day-to-day BSA/AML compliance
 3. Manages all aspects of the BSA/AML compliance program
 4. Manages the credit union's adherence to the BSA and its implementing regulations
 5. Should be fully knowledgeable of the BSA and all related regulations
 6. Should understand the credit union's products, services, members, entities, and geographic locations along with associated risks
 7. Have sufficient resources to do the job
 8. Have a written definitive job description / Level defined



WRITTEN BSA PROGRAM

- Risk Assessment
- Policy, procedures and processes
- Customer Identification and Due Diligence
- Transaction Monitoring
- CTR and SAR Reporting
- OFAC Requirements
- FinCEN 314(a) and 314(b) Requirements
- Recordkeeping Requirements
- Testing (*Independent and Internal*)
- Training



BSA/AML PROGRAM

Must adequately address the CU's risk profile

Controls should change and grow with the credit union

BSA RISK ASSESSMENT

- The first step in developing a comprehensive BSA/AML program
- Should provide a detailed analysis of the BSA/AML risks in a concise and organized presentation, and should be shared and communicated with all business lines across the credit union, board of directors, management, and appropriate staff



DEVELOPMENT

The development of a BSA/AML Risk Assessment generally involves two steps:

1. Identify specific risk categories unique to the credit union (products, services, membership, entities, transactions, & geographic locations)
2. Conduct a detailed analysis to better assess the risk within each category (*consider volume, dollar amounts, frequency*)



IDENTIFY

- Products & Services: Electronic Banking, Monetary Instruments, Lending Activities (loans secured by cash & marketable securities), Plastic Cards, Branch Services (shared branching), etc.
- Members & Entities: Nonresident Alien, Senior Foreign Political Figure, Professional Service Providers (doctors, attorneys, etc), MSB's, Marijuana-Related Business, etc.
- Geographic Locations: High Intensity Drug Trafficking or Financial Crimes Area, Countries subject to OFAC sanctions (*CU, member, and transaction location*)



STAFF/MANAGEMENT

High staff turnover:

- Upper management (*change in leadership style*)
- BSA staff (*knowledge, experience, etc.*)
- Branch staff – tellers (*training, level of understanding*)
- Information Technology (*security*)
- Lending/collection staff (*fraud*)

Training concerns:

- Front line staff / Designated BSA/AML officer (*risk of non-compliance*)



BOARD/VOLUNTEERS

- Are all volunteers adequately trained?
- Does the board review policies each year?
- Is the board receptive to compliance needs?
- Does the board provide adequate oversight?
- Is the board committed to BSA/AML compliance?

RISK PROFILE

1. Analyze the potential risk in each area
2. Determine steps to manage the risk (*limits, restrictions, increased monitoring, etc*)
3. Update with changes in the risk profile or (*in the absence of changes*) at least once every 12 to 18 months
4. Refer to the FFIEC BSA/AML Examination Manual
5. Various self-assessment tools are available



HIGH BSA/AML RISKS

- Money Services Businesses (MSB)
- Remote Deposit Capture (RDC)
- Computer E-Cash
- Reloadable Prepaid Access Cards

MARIJUANA RELATED BUSINESS

- 29 states plus DC have legalized medical marijuana
- Recreational marijuana use is fully legal in:
 - 1) Alaska
 - 2) California
 - 3) Colorado
 - 4) Oregon
 - 5) Washington
 - 6) Maine
 - 7) Massachusetts
 - 8) Nevada
 - 9) Vermont (*Not for sale*)
 - 10) Washington, DC (*Not for sale*)

MARIJUANA RELATED BUSINESS

- Marijuana related business risk assessment
- Definitive policies and procedures
- Customer due diligence requirements are high
- Transaction monitoring (*alerts are crucial*)
- Training (*front line, BSA staff, internal audit, board*)
- Medical vs. Recreation (*understanding laws for each*)
- Costs & resources to properly comply with BSA requirements can be significant (*staff, technology*)



MARIJUANA RELATED BUSINESS

- Marijuana is still illegal under Federal Law
- Cole Memo priorities (*Deputy Attorney General James Cole*) may make it difficult for credit unions to comply
 - *Prevent distribution to minors*
 - *Prevent sale revenue from going to criminal enterprises*
 - *Preventing the diversion of marijuana from states where it is legal under state law in some form to other states*
 - *preventing state-authorized marijuana activity from being used as a cover or pretext for the trafficking of other illegal drugs or other illegal activity*
 - *Prevent drugged driving*
 - *Prevent the growing of marijuana on public lands*
 - *Prevent possession or use on federal property*



REQUIRED REPORTING

Marijuana Related Businesses

SAR requirements:

- Marijuana Limited SAR – ID information, address of parties, filing is due to related business, no suspicious activity identified (*continued activity filing*)
- Marijuana Priority SAR – Violated Cole Memo priorities or state law
- Marijuana Termination SAR – Terminate relationship in order to maintain an effective AML compliance program.



BSA/AML PROGRAM

Policies, Procedures, and Processes

- The BSA/AML program must be written
- The policy must be approved by the board
- The credit union must have a BSA/AML compliance program commensurate with its respective BSA/AML risk profile



CUSTOMER IDENTIFICATION

1. Required by the USA Patriot Act (*CIP Final Rule 6/9/03 – implement by 10/1/03*)
2. Must be incorporated in the overall BSA program and approved by the Board of Directors
3. Requires adopted procedures that focus on identifying new members – Due Diligence
4. Record and retain identifying information (*documentary and non-documentary*)
5. Requires new members to be checked against the OFAC list (*within a reasonable time of account opening or earlier, if required by the government*)



ADEQUATE CUSTOMER (MEMBER) NOTICE

CIP must include procedures for providing notice that the credit union will request identifying information.

- Notice must describe identification requirements
- Provided in a manner designed to allow the member to view it before the account is opened
- Examples: *Posting the notice in the lobby, at stations where members can open accounts, included within the application documents, and on the web site for online account opening*



SAMPLE LANGUAGE

IMPORTANT INFORMATION ABOUT PROCEDURES FOR OPENING A NEW ACCOUNT

To help the government fight the funding of terrorism and money laundering activities, federal law requires all financial institutions to obtain, verify, and record information that identifies each person who opens an account. *What this means for you:* When you open an account, we will ask for your name, date of birth, and other information that will allow us to identify you. We may also ask to see your driver's license or other identifying documentation.



ADEQUATE CUSTOMER (MEMBER) NOTICE



MEMBER DUE DILIGENCE

- Effective Due Diligence requires the credit union to obtain additional information beyond the CIP requirements
- The credit union should obtain information (at account opening) that will enable the credit union to predict the normal and expected activity on a particular account
- Sufficient new account documents

EXPECTED SERVICES/ACTIVITY

- ACH/Payroll deposits
- Wire activity - Domestic and or International
- Checking account
- Online banking
- Mobile banking
- ATM or debit card activity
- Expected cash activity
- Credit card/Reloadable card and loan activity



EXPECTED SERVICES/ACTIVITY

- Are any of the expected services/activity identified as moderate to high risk in the credit union's BSA/AML risk assessment
- Do any of the expected services require approval (*mobile banking, ODP, credit lines, etc.*)
- Various expected services can place an account in a high risk category



MEMBER DUE DILIGENCE (CONT.)

- Due diligence procedures aid in the detection of unusual or suspicious activity
- Assist in identifying high risk accounts
- The type and degree of information sought will vary based on the risk presented by the particular member, products/services requested and the geographic location of the account



MEMBER DUE DILIGENCE (CONT.)

- For higher risk accounts (business, organizational, and club accounts), the credit union may consider obtaining the following information:
 1. *Purpose of the account*
 2. *Financial statements (explain changes in activity)*
 3. *Financial references*
 4. *Where the business is organized*
 5. *Trade area (weather or not international trade is expected)*
 6. *Occupation or type of business*
 7. *Individuals with ownership or control*



FINAL RULES

Customer Due Diligence Requirements for Financial Institutions

- RIN 1506-AB25
- Published in the Federal Register May 11, 2016
- Rule is effective 60 days after the date of publication
- Covered financial institutions must comply by May 11, 2018



IDENTIFYING BENEFICIAL OWNERSHIP

Ownership Prong:

- Natural Person
- Owns through one or more share holdings more than 25%

Control Prong:

- Individual with control or management over entity
- i.e. Executive Officer or Senior Manager



BENEFICIAL OWNERSHIP

- Identification and verification procedures are similar to those used under the customer identification program (CIP)
- May rely on copies of identity documents
- Identify account control
- Identify multiple signatories
- Include risk-based procedures for ongoing due diligence



IDENTIFYING BENEFICIAL OWNERSHIP

Certification for Beneficial Owner(s)

APPENDIX A to § 1010.230

Dept. of the Treasury - Financial Crimes Enforcement Network

Proposed Rule: RIN 1506-AB25

POTENTIAL CONCERNS FOR CERTIFICATION

- Recordkeeping
- Updating information
- Reliance on information received
- Existing members vs New members vs Account

CHALLENGES

- Beneficial ownership is not member relation based
- Beneficial owners may change often
- Increased monitoring required to identify changes
- New information obtained with each change (*new beneficial owner, new account, new service, etc.*)



AUTOMATIC PRODUCT & SERVICE RENEWALS

- Under CIP rules, each time a loan is renewed or a certificate is rolled over, a new account is established
- Covered financial institutions are required to obtain beneficial ownership information of any legal entity that opens a new account
- FinCEN understands these products are not treated as new accounts by the industry
- The risk of money laundering is low



AUTOMATIC PRODUCT & SERVICE RENEWALS

- May 11, 2018 – FinCEN grants an exception to covered financial institutions for 90 days, up to and including August 9, 2018, from the Beneficial Ownerships Rules requirements to identify and verify beneficial ownership information for rollover or renewal of certain financial products and services that were established before May 11, 2018.





MDiDC
Credit Union Association

TRANSACTION MONITORING

TRANSACTION MONITORING

- ▶ Should have policies and procedures in place to:
 1. *Monitor currency transactions*
 2. *Identify and monitor suspicious transactions*
 3. *Include type, method, frequency*
- ▶ Manual review of reports generated by DP system, and/or
- ▶ Automated systems that automatically detect large or suspicious transactions and other violations of the BSA - *(Require System Validation)*
- ▶ May be a combination of both



MONITORING FOR HUMAN TRAFFICKING & HUMAN SMUGGLING

Funnel Accounts

- Illicit money is deposited in one city...
- then quickly withdrawn from another location

This tactic is sometimes used by individuals paying debts, for example, to the source organization responsible for the transportation of trafficking victims.



HUMAN TRAFFICKING & HUMAN SMUGGLING

- High-volume deposits through funnel accounts and immediate withdrawals from border towns
- Ongoing ATM and credit card transactions in even amounts between 10 p.m. and 6 a.m.
- Credit card payments to online escort services for advertising
- Sudden changes in activity in business accounts outside the member's expected profile
- Use of anonymous monetary instruments to pay bills instead of personal checks



CTR AND SAR REPORTING

Mandatory electronic filing 3/31/2013

- CTR – Currency Transaction Reporting
- Cash transactions exceeding \$10,000
- Filed within 15 days of the transaction

- SAR – Suspicious Activity Reporting
- Filed within 30 days of initial detection
- A continued SAR is filed within 30 days following a 90 day investigation for repeated activity



CTR – EXEMPTIONS

- Congress enacted an exemption process whereby businesses may be exempted from Currency Transaction Reporting
- Phase I “exempt persons” include financial institutions, government entities, and business listed on the stock exchange
- Phase II “exempt persons” include non-listed business and payroll customers
- Individuals are not eligible for exempt status



SUSPICIOUS ACTIVITY REPORTING (SAR)

What is it?

If the Credit Union suspects any actual or attempted violation a “Suspicious Activity Report” (SAR) must be filed with the Treasury Department.



WRITTEN SAR FILING PROCEDURES

- Identifying unusual activity
- Law enforcement inquiries and requests
- National Security Letters
- Transaction monitoring
- SAR decision making and documenting
- Completing the narrative
- SAR completion and filing
- Timing of a SAR filing
- SAR quality
- Board notification requirements
- SAR record retention requirements
- Prohibition of SAR disclosure



REASONS TO FILE A SAR

- BSA structuring
- Check fraud/check kiting
- Computer intrusion
- Credit and debit card fraud
- Embezzlement
- Identity theft
- Terrorist financing
- Wire transfer fraud
- Evidence of money laundering
- And more



STRUCTURING TRANSACTIONS

It is illegal to assist or recommend actions that might help members structure cash transactions to avoid CTR reporting requirements.

It is important to report any member who asks about the filing limit or any member who informs you that they are depositing under the CTR threshold amount because they do not want a CTR filed on the transactions.



SAR FILING THRESHOLDS

- ▶ A SAR is filed for:
 1. Insider abuse involving any amount
 2. Transactions aggregating \$5,000 or more that involve money laundering or violations of the BSA
 3. Known or suspected criminal violations aggregating \$5,000 or more where the suspect can be identified
 4. Known or suspected criminal violations aggregating \$25,000 or more whether or not a potential suspect can be identified



DECISION MAKING PROCESS

- Training for staff involved in SAR filings should contain information specific to transaction monitoring and SAR filing guidelines
- “Initial Detection” does not always mean the moment the transaction was processed
- The 30 day filing period does not begin until after the activity has been investigated and determined suspicious
- Legitimate transactions may raise a red flag due to inconsistency



PROHIBITION OF SAR DISCLOSURE

No credit union, and no director, officer, employee, or agent of a credit union that reports a suspicious transaction may notify any person involved in the transaction that the transaction has been reported. A SAR and any information that would reveal the existence of a SAR, are confidential, except as is necessary to fulfill BSA obligations and responsibilities.



OFAC



Office of Foreign Assets Control

OFAC

Office of Foreign Assets Control

- OFAC is a division of the U.S. Treasury Department
- OFAC administers and enforces economic and trade sanctions against targeted countries and their agents, terrorism sponsoring agencies and organizations, and international narcotics traffickers



OFAC COMPLIANCE PROGRAM

There is no regulation that requires the development of an OFAC program, however:

- Without an OFAC program, everything you do is a risk
- Without an OFAC program, credit unions may be subject to stiff penalties



OFAC REQUIREMENTS

Specially Designated Nationals list (SDN)

- Check new members (*joint, beneficiaries, etc.*)
- Periodic database scrubs
- Report positive matches
- Block accounts, freeze assets, reject transactions



CONSOLIDATED NON-SDN LIST

- Foreign Sanctions Evaders (FSE) List
- Sectoral Sanctions Identifications (SSI) List
- Palestinian Legislative Council (NS-PLC) List
- The List of Foreign Financial Institutions Subject to Part 561 (the Part 561 List)
- Non-SDN Iranian Sanctions Act (NS-ISA) List
- Persons blocked solely pursuant to Exec. Order 13599



CONSOLIDATED NON-SDN LIST

- No requirement to block or freeze property
- May be persons whose property and interests in property are blocked pursuant to other authorities administered by OFAC
- Refuse to process transactions
- Report attempted wires on Foreign Sanctions Evaders list matches to OFAC within 10 days





MDiDC
Credit Union Association

ACH

ACH TRANSACTIONS

- Certain ACH transactions are higher risk than others, such as ACH files being handled by a third party or international transactions

ACH RISK

- Third party service providers
- Relying on another party for OFAC compliance
- Large dollar amounts – frequent ACH and IAT activity
- IAT transactions from high risk geographic areas
- ACH and IAT activity not normal for the account and/or business



FINCEN

MDiDC
Credit Union Association



Financial Crimes Enforcement Network

FINCEN 314(A) & 314(B) REQUIREMENTS

- 314(a) – Sharing information with FinCEN. Requests for information sent every 2 weeks, or more frequently if an emergency request is transmitted
- Respond to report matches within 2 weeks
- 314(b) – Sharing information with other FI's for the sole purpose of detecting and reporting terrorist activity or money laundering – Must register with FinCEN annually, and have definitive policies & procedures in place



FINCEN 314(A) & 314(B) REQUIREMENTS

- Have a designated contact person for each
- Maintain evidence of 314(a) searches
- Cannot disclose 314(a) request
- Shared information through 314(b) should be limited to the underlying transaction & member information
- 314(b) does not authorize SAR sharing or disclose the existence or nonexistence of a SAR
- 314(b) information can be used to determine whether or not to file a SAR



314(A) INFORMATION REQUESTS

Major Compliance Violations

- Not conducting the search after notification
- Sharing access authorization allowing other staff to conduct the search
- Allowing other staff to view 314(a) list
- Failure to update 314(a) contact with staff changes



314(B) INFORMATION REQUESTS

Major Compliance Violations

- Failure to keep registration updated
- Failure to verify sharing party
- No definitive written policy and procedures
- Unsecured sharing process



MDiDC
Credit Union Association

MONEY LAUNDERING

WHAT IS MONEY LAUNDERING?

- Very simply – It's criminal finance.
- A person who conducts a financial transaction with knowledge that the funds or property involved are the proceeds of a crime and who intends to further that crime or to conceal or disguise those proceeds is indeed laundering money
- The process of converting cash from criminal activity into a form that can be easily exchanged without tracing it back to its original origin



WHAT IS MONEY LAUNDERING?

Most common perceptions connect money laundering with:

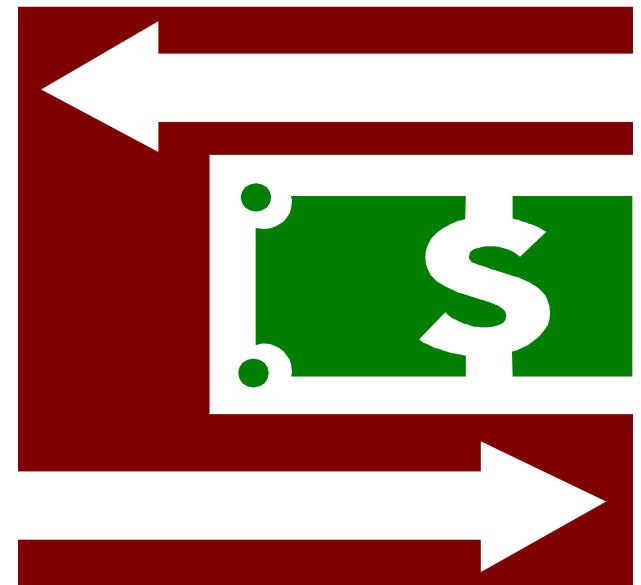
- drug trafficking
- tax evasion
- terrorist activity



BASIC WAYS MONEY IS LAUNDERED

Deposits to financial institutions

- Wire transfers
- Business fronts
- Fictitious identities
- Off-shore transactions



THREE STAGES OF MONEY LAUNDERING

- Placement - The first and most vulnerable stage for getting illegal funds into the financial system (*Various deposits into multiple institutions*)
- Layering - Consolidating the funds into one (*or more*) financial institution
- Integration - Buying and selling investments, real estate, etc. Funds reintroduced into the system (*The trail grows colder*)





MDiDC
Credit Union Association

INDEPENDENT TESTING

INDEPENDENT TESTING

- Frequency is not defined in any statute
- Every 12 to 18 months is a sound practice (*refer the BSA/AML FFIEC Examination Manual*)
- Evaluation of adequacy & effectiveness of the BSA/AML compliance program
- Internal controls must be adequate for the size and complexity of the institution
- Internal controls must be in compliance with established regulations



INDEPENDENT TESTING (CONT.)

- Must be conducted by trained, competent professionals (*does not include the CEO/Manager*)
- Testing can be done internally provided person(s) performing the testing are not involved with the credit union's BSA program
- May consider CPA firms, attorneys, or League/Association professionals
- Documentation and written analysis is required for compliance



MOST COMMON BSA VIOLATIONS

- *Incomplete independent testing*
- *Incomplete BSA and OFAC risk assessments*
- *No written or updated BSA and related policies/procedures*
- *Failure to comply with written policy*
- *Undocumented training (or failure to train)*
- *Incomplete CTR's*
- *Improper SAR process*
- *Failure to download and check 314(a) list*
- *Improper OFAC process (no OFAC check on new mbr's)*



COMPLIANCE WITH BSA IS CRITICAL

- Assist US government agencies - detect and prevent money laundering
- International drug trafficking (*5% to 25% of US murders are drug related*)
- September 11, 2001 (*Terrorist attacks on the US*)
- April 15, 2013 (*Boston bombing*)
- Terrorist attacks in Paris
- ISIS
- Various, stabbings, shootings, and bombings throughout the US in 2016



TERRORIST ATTACKS 2017

- Jan 6 – Ft. Lauderdale, FL: Airport shooting, 5 killed, 6 injured
- Jan 31 – Denver, CO: Fatal shooting transit authority guard
- Jun 14 – Alexandria, VA: Baseball field shooting, 5 injured
- Aug 12 – Charlottesville, VA: Vehicular attack on protesters
- Sept 24 – Antioch, TN: Shooting attack on church service
- Oct 31 – New York City, NY: Vehicle attack on bike path, 8 killed
- *Las Vegas concert attack and TX church shooting were not classified as terrorist attacks (Criminal)*



TERRORIST ATTACKS 2018

- Jan 31 – Philadelphia, PA: Vehicular attack injured one civilian; driver was fatally shot by off-duty police officer who was injured during struggle
- March 12 – Palm Beach, FL: Teenager fatally stabbed a 13-year-old and stabbed two others, including one other 13-year-old
- March 22 – Travis AFB, CA: Attacker in a minivan carrying propane tanks drove through gate at Travis AFB and crashed, killing himself. No others killed or injured



COST OF TERRORIST ATTACKS

- 1998 U.S. Embassy bombings in Kenya & Tanzania - \$50k
- 2000 attack on the *USS Cole* - \$10k
- 2002 bombings in Bali - \$50k
- 2004 attacks in Madrid - about \$10k
- 2005 subway attacks in London - about \$35k
- 2010 Times Square bombing - \$12k
- 2010 cargo plane attacks - \$4.2k



RISK OF NON-COMPLIANCE

- Findings can affect CAMEL ratings
- Large monetary penalties levied against the credit union
- Monetary penalties (*Can be levied against individual employees and board members*)
- Cease and desist order
- Incarceration





MDIDC
Credit Union Association

BANK SECRECY ACT

PENALTIES FOR NON-COMPLIANCE

- Standard negligence: \$500
- Pattern of negligence: up to \$50,000
- \$10,000 per day for CTR's not filed within fifteen days
- Intentional non-compliance: up to \$100,000 in civil penalties – can be levied against individual employees and board members



PENALTIES (CONT.)

- If international money laundering is evident: penalties can reach up to \$1,000,000
- Criminal penalties for willful non-compliance: \$500,000 and up to ten years in prison, or both

The costs of compliance is much less than the costs of non-compliance.



CHASE BANK – RIVERSIDE, CA

- Frank E. Mendoza reported mortgage related fraud resulting in a SAR filing in November 08
- Mendoza later contacted the borrower asking for \$25k in exchange for assistance with Chase and a possible federal criminal investigation
- The borrower delayed making payment and Mendoza lowered the amount to \$10k
- The borrower reported Mendoza to the FBI
- FinCEN assessed a \$25,000 civil money penalty against Mendoza December 15, 2011



HSBC

- British multinational banking and financial services company headquartered in London
- Total Assets 2011: \$2.555 trillion
- 7,200 offices over 85 countries
- In 2007 & 2008 HSBC Mexico sent \$7 billion in cash to the United States
- Also skirted U.S. bans on financial transactions with Iran and other countries
- Paid \$1.9 billion to settle a U.S. money-laundering probe



JPMORGAN CHASE BANK

- Global bank and financial services company
- Part of the largest bank holding company in the U.S.
- Approximately \$2.5 trillion in assets
- JPMorgan failed to maintain an effective anti-money laundering program
- JPMorgan failed to file timely SAR's on transactions arising out of the Bernard Madoff fraudulent investment scheme
- January, 2014 - Paid a combined \$2.05 billion



NORTH DADE COMMUNITY DEVELOPMENT FCU

- Assets: \$3.1 million
- *MSB conducted close to \$2 billion in transactions*
- Failed to have an effective AML program
- Failed to implement an effective system of internal controls
- Did not perform a risk assessment until November 2013
- Insufficient controls to identify suspicious activity
- *\$300,000 Civil Money Penalty – November 2014*



FIRST NATIONAL COMMUNITY BANK DUNMORE, PENNSYLVANIA

- Assets: \$1 billion
- Failed to detect or adequately report suspicious activity
- Failed to identify red flags in accounts controlled by a board member
- *\$1.5 million Civil Money Penalty – February, 2015*



BANK OF MINGO, WILLIAMSON, WV

- Assets: \$93.879 million
- Failed to establish adequate AML compliance program
- Failed to implement effective system of internal controls
- Inadequate independent testing
- Ineffective staff training program
- *\$4.5 million Civil Money Penalty – June, 2015*



GIBRALTAR PRIVATE BANK & TRUST CO. CORAL GABLES, FLORIDA

- Assets: \$1.57 billion
- Failed to implement effective system of internal controls
- Ineffective transaction monitoring procedures
- Failed to adequately assess money laundering risks
- Ineffective staff training program
- *\$4 million Civil Money Penalty – February, 2016*



BETHEX FCU – BRONX, NY

- Assets: \$12.3 million
- MSB volume increased from \$657 million domestic transactions in 2010 to over \$4 billion in domestic and international transactions in 2012
- Failed to make commensurate changes in compliance controls to account for risks posed by MSB accounts
- No risk assessment conducted in 2011
- 2012 risk assessment did not assess MSB risk
- *\$500,000 Civil Money Penalty – December, 2016*



MERCHANTS BANK – CARSON, CA

- Assets: \$64 million
- Inadequate internal controls to ensure BSA compliance
- Inadequate due diligence for high risk customers
- Inadequate controls to mitigate risks of RDC services to high risk MSBs
- Independent testing not commensurate with risk profile
- BSA officer lacked proper level of authority
- Inadequate BSA/AML training
- *\$7 million Civil Money Penalty – February, 2017*



ENFORCEMENT ACTION

- In 2013 FinCEN started placing emphasis on Corp. and individual responsibility
- FI's were able to consent to monetary penalties without admitting or denying the alleged wrongdoing
- Practice is changing – Admitting responsibility to an enforcement action increases the liability risk for the D&O's and widens avenues for private litigation against financial institutions and their D&O's
- Confirm adequate insurance coverage



COMPLIANCE CULTURE

- BoD, Exec, & Sr. Mgmt. will actively support, understand and be engaged in BSA/AML compliance efforts
- Managing and mitigating BSA deficiencies will not be compromised by revenue interest
- Relevant compliance information will be shared throughout the CU
- Adequate human and technological resources will be devoted to compliance functions
- CU leadership and staff will understand the purpose of BSA efforts and reporting
- The BSA compliance program will be tested by an independent and competent party



BOARD OF DIRECTORS

- Exhibit a strong commitment to compliance
- Know and Understand the risk
- Provide oversight
- Ensure the credit union has sufficient resources to mitigate risks, and maintain compliance with Anti-Money Laundering regulations
- Ultimately, the Board of Directors is liable for compliance with the regulation



WEB ADDRESSES FOR BSA INFOBASE

- http://www.ffiec.gov/bsa_aml_infobase
- <http://www.ustreas.gov>
- <http://www.fincen.gov>
- <http://www.ffiec.gov> (*BSA Examination Manual*)
- <http://www.treas.gov/offices/enforcement/ofac/>



This presentation is general in nature and for informational purposes only. It should not be relied upon as legal advice or legal opinion. Should you have any questions concerning the information provided, please contact:

Andre A. Lucas, CUCE, BSACS

Director of Compliance

443-325-0777

alucas@mddccua.org