THE COMPLIANCE ORGANIZATION
www.thecomplianceorganization.com

AML/BSA Training Manual

An employee guide to anti-money laundering laws and regulations under the Bank Secrecy Act

Mitchell Levy, CAMS
Mitchell@TheComplianceOrganization.com
(c) 301-793-8188

Table of Contents:

SECTION 1: Introduction

This manual is designed to instruct employees of MSBs on the anti-money laundering laws and regulations enforced by the United States Government.

Failure to comply with U.S. anti-money laundering laws may subject but you and your employer to significant penalties. For the protection of both you and your employer, it is important that you understand these requirements and how to comply with them.

After reviewing this Manual, please go take the AML/BSA Training Quiz at www.thecomplianceorganization.com to verify your knowledge and understanding. If you pass the quiz (score of 80% or better), you will be awarded a Certificate of Achievement.

Any specific questions about your employer's operations should be directed to Company Management and/or your company's Bank Secrecy Act (BSA) Compliance Officer.

SECTION 2: Key Terms and Definitions

All employees must be familiar with the following key terms, which will be discussed and referenced throughout this Manual.

Anti-Money Laundering Compliance Program - All MSBs must have an Anti-Money Laundering (AML) Compliance Program to protect the company from criminals trying to launder money and from terrorist financiers. AML Compliance Programs must include, among other requirements, employee training.

Bank Secrecy Act (BSA) - The Bank Secrecy Act or BSA is the federal law governing U.S. anti-money laundering procedures. The BSA and its implementing regulations require compliance with a number of obligations, including that MSBs file reports on certain transactions, which helps create a "paper trail" for law enforcement officials to follow.

Business Day - A business day typically means from the time your business opens in the morning to the time it closes in a single day.

BSA Compliance Officer - All MSBs must have a BSA Compliance Officer to administer the company's Anti-Money Laundering Compliance Program. The BSA Compliance Officer must also ensure that all employees are properly trained.

Cash-In/Cash-Out - The Treasury Department classifies transactions as either cash-in or cash-out. Cash-in transactions (where cash is received from the customer) include such currency transactions as buying money orders, sending wire transfers, purchasing or reloading of prepaid access devices or vehicles and exchanging currency for currency. Cash-out transactions (where cash is tendered to the customer) include cashing checks, paying out a "receive" wire transfer to customer, and exchanging currency for currency.

Currency - Currency is the coin and paper money of the United States or any other country and is designated as legal tender. Currency is the same as "cash."

Currency Transaction Report (CTR) - Check cashers and other MSBs must file a Currency Transaction Report (CTR) for each transaction in currency in excess of $10,000 by or on behalf of any person during any single business day. This includes check cashing transactions (which are "cash-out") or money order sales and funds transfers ("cash-in"). CTRs are to be filed through FinCEN's E-Filing System.

Financial Crimes Enforcement Network (FinCEN) - FinCEN is a federal bureau of the United States Department of Treasury that administers and regulates U.S. anti-money laundering efforts, including promulgating regulations governing the AML-related obligations of MSBs.

Funds Transfer Rules - Money transmitters and their agents (including many check cashing companies) must maintain records on customer funds transfers, such as sending or receiving a

payment for a money transfer of $3,000 or more, regardless of the method of payment. (Note: Many money transmitter companies, such as Western Union® and MoneyGram®, require recordkeeping for transactions under $3,000.)

Identity Theft - "Identity theft" occurs when criminals assume the identity of innocent persons to engage in criminal activity. Identity thieves often try to access credit or bank accounts of their victims and run up thousands of dollars in illegal purchases. Typically, the criminal will then "fence" or sell the goods, leaving the victim responsible for the purchases – and ruining his or her credit. There are many types of identity theft scams.

Internal Revenue Service (IRS) - The Internal Revenue Service is the U.S. government agency that examines check cashers and other MSBs to determine whether the companies are complying with the Bank Secrecy Act. The IRS may also interview company employees to ensure that they have received proper AML training.

Monetary Instruments - Monetary instruments include money orders, traveler's checks and all negotiable instruments, including all forms of checks.

Monetary Instrument Log - MSBs must maintain a record or "log" of sales of money orders or other monetary instruments between $3,000 and $10,000. (Sales in excess or $10,000 must be reported on a CTR).

Money Laundering - Money laundering conceals the source or ownership of criminal profits so that the money can be used without detection by law enforcement. Criminals are known to exploit financial institutions by using them to "launder" money derived from criminal activity.

Money Services Businesses - Money services businesses (MSBs) include check cashers, money transmitters and their agents, currency dealers and exchangers, and sellers and issuers of money orders and prepaid access.

MSB Registration - Most MSBs are required to register with FinCEN by filing a Registration of Money Services Business form through FinCEN's E-Filing System. Registration must be renewed every two (2) years.

Multiple Transaction Rule - The multiple transaction rule states that "multiple transactions must be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any [i.e., the same] person..." This means that if someone performs several currency transactions in one day, and when added together all of the transactions exceed $10,000 in cash-in or cash-out in currency, and the MSB has knowledge that the transactions are on behalf of the same person, a CTR must be filed.

OFAC - The Office of Foreign Assets Control (OFAC) is an office of the U.S. Treasury Department that enforces sanctions against rogue countries, and individuals and organizations involved in

terrorism and criminal activity. OFAC maintains a list of these individuals and organizations called the Specially Designated Nationals List (SDN List), as well as other sanctions lists on its website. OFAC also identifies jurisdictions subject to embargoes on its website.

Person - The term "person" means any individual or legal entity, including companies, corporations, partnerships or associations.

Prepaid Access Requirements - Companies offering prepaid access sales and reloads must comply with anti-money laundering requirements. Purchasers of prepaid access devices or vehicles must be verified through proper ID. Also, employees must report suspicious prepaid access activity via a Suspicious Activity Report (SAR), and file CTRs on qualifying transactions.

Record Retention - All reports (CTRs/SARs) and records must be retained for a period of five (5) years and must be filed or stored in such a way as to be accessible within a reasonable period of time.

Smurfs - Criminals use runners, commonly known as "smurfs" (named after the little cartoon characters from television), to help them launder money. Smurfs typically visit many financial institutions to deposit dirty money into bank accounts, convert it to money orders, or send it by funds transfers. Transactions are frequently conducted in amounts under applicable reporting requirements in order to evade reporting requirements.

- Smurfs also engage in other types of currency transactions. They may exchange small bills for large bills (to reduce the volume of cash). They may send wire transfers to other bank accounts. They may buy money orders or other financial instruments in the names of third parties, usually anonymous companies.

Structuring - Structuring involves the breaking up of a large cash transaction into several smaller transactions for purposes of evading transaction reporting or recordkeeping requirements. Money launderers try to "structure" transactions to avoid the filing of any reports (such as CTRs) or records (such as Monetary Instrument Log) linking them with their activities. It is illegal to structure a transaction, or to help a customer engage in structuring activity.

- For example, a criminal trying to launder $12,500 in cash might make several trips to a check casher, each time buying $2,500 in money orders. That way, the criminal will try to evade the requirement that any cash transaction over $10,000 must be reported to the government.

Suspicious Activity Report (SAR) - MSBs must file a SAR for a transaction or series of transactions of $2,000 or more where the MSB determines it meets applicable reporting requirements described below. These requirements may indicate that the customer is attempting to launder money or engage in other illegal activity. SARs are to be filed through FinCEN's E-Filing System.

Terrorist Financing - Terrorist financing involves an attempt to send or transfer funds to terrorists, terrorist- supporting organizations or in support of terrorist activity. Terrorist financing may involve funds from either legitimate or illegal sources. All check cashers and other MSBs must report any attempts by customers to finance terrorist activities, whether domestic or abroad.

- Terrorist financing was used in connection with the 9/11 terrorist attacks. A number of the 9/11 terrorists received funds from their supporters abroad, which were used to pay for the terrorists' flight lessons and living expenses. As a result, U.S. laws were strengthened to assist in the identification and seizure of terrorist funds.
- Terrorist financing may include money laundering-like activity intended to hide the source of the funds, particularly if the funds have been derived illegally. Terrorist financing may also include attempts to obscure the beneficiary of the transaction (i.e., the terrorist organization).

Willful Blindness - It is illegal for any employee of a check casher or other MSB to "turn a blind eye" to suspicious customer activity. If an employee engages in willful blindness, and intentionally ignores or assists money laundering or terrorist financing activity, he or she may be subject to criminal prosecution, fines – and prison.

SECTION 3: Money Laundering

With increased focus on the war on drugs and terrorist financing, the U.S. government has passed many important laws to fight money laundering activity, with increased enforcement beginning in 2010.

Money laundering is the act of moving illegally obtained assets through the financial system to disguise their origin and make them appear legitimate to avoid interference by law enforcement. Money laundering takes many forms and may involve different types of criminal activity. Money laundering is not limited to cash; criminals may use different types of financial instruments, including money orders or traveler's checks. However, criminals involved in illegal activities most often deal with cash since cash leaves no paper documentation of the transaction.

Money Laundering occurs in three stages:

1. Placement: introducing illegally obtained money into the financial system or retail economy. This may involve MSBs with the purchase of Money Orders, Traveler's checks, prepaid access, money transmission, or foreign exchange. *Money laundering is most vulnerable to detection and seizure at this stage.*

2. Layering: this phase is the movement of funds in an effort to further disguise the audit trail and ownership of funds. In this stage, assets that have been 'placed' are liquidated and transferred to other vehicles such as Money Orders, Traveler's checks, money transfers, foreign exchange, brokerage accounts, additional bank accounts (deposits from re-sale of high value goods) and real estate. This makes it more difficult to trace the money back to its original source.

3. Integration: to further obscure their source, the assets are again converted to give the appearance of legitimacy. This may include the purchase of automobiles, businesses, real estate, etc.

An important factor connecting the three stages of this 'process' is the 'paper trail' generated by financial transactions. Criminals attempt to avoid leaving this 'paper trail' by trying to avoid reporting and record keeping requirements, including by coercing or bribing employees not to file proper reports or complete required records, or by "structuring" transactions to keep them below reporting thresholds.

To fight money laundering, Congress enacted the Bank Secrecy Act (BSA), which requires that financial institutions file reports on transactions, which helps create a "paper trail" for law enforcement officials to follow.

Following the 9/11 terrorist attacks, Congress enacted the USA PATRIOT Act to strengthen existing laws to assist law enforcement in combating terrorism and terrorist financing.

Anti-money laundering efforts are administered by the Financial Crimes Enforcement Network (FinCEN), which is a bureau of the U.S. government. Also, the Internal Revenue Service (IRS) is required to examine check cashers and other MSBs to determine whether they and their employees are complying with the BSA. Check cashers and other Money Services Businesses (MSBs) must register with FinCEN. All MSBs must also have an Anti-Money Laundering (AML) Compliance Program to protect the company from criminals trying to launder money or finance terrorism. All AML Compliance Programs must include training for employees.

You can be a valuable deterrent to money laundering by diligently following the rules and regulations covered in this Manual. You can be a 'gate keeper' and help prevent AML violations.

SECTION 4: Money Services Businesses (MSB)

An MSB is a business, as defined by FinCEN and the IRS, that offers one or more of the following products or services:

1. Money Orders
2. Check Cashing
3. Foreign Exchange
4. Traveler's checks
5. Prepaid access (previously called 'stored value')
6. The business conducts more than $1,000 in money services business activity with the same person (in one type of activity) on the same day.
7. The business provides money transfer services in any amount.

Whether a person is subject to regulation as an MSB does not depend on factors such as whether the person is licensed as a business, has employees, or is engaged in a for-profit venture. It is the *activity* performed that causes a person or business to be categorized as an MSB subject to anti-money laundering rules. Additionally, an entity qualifies as an MSB based on its *activity within the United States*, not the physical presence of one or more of its agents, agencies, branches or offices in the United States.

Requirements of MSB/AML Program

As outlined in the Bank Secrecy Act, in order to guard against money laundering through financial institutions, MSBs and their agents shall establish anti-money laundering programs in writing, which are to include:

1. A written AML Policies, Procedures and Controls Plan
2. A designated Compliance Officer
3. Annual and on-going training – *this Manual, when followed by a passing score on the AML/BSA Quiz at www.thecomplianceorganization.com fulfills the annual requirement.*
4. An independent review function to test the program

SECTION 5: Suspicious Activity Report (SAR)

A Suspicious Activity Report (SAR) is the form you fill out and send in when you believe or have reason to believe a customer has broken or attempted to break an AML rule or regulation, for certain transactions of $2,000 or more.

SARs allow financial institutions to directly report possible illegal activity. All SARs are reviewed by law enforcement officials.

MSBs are required to file a SAR on most transactions of $2,000 or more that are known or suspected of involving money laundering or other crimes. Note that SARs are not limited to cash transactions.

A SAR must be filed if:

You have knowledge or suspect a transaction:

- Involves funds derived from an illegal activity,
- Is designated to evade Bank Secrecy Act requirements, whether through structuring or other means
- Serves no business or apparent lawful purpose
- Involves use of an MSB to facilitate criminal activity.

Transaction thresholds have been exceeded. For example:

- The transaction or series of transactions involves $2,000 or more, or
- $3,000 or more if discovered in the MSB's review of daily records for Money Orders or Traveler's checks.

An MSB can file a SAR on a voluntary basis, for transactions below the $2,000 threshold if it is believed that the transactions are suspicious. One common way money launderers avoid reporting and record keeping requirements is by 'structuring' transactions. Generally, the MSB and employee who filed the SAR are protected from civil liability. An intentionally false SAR, however, may result in both civil and criminal penalties.

All SARs must be filed via FinCEN's E-Filing system within 30-days after the date that the MSB knows, has reason to know, or has reason to suspect that the activity meets the above-described criteria. Where the MSB becomes aware of a violation of law that requires immediate attention, such as ongoing money laundering schemes or terrorist-related activities, the MSB should immediately notify law enforcement in addition to filing a SAR. (*FInCEN has established a Financial Institutions Hotline at 866-556-3974 for financial institutions to voluntarily report transactions that may relate to terrorist financing or other terrorist activity.)*

When filing a SAR, you must include a 'narrative' where you describe the suspicious activity, including what was unusual, irregular, or suspicious. Consider the following questions:

1. *What was the conduct that raised suspicion?*
2. *Was the transaction attempted or completed?*
3. *Who benefited from the transaction and why?*
4. *What explanation did the customer give?*

5. *Describe the subject: such as, but not limited to, gender, race, tattoos, height, weight, age, clothing, jewelry, unusual mannerisms, video surveillance, time of day, vehicle (car, truck) and license plate number if possible.*

A SAR should also attach all supporting documentation, including forms of ID of the suspect(s) involved, copies of all monetary instruments, and account numbers. Copies of all documentation must be maintained for a period of five years.

It is important that SARs are filed with complete and accurate information. Common SAR errors include:

- Critical fields (those marked with an *) left empty, inaccurate, or incomplete.
- Incomplete Narrative. What's missing: who, what, when, where, why, how?
- Empty narrative field. You must answer why the transaction was suspicious (see above)
- Supporting documents are attached and used (incorrectly) as a replacement for a narrative. *This is prohibited.* Supporting documents are to be kept by the MSB for five years and made available upon request.
- Inadequate narrative. Narrative that simply restates the information from the form's required fields is not adequate.
- Missing or incomplete filer or Employer Identification Number (EIN). Fill in the nine-digit number accurately. Do not use hyphens or dashes.
- Missing filer phone number.
- Missing transaction location.
- Invalid Social Security Number: 000000000 or 999999999 are invalid.
- Incomplete subject information: government issued identification such as driver's license or passport should be as complete as possible. Provide both the number and issuer of the ID card or document.

With limited exceptions, it is illegal to inform any party to the transaction that a suspicious transaction has been reported. This reason for nondisclosure is to allow law enforcement an opportunity to investigate and apprehend money launderers. Violation of this law can result in fines and other serious penalties.

Red flags of suspicious customers include, but are not limited to:

- A customer who comes in several times over a period of days to send large funds transfers (all under $1,000) to different people in the same town.
- A customer who uses a different spelling of his name for different transactions.
- A younger customer who conducts large transactions but cannot provide an explanation for the source of the cash.
- A customer who tries to make multiple money order purchases of slightly under $3,000 over a period of a few days.
- A customer who attempts to purchase multiple prepaid access devices/vehicles (e.g., prepaid debit cards) in different names, or over a period of several days.
- A customer who attempts to make multiple wire transfers to several people at the same address.

- A customer who uses false ID or different ID for different transactions.
- A customer who tries to break up a large transaction into several smaller transactions.
- Unusually large or frequent prepaid access transactions.
- Very young persons (or others not likely to possess large amounts of cash) attempting very large or repeated cash transactions.
- Unusually nervous or evasive persons.
- Persons who are unable or unwilling to provide information or identification.
- Persons who come in frequently to perform transactions slightly under the reporting thresholds.
- Persons who appear to be working together, perhaps going to different tellers to conduct cash transactions.
- Customers attempting to avoid or circumvent the Company's ID requirements.

Red flags of suspicious employees (fellow worker) include, but are not limited to:

- Never or almost never takes a vacation
- Always tries to wait on the same suspicious customer
- Does not want you to see or be aware of transactions with a suspicious customer
- Behavior changes to secretive with a certain customer
- Acts guilty
- Whispers with a certain customer
- Asks a certain customer to come back later
- Does more MSB business when working alone
- Lives beyond apparent means (receiving bribes?)
- Employee accepting tips or bribes for 'overlooking' MSB/AML rules
- Your intuition tells you something is not quite right

SECTION 6: Currency Transaction Report (CTR)

A Currency Transaction Report (CTR) is to be filed for all transactions (in or out) larger than $10,000 in cash (bills or coins, U.S. or foreign) conducted in one business day by any person(s) or on behalf of another person(s).

If the transaction is being conducted on behalf of another person(s), you must obtain all the required information for all parties. Multiple cash transactions are considered to be one transaction about which a CTR must be filed if the MSB has knowledge that: they are by or on behalf of the same customer during one business day, and they are conducted at one or more branches or agents of the same MSB, and they total more than $10,000 in either cash-in or cash-out.

The multiple transaction rule states that "multiple transactions must be treated as a single transaction if the financial institution has knowledge that they are by or on behalf of any [i.e., the same] person..." This means that if someone performs several currency transactions in one day, and when added together all of the transactions exceed $10,000 in cash-in or cash-out in currency, and the MSB has knowledge that the transactions are on behalf of the same person, a CTR must be filed.

The CTR must be filed within 15 days of the date of the transaction via FinCEN's E-Filing system.

All persons conducting a currency transaction in excess of $10,000, thus requiring a CTR, must be identified by an official, government-issued form of ID, such as:

- Driver's license
- Military and Military Dependent ID card;
- Passport – United States or Foreign Country
- State-issued ID card
- Resident alien ID card (Green Card)
- Government-issued ID (e.g., Mexico Matricula Consular ID, or other legitimate foreign government-issued ID)

If the customer does not have or refuses to provide proper ID, you must refuse to complete the transaction. Refusing to provide ID may also be regarded as "suspicious," requiring a SAR.

Examples where a CTR is required:

- A customer cashes an $12,000 insurance claim check.
- In the morning, a customer cashes a $3,000 insurance claim check. Later that afternoon, he cashes a $8,000 tax refund check.
- A customer sends a $11,800 funds transfer and pays with cash.
- A customer purchases $15,000 in prepaid debit cards.
- A customer receives a $7,500 wire transfer and cashes a $3,500 check.
- A customer buys $8,000 in money orders and puts $2,500 on a prepaid access device/vehicle.

SECTION 7: Monetary Instrument Log

The BSA requires that MSBs keep records on all customer cash purchases of monetary instruments (money order sales) between $3,000 and $10,000, inclusive. (Monetary instrument sales above $10,000 require a CTR.) Multiple cash purchases of monetary instruments totaling $3,000 or more within one business day must be treated as one purchase which must be recorded. Many MSBs maintain a "Monetary Instrument Log" to satisfy this requirement.

Regulations require that the Company obtain proof of identification and keep a record of the following items for a period of five years from the date of purchase:

1. Customer (purchaser's) name and address
2. Customer's Social Security number, or Alien Identification number
3. Customer's date of birth
4. Date of purchase of the monetary instrument
5. Type of instrument(s) purchased
6. Serial number of instrument(s) purchased
7. Dollar amount of instrument(s) purchased

If the customer does not have or refuses to provide a Social Security or Alien ID number, you must refuse to complete the transaction. All persons making cash purchases of monetary instruments of $3,000 or more in a single or multiple transaction must be identified.

SECTION 8: Records for Funds Transfers

If the MSB performs funds or “wire” transfers for customers, the BSA requires that in connection with any send or receive wire transactions of $3,000 or more, the Company must verify the customer’s identity and record certain detailed information concerning the transaction, regardless of the method of payment.

Your money transmitter may have a policy of requiring identification and recordkeeping or transactions less than $3,000. If your employer is an agent of a money transmitter, you must follow the money transfer policies and procedures implemented by the money transmitter.

SECTION 9: Prepaid Access Services Requirements

If your MSB provides prepaid access services, including sale and reloads, federal law requires that MSBs must file CTRs and SARs on, and retain records related to, certain customer prepaid transactions, for a period of five years after the last use of the prepaid access device.

MSBs providing sales and reloads of prepaid access must have procedures to verify customer identity by obtaining proper ID, and recording name, date of birth, address, and ID number.

MSBs also must have procedures to identify and file CTRs on customer prepaid access transactions involving access to funds in excess of $10,000 during one business day.

MSBs must also have procedures to identify and file SARs on suspicious customer transactions involving prepaid access usage. SAR criteria are identical to those detailed above.

SECTION 10: Customer Privacy

Federal law requires that MSBs and their employees maintain the integrity and confidentiality of customer information, including records, Social Security information, and other personal information. All customer records should be maintained in a secure area with the Company's other books and records. Records on computer files must also be protected from theft or intrusion.

Never discard in the trash any documents, check stubs, old CDs or other records of any kind that contain confidential customer information. Criminals are known to search the garbage of financial institutions to gather personal information for use in identity theft schemes.

Immediately report to your BSA Compliance Officer and/or Management any attempt to access confidential customer information. This includes any unauthorized use of customer information by other employees, or any unauthorized computer access. SARs may be required in the event of identity theft, and FinCEN has issued specific instructions for filing identity-theft related SARs. Contact your BSA Compliance Officer for more information.

SECTION 11: Penalties

Violation of the U.S. anti-money laundering laws can result in significant fines and penalties, and even prison sentences. Penalty amounts are updated on a yearly basis.

It is illegal to intentionally ignore suspicious activity. You cannot engage in “willful blindness” and allow your company to be used by criminals to launder money.

Management may in its discretion take disciplinary action against any employee that violates the Company’s BSA/AML policy and procedures.

SECTION 12: Conclusion

Failure to comply with U.S. anti-money laundering laws may subject both you and your employer to significant penalties. For the protection of both you and your employer, it is very important that you understand and follow these requirements.

All compliance questions should be directed to your BSA Compliance Officer and/or Management.

After reviewing this Manual, please take the AML/BSA Training Quiz at www.thecomplianceorganization.com to verify your knowledge and understanding. If you pass the quiz (score of 80% or better), you will be awarded a Certificate of Achievement.