AML/BSA Training Manual

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

DISCLAIMER

This sample AML/BSA Training Manual developed by The Compliance Organization (TCO) is a generic document for general information purposes only. It must be revised and adapted to fit your company's business and operations, as appropriate. In developing the sample, TCO did not have one specific company/operation in mind, but primarily a general MSB that is acting as an agent of a primary/principal Money Transmitter. TCO based the sample on the legal requirements underpinning most of such an agent's business operations. The sample is intended as a starting point to assist you with your BSA compliance training program. Your company will need to make sure that the training program that becomes a part of your BSA/AML compliance program is accurate and applicable to your actual business practices and BSA/AML risks (and revise the sample accordingly).

Note that the sample is not intended to promote or recommend any particular policy or procedure. All policies and procedures must be implemented in a manner consistent with the legal requirements governing your company.

Your use of this sample AML/BSA Training Manual is at your own risk, and you should not use it or any TCO sample documents without first seeking your own legal and other professional advice. The provision of such sample documents (and the documents themselves) does not constitute legal advice or opinions of any kind, or any advertising or solicitation. No lawyer-client, advisory, fiduciary, or other relationship is created between TCO and any person accessing or otherwise using any of the TCO sample documents. TCO and its affiliates (and any of their respective directors, officers, agents, contractors, interns, suppliers, and employees) will not be liable for any damages, losses or causes of action of any nature arising from any use of any TCO sample documents or the provision of such sample documents.

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 cards and exchanging currency for currency. Cash-out transactions (where cash is given 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 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 – A Money Services Business (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.

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 cards 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.

Routing Number - Used by banks to identify themselves in the clearing process. The routing number is found on the encoding line and is usually the second set of numbers. Routing number is always nine (9) digits. The first two digits identify which banking district the bank is located, and will be between 01-12 and 21-32.

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).

USA PATRIOT Act – 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.

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 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.

Licensing and Reporting Requirements

FinCEN Registration

FinCEN Registration of an MSB is the responsibility of the owner or controlling person of the MSB. Registration, through FinCEN Form 107, must be completed by the owner or controlling person and filed within 180 days after the date on which the MSB was established.

Registration must be renewed every two (2) years. Copies of the filed registration form and supporting documentation must be retained for a period of five (5) years.

FinCEN may impose civil and criminal penalties for violation of the registration requirement.

Report of Foreign Bank & Financial Accounts (FBAR)

A U.S. person, including a citizen, resident, corporation, partnership, limited liability company, trust, and estate, must file an FBAR to report:

1. a financial interest in or signature or other authority over at least one financial account located outside the United States if.
2. the aggregate value of those foreign financial accounts exceeded $10,000 at any time during the calendar year reported.

The FBAR is an annual report, due April 15 following the calendar year reported.

Government Filings

MSBs are required to file the following reports with FinCEN:

- Currency Transaction Report (CTR) – cash transactions in excess of $10,000 in currency
- Suspicious Activity Report (SAR) – activity that appears to be suspicious or unusual in nature, and where the amount is $2,000 or more.

State-Level Licensing

As a condition of FinCEN registration, MSBs must obtain licensure from the state(s) within which they operate that require licensing. Thus far, states have taken a diverse array of approaches to the regulation of digital currency MSBs. State-level registration remains highly fluid and subject to change at any moment. With greater subject matter understanding and growing adoption of digital currencies, financial regulators will continue to evolve their requirements and expectations.

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 Internal Controls
2. A designated Compliance Officer
3. Employee Training Program
4. Independent Review & Testing of the AML Program
5. Establishment of a Risk Based Customer Due-Diligence Procedure

SECTION 4: Employee Compliance Training Program

The front line in the war against money laundering and other financial crimes is the financial institution's tellers. A comprehensive training program is critical to ensure that the Company's employees are knowledgeable and in compliance with all pertinent laws and regulations, while accurately and efficiently processing transactions.

SECTION 5: 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 and the financing of terrorism, with increased enforcement beginning in 2010.

Money Laundering occurs when someone knowingly conceals the illegal source of their funds and conducts transactions designed to make their funds appear "clean". The objective is to deceive the authorities by making assets appear to have been obtained through legal means, or appear to be owned by unrelated third parties. They may also be trying to avoid government-reporting requirements for payment of taxes.

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.

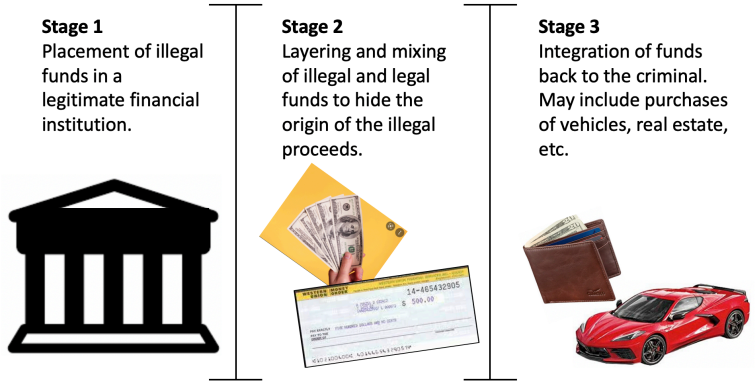
Money laundering is a major threat to financial institutions and the economic stability of entire countries. Governments worldwide have introduced legislation to prevent it, including specific money laundering offenses and legally imposed requirements on institutions operating in their jurisdictions.

The economic/social consequences of money laundering include:

- Increased crime and corruption
- Undermining the legitimate private sector
- Weakening financial institutions
- Loss of control of, or mistakes in, economic policy
- Economic distortion and instability
- Loss of tax revenue
- Reputation risk for the country
- Social costs

Why do criminals launder money?
In order to enjoy their ill-gotten gains, criminals must find a way to use the funds without drawing attention to the underlying activity or "predicate crime" involved in generating such profits.

Money Laundering occurs in three stages:



1. Placement: When cash first enters the financial system. 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.*

   Placement of currency into the financial system is often the most difficult step in laundering, particularly for drug traffickers. Traffickers can receive hundreds of thousands of dollars a day in small bills. The Bank Secrecy Act currency reporting provisions have created a logistical nightmare for traffickers. Traffickers can no longer simply take their cash to the bank for deposit or wire transfer abroad. Now they must smuggle their cash into the financial system, either within the United States or outside the United States. Launderers are always trying to find innovative ways to get their cash into the financial system. Some of these innovations have directly affected the check cashing industry.

2. Layering: The movement of funds in an effort to further disguise the audit trail and ownership of funds. This stage further separates the money from its criminal origin. 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.

   Launderers layer funds by moving them from one financial institution to another. These institutions are often banks in foreign countries that have very strict bank secrecy laws. The bank accounts are often held in the names of various secrecy haven companies. Launderers form these companies using local attorneys who act as the registered representative in the secrecy havens. The companies' stock may be in the form of bearer shares. Whoever has physical possession of the shares owns the companies. The attorneys are not required to register the shares in any person's name. This movement of

funds sets up a series of layers, each protected by secrecy laws. The bank account is secret. The company ownership is secret. This system of layers makes it extremely difficult for anyone to trace the source or disposition of funds that have entered the system.

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.
   The final step in the laundering process is integration. This is the process of bringing the funds back into the open, disguised as "legitimate" funds. Obviously, dirty money is no good to anyone if they cannot use it. Therefore, launderers must devise a way to use the money without revealing its source or true ownership. Funds are integrated in any number of ways. One of the most common is to "loan" the funds to a business or person. Launderers set up "finance companies" in the secrecy havens that loan money to the true owner's business. The finance companies issue full documentation for the loans. They charge interest, which the launderers pay to increase the disguise. They may even repay the loans.

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. The purpose of this law is to require financial institutions to assist the U.S. government in detecting and preventing money laundering.

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 Treasury Department. 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.

Money Laundering Techniques

Techniques utilized by criminals to launder illicit funds are nearly infinite and becoming increasingly more creative in order to adapt to a strengthening regulatory environment. Nevertheless, there are some core money laundering techniques all personnel should understand and be able to detect.

Structuring

Executing transactions in a pattern calculated to avoid certain government reports required by law.

For example, a Currency Transaction Report (CTR) must be filed for cash transactions in excess of $10,000.

- Scenario 1: Criminal breaks up a $12,000 transaction into two $6,000 transactions.
- Scenario 2: Criminal makes routine transactions of $9,900, just under the reporting threshold.

Rapid Movement of Funds

Executing a series of transactions in rapid succession that do not appear to have a lawful purpose. The activity often does not make sense or is not the most efficient manner for transferring stored value.

Social Engineering

The process of psychologically manipulating people into performing actions or divulging information. For example, a criminal calls an institution to request help avoiding reporting requirements or divulging proprietary Know Your Customer (KYC) thresholds and other controls in order to inform his/her tactics.

SECTION 6: Customer Verification

The war against money laundering starts with verifying the identity of the consumer at the front desk. The company and its employees must make every effort to ascertain the identity and check cashing habits of their consumers. This policy protects the consumers and the Company and helps to guard against money laundering and other financial crimes.

A concerted effort to "Know Your Customer" is a key tool for addressing the problem of money laundering and its related consequences. Knowing your customer may also enable you to stop your valued customer.

There are three main points to consider when evaluating a check before cashing it. The first is, are we paying the right person? The second, is the check good? The third is, could we find this person and collect our money if the check is returned?

Throughout the transaction, always ask yourself, "Does this transaction make sense"?? (i.e.: an 18-year-old boy comes in to cash a monthly Social Security check, his name is Bob Smith, but the name on the check reads "Bob Smith, Sr.).

Acceptable Forms of Identification

- Valid government issued documents containing the customer's name, photograph, and street address.
- Driver's License
- Passport
- State-Issued Identification
- National Identification Card
- Alien Identification Card
- Military ID
- Mexican Metricula Card

Evaluating First Time Customers

While it is very possible for existing customers to pass bad checks, usually, majority of checks that are returned and are not collected are the first check that a customer presents. It is with this understanding of the business that we recommend verifying the checks of all first-time customers.

When cashing a payroll check from an unfamiliar local business, you should look up the business online. Then contact the issuer & the bank on which the check is drawn to confirm that the account is active, and the check was legitimately issued.
The endorsement should be examined closely before cash is paid to the customer. It must match the signature on the customer's identification. Checks presented by the payee should always bear the payee's endorsement exactly as it is written on the "Pay to the Order of" line on the check.

Common sense is a very strong tool when evaluating customers and their checks. For example: what is acceptable identification for a teenager presenting a check from a fast-food restaurant is not acceptable for the truck driver working for a national carrier.

Most of the criminal element passing bad checks will not invest the time to create a check history with you in order to pass one check that is bad. They strike once or several times very quickly and then move on.

Evaluating Existing Customers

Along with the other steps in evaluating checks, which we will discuss below the first step when presented with a check from an existing customer, is to compare his check history to the check he is presenting.

The questions that should be answered by the history should be:

1) Is this check from the same maker as his previous checks?
2) Is the date of this check too close to his previous check of this type?
3) Is the amount of this check comparable to the previous check?
4) Is there any information on this check that is different than the previous check?

SECTION 7: Office of Foreign Assets Control (OFAC)

OFAC is an office of the U.S. Treasury that administers and enforces economic sanctions and embargoes based on U.S. foreign policy and national security goals that target geographic regions and governments (e.g., Cuba, Iran, and Syria), as well as individuals or entities that could be anywhere (e.g., international narcotics traffickers, foreign terrorists, and proliferators of weapons of mass destruction). As part of its enforcement efforts, OFAC publishes a list of Specially Designated Nationals and Blocked Persons (SDN list), which includes names of companies and individuals who are connected with the sanction's targets. U.S. persons are prohibited from dealing with SDNs wherever they are located, and all SDN assets must be blocked.

All check cashing customers must be searched against the OFAC Database (http://sdnsearch.ofac.treas.gov/) when they perform a check cashing transaction. The customer's ID name and information must be scrubbed against the OFAC Database to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC.

Searching customers against OFAC can be done manually using the link above, but is often hardwired into check cashing point-of-sale (POS) systems to search customers automatically at the time of transaction.

If it is determined that a customer is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, the transaction should be rejected and/or customer's assets blocked, and a blocked asset and/or rejected transaction form should be filed with OFAC within 10 days. The OFAC Hotline should also be called immediately at (800) 540-6322.

SECTION 8: Evaluating Checks

The process in evaluating checks starts with the check and the identifications being presented. The experienced check casher will be able to evaluate a check in a few moments.

The goal in evaluating a check is to determine if there is sufficient information to reasonably cash this check without verifying it or do I need to do further work?

"Red flags" are scenarios that may be indicative of potential money laundering. Being able to spot "red flags" is critical to a successful BSA/AML Program, both as a method to strengthen AML processes and to demonstrate to regulators the soundness of the overall program. "Red flags" are numerous and constantly evolving as money launderers become increasingly sophisticated and creative. While not suspicious activity in and of itself, a "red flag" raises the alarm and encourages subsequent action, including, but not limited to, further investigation or the reporting of illegal activities to relevant authorities.

The ten procedures below are to be performed on every check when it is presented at the window to help identify "red flags". We have found that if the check casher is trained early on in their training to examine checks in a specific order that it will become second nature to them.

1) Examine The Pay To Line & Customer Identification

The first and most important item that needs to be checked is the pay to line; this is the line that indicates who the check is payable too. This line instructs the check casher to verify the identification of all individuals named on the check. If there are multiple payees, then each payee needs to present proper ID. The ID must match the pay to line.

It is best practice to require that each payee named on the check be present when the check is cashed. The only exception to this rule is when one or more of the payees are businesses. If a business is named as a payee, then the check casher must verify that the appropriate representative of the business has endorsed the item.

By reading the pay to line it should be clear who needs to be present with Identification.

Examples:

Pay to the order of:	John and Mary Smith	Both John & Mary
Pay to the order of:	John Smith for Mary Smith	Only John not Mary
Pay to the order of:	John Smith c/o Mary Smith	Only John not Mary
Pay to the order of:	John Smith Mary Smith	Both John & Mary
Pay to the order of:	John Smith, Mary Smith & GMAC Mortgage	Both John, and Mary with a call placed to GMAC, or GMAC has stamped off on it

Once you have established who the check is payable to, take as much ID as they have on your side of the teller window. The minimum they should have been a government issued picture ID, like a valid driver's license, state issued ID card, US passport, resident alien card, or welfare card. It is also recommended that they provide a secondary ID, but this ID alone may NOT be sufficient to cash a check. Examples of secondary ID are Social Security cards, membership cards, credit cards or employee work ID (these are easily forged so be cautious) from a company with which you are familiar.

Also ask for the check stub or envelope that the check was mailed in, when asking for ID, as this is another indication that the person at the window is the actual payee.

2) Examine The Date Of The Check

The "fresher" the date is, the better the check is. It is recommended that you call the maker and verify there are no stop payments or holds on a check if the date is older than ten days. Remember that many of your customers will not, or cannot wait for their money and typically present their checks for payment as soon as they are received. The older a check, the greater the risk of it having a stop payment order placed against it. Checks older than thirty days become less collectable under the uniform commercial code and should be reissued by the maker.

Also, be careful that the check is not being presented prior to the check date. This occurs if a check was post-dated. It is recommended that you do not cash checks that are presented more

than 2 days prior to the check date. Some states mandate no post-dated checks in their regulations.

3) Examine The Check Number

All checks are numbered. Checks with low check numbers may be issued from newer accounts and are the most frequently returned for "non-sufficient funds" and "account closed". The cause of this is that many new businesses will be started by individuals with limited capital and business experience. If business is not profitable, they run into problems and checks will bounce.

The check number on most checks will appear in two places, the upper right corner and lower left corner on the encoding line. The numbers should be the same. If not, call the maker to verify the issuance of the check. Business checks generally start at 1001 and personal checks at 101. This is not a rule, and can vary from maker to maker.

4) Examine The Addresses Of The Maker & The Payee

The maker's address should be on the check. If not, you must determine it from an outside source or web search. Be suspicious if the address is a PO box. The payee's address should be on their identification and may be on the check. If the addresses do not match, require the payee to produce some material (mail, utility bill) that has his name and present address (check address). Either the maker's or payee's address should be in your local area as customers will usually not drive out of their local area to cash a check unless they work out of that area. Payee addresses can be verified from the customer's valid ID. If a difference exists between the payee address on the ID and check, determine the present address for your records by searching on-line, and/or calling the employer or a relative.

5) Examine The Amount Of The Check

Always use the written amount of the check (words) as the true amount because the numeric amount (numbers) can be easily forged. The written amount and the numeric amount should match exactly. The dollar amount should be written in words or by a check imprinter or computer and should reflect the type of work that the customer does. Be careful of checks that end in an even amount that appear to be payroll checks: there should be itemized deductions of uneven amounts. Forgers will generally create checks in amounts that are not so large to prompt a phone call, but still large enough to make it worth their while, approximately $600 or less. Many employers issue payroll checks bi-weekly, so a good question to ask a customer whose check amount seems out of line is "Is this check for one week's work?" You would like the customer to answer "no" because most passers of bad checks will answer "yes" to questions asked of them. Keep in mind that as the amount of the check increases, the amount of ID and the need to verify the check and ID increases.

6) Examine The Appearance Of The Check

You should be looking at the overall appearance of the check, paying special attention to the encoding and perforation. Many large organizations and companies will have security features built into their check stock. Examine the security features of the check. These are usually printed on the check.

Examples are:

1) Look for the "mp" symbol that indicates somewhere on the check micro printing should appear. It will first appear as a line but if you look closer you will see it very small print that a copier will be able to copy.

2) Stains or watermarks with the Company's name or logo are visible when you hold the check up to a light.

Look for erasures or misspellings; the appearance should be professional looking. Does it make sense for this company to be using this style of checks? Large employers will use check stock that has been special prepared for them not generic stock purchased from office supply stores. Many employers will subscribe to payroll services, such as ADP and Paychex.

Encoding is without variation and will appear the same way on every check issued from the any bank. Encoding is printed using magnetic ink, which is black and will have a dull finish. If it shines or feels raised, it may be forged. Most importantly, the numbers themselves should be formed the same way from one check to the next. A simple test is to compare the encoding of the check in question to a good check. The micro encoding numbers will appear in a different order but will be the exact size and shape.

7) Examine The Routing & ABA Codes

These are numbers used by banks to identify themselves in the clearing process. The routing code of a bank is found on the encoding line and is usually the second set of numbers. The first two digits identify in which banking district the bank is located, and will be between 01 – 12 and 21 – 32. The name of the bank on which the check is drawn should appear on the check as well. The ABA number appears as fraction and parts of it are contained in the routing number.

8) Obtain The Customer's Social Security Number

Do so by copying the number from their Social Security card if presented to you as ID. If the payee does not have their card their number may be on their pay stub. Some payees will be reluctant to provide their number for security reasons.

Social security numbers reveal information that is helpful when cashing a check. The first 3 digits indicate the state in which the number was issued. The next 2 indicate the year of issue. For additional information, see the Social Security number verification manual.

*Note: SSNs issued on June 25, 2011, or later were assigned based on "randomization" of numbers. This has eliminated the geographical significance of the SSN noted above for SSNs issued on June 25, 2011 or later.

9) Examine The Customer's Signature & Compare It To The ID

Have the customer sign the check in your presence. Compare the signature on the check to the signature on the ID and record the ID in the POS.

In cases where there are multiple payees make sure you have each payee sign the check and compare the signatures to the IDs.

10) Record The Customer Information Into The POS

When entering the customer information into the POS it is recommended that you ask the question to fill in the fields and compare the information given to the identification presented in Step 1. Look for inaccuracies and be wary of any customer that cannot answer these questions or appears nervous while giving answers.

SECTION 9: Check Fraud

There are many ways that people can commit check fraud, and criminals can be very skilled at this, making detection of fraud/altered checks very hard. Even the most cautious consumers can fall victim to check fraud. Detecting fraud starts with a diligent check cashing process. By properly checking checks, catching red flags, and knowing what to look for will help stop fraudulent activity before it starts**.** If you believe a customer has brought you a fraud check, reach out to your company's Compliance Officer to verify next steps.

Types of Check Fraud

- *Forgery:* For a business, forgery typically takes place when an employee issues a check without proper authorization. Criminals will also steal a check, endorse it, and present for payment at a retail location or at the bank teller/FLA window, probably using bogus personal identification.
- *Counterfeiting:* Counterfeiting can either mean wholly fabricating a check – using readily available desktop publishing equipment consisting of a personal computer, scanner, sophisticated software, and high-grade laser printer – or simply duplicating a check with advanced color photocopiers.
- *Alteration:* Alteration primarily refers to using chemicals and solvents such as acetone, brake fluid and bleach to remove or modify handwriting and information on the check. When performed on specific locations on the check such as the payee's name or amount, it is called spot alteration; When an attempt to erase information from the entire check is made, it is called check washing.
- *Paperhanging:* This problem primarily has to do with people purposely writing checks on closed accounts (their own or others), as well as reordering checks on closed accounts (theirs or others).
- *Check Kiting:* Check kiting is opening accounts at two or more institutions using "the float time" of available funds to create fraudulent balances. This fraud has become easier in recent years due to new regulations requiring banks to make funds available sooner, combined with increasingly competitive banking practices.

Unusual Customer Activities

People committing check cashing fraud often exhibit certain behaviors that can be red flags, such as being overly friendly/ asking questions or trying to buy other things to get you to not fully inspect the check, rushing the teller or being impatient, seeming nervous, fidgety, or looking around/avoiding eye contact.

- A customer, for no apparent reason, cannot give sufficient information to enable you to record appropriate monetary instrument identification information or to complete a required CTR.
- A customer refuses to provide the information necessary to enable you to record appropriate monetary instrument identification or wire transfer information or to complete a required CTR.
- A customer cancels a transaction and leaves without providing further information when you ask the customer for identification and the additional information necessary to record appropriate monetary instrument identification information or to complete a required CTR.

SECTION 10: Suspicious Activities Related to Business Check Cashing

There are legitimate reasons for a business to use the services of a check casher; however, we must satisfy ourselves as to the legitimacy of the customer's use. The following are examples of "red flags" of business transactions that may prove to be suspicious. It is important to review these transactions based upon what you know about the business customer involved. It is important to review these transactions based upon what you know about the business customer involved. You should investigate the circumstances of these types of transactions in order to satisfy yourself that they are legitimate.

- A business consistently cashes an unusual number of checks made payable to the business, in a manner that appears to be designed to evade the BSA/AML compliance filings.
- A known business owner conducts an unusual number of wire transfers or buys large volumes of money orders with third party checks, in a manner that appears to be designed to evade the stores compliance policies.

We should have strict compliance and KYC practices for businesses cashing checks made payable to their business and/or third-party checks. We should ensure that each transaction fits within these compliance measures.

- If a customer attempts to evade these requirements, the check casher should consider the transaction suspicious.
- A person buys an unusual number of money orders with his/her own business checks or cashes an unusual number of his/her own business checks.
- An individual attempts to cash a bank check or cashier's check that has multiple endorsements on the back, in a manner that appears to be designed to evade the check casher's compliance procedures.

SECTION 11: Suspicious Activity Report (SAR)

A Suspicious Activity Report (SAR) is the form the Compliance Officer fills out and sends in when they 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.

As frontline employees interacting with customers, tellers must continually observe and get to know their customers in order to know when to initiate the SAR process.
If you believe that a customer is engaging in possible suspicious activity:

1. Do not tip off the customer that you are suspicious!
2. Document the customer and transaction information and give it to the Compliance Officer.

You should never tell the customer that you think their behavior or check is suspicious. The Compliance Officer will discuss the transaction with you to determine if a SAR must be submitted.

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.

Copies of all SARs filed and supporting documentation must be retained by the Company for five years from the date of filing the SAR.

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 12: 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).

Who or What is a Person?
The regulation defines a "person" as an individual, a corporation, a partnership, a trust or estate, a joint stock company, an association, a syndicate, joint venture, or other unincorporated organization or group, and all entities cognizable as legal persons. As a practical matter, this definition includes any payee on a check or monetary instrument.

What is Cash-In/Cash-Out?
The Treasury Department classifies transactions as either cash-in or cash-out. Cash-in transactions include such currency transactions as buying money orders, sending wire transfers, and exchanging currency for currency. Cash-out transactions include cashing checks, receiving wire transfer proceeds in currency, and exchanging currency for currency.

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.

> An example of a multiple transaction would be a person bringing in a corporate check issued to John Doe Corporation for $7,000 in the morning and later in the same day the same person brings in a check issued to John Doe Corporation for $5,000. Since the checks cashed total $12,000 in a 24-hour period, 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 13: 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 14: 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 15: 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 16: 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 17: 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.