



MONEY LAUNDERING PREVENTION

A Money Services Business Guide

Financial Crimes Enforcement Network
U.S. Department of the Treasury
Washington, DC



Your business may be an MSB (Money Services Business) if...

The business offers one or more of the following services:

- money orders
- traveler's checks
- check cashing
- currency dealing or exchange
- stored value

-AND-

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.

-OR-

The business:

- Provides money transfer services in any amount.

Table of Contents

Introduction	1
Background on Money Laundering	2
Bank Secrecy Act (BSA) Regulations	4-9
Summary of Certain BSA Regulations	4
Registration Requirements.....	6
Filing Instructions.....	7
Agent Lists.....	7
Supporting Documentation.....	8
Civil and Criminal Penalties.....	9
MSBs Can Help Fight Money Laundering	10-24
Establish Anti-Money Laundering Compliance Programs	10
Establish Customer Relationships	11
File Suspicious Activity Reports	12
What is "Suspicious Activity?".....	14
Red Flags	16
What Should MSBs Look For?.....	17
MSBs Can Help In Other Ways.....	25-28
File Currency Transaction Reports.....	25
Keep Records.....	26

Table of Contents (Cont.)

Reports That Can Help MSBs Identify Suspicious Transactions	29-31
Cash-In and Cash-Out of Large Transaction Reports	29
Kiting Reports	29
Money Transfer Reports	29
\$3,000 Instrument "Log"	30
Clearance Records/Receipts	30
\$3,000 Funds Transfer Records	30
Customer Activity Reports	31
Some Money Laundering Schemes	32
Legislation	36
International Money Laundering Efforts	41
Country Advisories and Economic Trade	43
Glossary	44

Introduction

Money is “laundered” to conceal illegal activity, including the crimes that generate the money itself, such as drug trafficking. Money laundering conceals the source of illegal proceeds so that the money can be used without detection of its criminal source.

Financial institutions – including the expanding network of money services businesses (MSBs) – have been both witting and unwitting participants in laundering activities. Banks have been major targets in laundering operations because they provide a variety of services and instruments, including cashier’s checks, traveler’s checks, and wire transfers, which can be used to conceal the source of illicit proceeds. Similarly, criminals use MSBs – establishments that provide money orders, traveler’s checks, money transfers, check cashing, currency exchange, and stored value services – to hide or disguise the origin of funds derived from illegal activity.

In order to protect themselves, and to support national and international efforts against financial crime, it is important that MSBs know how money laundering schemes can operate.

This guide provides some basic background information on money laundering laws, discusses actions taken in the international arena, describes several schemes that have involved financial institutions, and gives examples of certain warning signs that may help MSBs protect themselves against money launderers and other criminals.

Background on Money Laundering

Money laundering can be a complex process. It involves three different, and sometimes overlapping, stages:

Placement involves physically placing illegally obtained money into the financial system or the retail economy. Money is most vulnerable to detection and seizure during placement.

Layering involves separating the illegally obtained money from its criminal source by layering it through a series of financial transactions, which makes it difficult to trace the money back to its original source.

Integration involves moving the proceeds into a seemingly legitimate form. Integration 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 try to avoid leaving this "paper trail" by avoiding reporting and recordkeeping requirements.

One way money launderers avoid reporting and recordkeeping requirements is by "structuring" transactions, coercing or bribing employees not to file proper reports or complete required records, or by establishing apparently legitimate "front" businesses to open accounts or establish preferred customer relationships.

Background on Money Laundering

In recent years, more countries have implemented laws to combat money laundering. Financial service regulators and enforcement agencies around the world are working to improve communications and share information in anti-money laundering efforts.

In this guide, you will find a summary of these international initiatives, as well as efforts the government has taken to combat money laundering in the United States. You will also find ways you can help combat money laundering and make your community – and your country – a safer place to live and work.

Bank Secrecy Act (BSA) Regulations

The Financial Crimes Enforcement Network (FinCEN), a bureau of the U.S. Department of the Treasury, administers and issues regulations pursuant to the Bank Secrecy Act (BSA). Through certain BSA reporting and recordkeeping requirements, paper trails of transactions are created that law enforcement and others can use in criminal, tax and regulatory investigations.

The reporting and recordkeeping provisions of the BSA apply to banks, savings and loans, credit unions and other depository institutions (collectively referred to as "banks") and to other businesses defined as financial institutions, including casinos, brokers and dealers in securities, and money services businesses (collectively referred to as "non-banks").

BSA regulations require certain Money Services Businesses (MSBs) to register with FinCEN and prepare and maintain a list of agents, if any. In addition, BSA regulations require certain MSBs to report suspicious activity to FinCEN.¹

Summary of Certain BSA Regulations

- 1. Registration** – each business that meets the definition of an MSB must register, except for the following:
- A business that is an MSB solely because it serves as an agent of another MSB;
 - A business that is an MSB solely as an issuer, seller, or redeemer of stored value;
 - The U.S. Postal Service and agencies of the U.S., of any State, or of any political subdivision of any State.

¹ See 31 CFR103.20

Bank Secrecy Act (BSA) Regulations

- A branch office of an MSB is not required to file its own registration form.

2. Agent List –

- MSBs that are required to register must prepare and maintain a list of their agents, if any, each January 1 for the preceding 12-month period.
- Upon request, MSBs must make their list of agents available to FinCEN and any other appropriate law enforcement or supervisory agencies (including the IRS in its capacity as BSA examination authority).

3. Suspicious Activity Report (SAR) – MSBs required to file SARs are:

- MSBs serving as money transmitters;
- Currency dealers or exchangers;
- Issuers, sellers, or redeemers of money orders;

- Issuers, sellers, or redeemers of traveler's checks; and
- U.S. Postal Service.

MSBs must maintain a copy of all SARs filed as well as the original or business record equivalent of any supporting documentation for a period of five years from the date of the report. Supporting documentation must be identified as such, and, although it is not to be filed with the report, supporting documentation is deemed to have been filed with the report. Upon request, MSBs must make all supporting documentation available to FinCEN and any other appropriate law enforcement or supervisory agencies (including the IRS in its capacity as BSA examination authority).

Bank Secrecy Act (BSA) Regulations

Summary of Certain BSA Regulations (cont.)

4. Anti-Money Laundering (AML) Compliance Program – all MSBs, including issuers, sellers, or redeemers of stored value, are required to develop and implement an AML compliance program as required by section 352 of the USA PATRIOT Act and implemented by regulation at 31 CFR 103.125.

5. Currency Transaction Report (CTR) – MSBs must file CTRs on transactions in currency involving more than \$10,000, in either cash-in or cash-out, conducted by, through, or to the MSB on any one day by or on behalf of the same person.

6. Monetary Instrument “Log” – MSBs must maintain certain information on the sale of monetary instruments – such as money orders or traveler’s checks – from \$3,000 to \$10,000, inclusive.

7. Funds Transfer Rules – MSBs must maintain certain information for funds transfers, such as sending or receiving a payment order for a money transfer, of \$3,000 or more, regardless of the method of payment.

8. Currency Exchange Record – MSBs must maintain certain records for each currency exchange in excess of \$1,000.

9. Record Retention – All BSA records must be retained for a period of five years and must be filed or stored in such a way as to be accessible within a reasonable period of time.

Registration Requirements

BSA regulations require certain MSBs to have registered with FinCEN by December 31, 2001. An MSB established after that date must register by the end of the 180-day period beginning on the day after the date

Bank Secrecy Act (BSA) Regulations

it was established. A branch or an agent of an MSB is not required to file its own registration form. The U.S. Postal Service and Federal or State government agencies are not required to register. Also, MSBs that provide only stored value services are not required to register at this time.

MSBs are required to renew their registration every two years by December 31 at the end of the two-calendar year period following their initial registration. In addition, MSBs that are required to register are also required to prepare and maintain a list of agents, if any, each January 1 for the preceding 12-month period.

Filing Instructions

MSBs must register by filing Form TD F 90-22.55, Registration of Money Services Business, which is available at www.msb.gov

or by calling the IRS Forms Distribution Center at 1-800-829-3676. Registration is the responsibility of the owner or controlling person of the MSB, who must sign and file the completed registration form.

Agent Lists

An MSB that is required to register and that has agents must prepare and maintain a list of those agents. This list must be updated by January 1 of each year. An MSB must make its list of agents available to FinCEN, as well as other appropriate law enforcement agencies, including the IRS, upon request. Generally, the agent list must include:

- *Name*: The name of the agent, including any trade names or doing-business-as names.

Bank Secrecy Act (BSA) Regulations

Agent Lists (cont.)

- *Address:* The address of the agent, including street address, city, state, and ZIP code.
- *Type of Services:* The type of MSB services the agent provides on behalf of the MSB maintaining the list.
- *Gross Transaction Amount:* A listing of the individual months in the 12 months preceding the date of the agent list in which the agent's gross transaction amount, for financial products or services issued by the MSB maintaining the agent list, exceeded \$100,000.
- *Depository Institution:* Name and address of any depository institution at which the agent maintains a transaction account for any of the funds received in or for the MSB services the agent provides on behalf of the MSB maintaining the list.

- *Year Became Agent:* The year in which the agent first became an agent of the MSB.
- *Branches:* The number of branches and sub-agents the agent has, if any.

Supporting Documentation

Supporting documentation, including a copy of the filed registration form, an estimate of business volume, information regarding ownership or control, and the agent list must be retained by the MSB for a period of five years.

Bank Secrecy Act (BSA) Regulations

Civil and Criminal Penalties

Civil and criminal penalties can be imposed for violations of anti-money laundering laws and regulations. Penalties can result in substantial fines and in prison terms. Any MSB that fails to comply with BSA reporting and record keeping requirements faces possible civil penalties of up to \$500 for negligent violations and the greater of the following two amounts for willful violations: the amount involved in the transaction (up to \$100,000) or \$25,000. Under certain circumstances, businesses can also be held criminally liable for the acts of their employees. The maximum criminal penalty for violating a BSA requirement is a fine of up to \$500,000 or a term of imprisonment of up to 10 years, or both.

It is therefore important that employees are thoroughly trained on how to comply with BSA regulations and that a system is in place to ensure that employees are

following all anti-money laundering laws and regulations.

MSBs can do a great deal to help the federal government in its anti-money laundering efforts. At a minimum, MSBs should file all BSA reports accurately and in a timely fashion, create and maintain accurate BSA records for the requisite time period, establish and maintain appropriate compliance programs and follow all Treasury Department guidance related to the BSA.

MSBs Can Help Fight Money Laundering

Establish Anti-Money Laundering Compliance Programs

Each MSB is required by law to have an effective anti-money laundering (AML) compliance program. The regulation requiring MSBs to develop and maintain an AML compliance program is contained in 31 CFR 103.125. Each program must be commensurate with the risks posed by the location, size, nature and volume of the financial services provided by the MSB. For example, a large money transmitter with a high volume of business located in the Los Angeles area is at higher risk than a small check casher with a low volume of business located in Boise. Therefore, the large California money transmitter would be expected to have a more complex AML compliance program, commensurate with its higher risk, than the smaller Idaho

check casher, who is at lower risk of being used to facilitate money laundering. An effective program is one designed to prevent the MSB from being used to facilitate money laundering.

Each AML compliance program must be in writing and must:

- Incorporate policies, procedures and internal controls reasonably designed to assure compliance with the BSA;
- Designate a compliance officer responsible for day-to-day compliance with the BSA and the compliance program;
- Provide education and/or training of appropriate personnel; and
- Provide for independent review to monitor and maintain an adequate program.

MSBs Can Help Fight Money Laundering

Strong management commitment to the AML compliance program promotes ongoing compliance and helps prevent the MSB from being used by money launderers.

FinCEN further encourages MSBs to adopt policies and procedures that incorporate the Basel Committee Statement of Principles on Money Laundering, which urges:

- Proper identification of all persons conducting financial transactions with the financial institution.
- High ethical standards in financial transactions and compliance with laws and regulations governing financial transactions.
- Cooperation with law enforcement.
- Information and training for staff to ensure that they can and do carry out these principles.

Establish Customer Relationships

Strict customer identification and verification policies and procedures can be a financial institution's most effective weapon against money laundering. Requiring appropriate identification and verifying information in certain cases, and being alert to unusual or suspicious transactions can help an MSB deter and detect money laundering schemes.

A customer identification and verification policy tailored to the operations of a particular business:

- Helps detect suspicious activity in a timely manner.
- Promotes compliance with all state and federal laws applicable to MSBs.
- Promotes safe and sound business practices.

MSBs Can Help Fight Money Laundering

Establish Customer Relationships (Cont.)

- Minimizes the risk that the MSB will be used for illegal activities.
- Reduces the risk of government seizure and forfeiture of funds associated with customer transactions (such as outstanding money orders/traveler's checks and outstanding money transfers) when the customer is involved in criminal activity.
- Protects the reputation of the MSB.

File Suspicious Activity Reports

Suspicious Activity Reports (SARs) are among the government's main weapons in the battle against money laundering and other financial crimes. Such reports are also a key component of an effective anti-money-laundering compliance program.

Many MSBs are required to file SARs when they suspect that potentially illegal activity has occurred **and** when the activity has met the relevant reporting threshold.

The types of MSBs that are currently covered by the MSB SAR requirements are:

- Money transmitters,
- Currency dealers or exchangers,
- Money order – issuers, sellers or redeemers,
- Traveler's checks – issuers, sellers, or redeemers,
- U.S. Postal Service

MSBs that provide only check cashing or stored value services are not required to report suspicious activity at this time.

Refer to www.msb.gov for updates on which MSBs are required to file SARs.

MSBs Can Help Fight Money Laundering

A SAR must be filed by an MSB when a transaction is **both**:

- Suspicious, *and*
- \$2,000 or more (\$5,000 or more for issuers reviewing clearance records).

A SAR must be filed within 30 days of detection of the suspicious transaction by the MSB.

MSBs that are not currently covered by the SAR rule – check cashers, and issuers, sellers, or redeemers of stored value – may voluntarily file SARs. Any MSB may also voluntarily file SARs for suspicious activity below the reporting threshold.

It is illegal to tell any person involved in a transaction that a SAR has been filed. Maintaining the confidentiality of SARs will prevent suspected individuals involved in criminal activity from structuring their activity in such a way as to evade detection by law enforcement. It also will help

protect the MSB filing the report. A SAR and/or the information contained in a SAR must only be provided to FinCEN or an appropriate law enforcement or supervisory agency when requested.

Some suspicious transactions require immediate action. **If the MSB has reason to suspect that a customer's transactions may be linked to terrorist activity against the United States, the MSB should immediately call the Financial Institutions Hotline, toll-free at: 1-866-556-3974.**

Similarly, if any other suspected violations – such as ongoing money-laundering schemes – require immediate attention, the MSB should notify the appropriate law enforcement agency. In any case, the MSB must also file a SAR if the MSB is subject to mandatory reporting. A BSA provision (called a "safe harbor") provides broad protection from civil liability to MSBs and their employees that file SARs or otherwise report suspicious activity.

MSBs Can Help Fight Money Laundering

What is “Suspicious Activity?”

A SAR must be filed by a covered MSB when the MSB knows, suspects or has reason to suspect that the transaction or pattern of transactions is suspicious and involves \$2,000 or more. A suspicious transaction is one or more of the following:

- **Involves funds derived from illegal activity**, or is intended or conducted in order to hide or disguise funds or assets derived from illegal activity.
- **Is designed to evade BSA requirements**, whether through structuring or other means.
- **Appears to serve no business or apparent lawful purpose**, and the MSB can determine no reasonable explanation for the transaction after examining all available facts.

- **Involves use of the money services business to facilitate criminal activity.**

All MSBs should have a system or procedure to ensure that SARs are filed when appropriate. When an MSB employee suspects a person is laundering money, conducting transactions to evade BSA requirements, or conducting a transaction that has no apparent lawful purpose and for which no reasonable explanation can be determined, or involves use of the money services business to facilitate criminal activity, the employee should report that activity to his/her manager or to the MSB compliance officer. Then, if the MSB determines that a SAR should be filed, it must file the SAR and keep a copy of it for five years. Any supporting documentation, such as transaction records, must be maintained with the copy of the filed form and also kept for five years from the date of filing the report.

MSBs Can Help Fight Money Laundering

What are "Funds Derived from Illegal Activity?"

The phrase "funds derived from illegal activity" means the monetary proceeds of a criminal act.

Example. A drug trafficker sells drugs to a user for \$500. The money received from the drug purchaser, the \$500, is proceeds of the drug sale and is "funds derived from illegal activity."

What is a transaction that "Is Designed to Evade BSA Requirements?"

Example. A customer conducting an \$11,000 cash transaction attempts to bribe an MSB employee not to file a CTR.

What is a Transaction that "Serves No Business or Apparent Lawful Purpose?"

Some transactions may be conducted in such a way that they appear unusual or suspicious. However, additional facts, if known by the reporting business, might disclose a reasonable basis for what, at first, appears unusual or suspicious.

Example. A customer, a retired teacher, frequently sends and receives money transfers of more than \$2,000 to and from many different people. The MSB might at first conclude that these transactions are suspicious because they appear to "serve no business or apparent lawful purpose" and because there does not seem to be a legal source for these funds. However, with more information, the MSB might conclude that a business purpose exists. For example, the retired teacher might be regularly using an Internet auction site to buy and sell antique jewelry.

MSBs Can Help Fight Money Laundering

What is a transaction that “Involves Use of the MSB to Facilitate Criminal Activity?”

Example. An MSB suspects that a customer is sending a money transfer in order to fund a terrorist organization.

It is important to note that size alone, such as a large cash transaction or money transfer, should not be a determining factor in the decision to file a SAR. Factors that should contribute to that decision, however, include the following: the size, frequency and nature of the transactions; the MSB’s experience with the customer and other individuals or entities associated with the transaction (if any); and the norm for such transactions within the MSB’s line of business and geographic area.

Red Flags

When a single factor signals that a

transaction is unusual and possibly “suspicious,” it is called a “red flag.”

Examples of Some Common Red Flags:

Customer ID or Information

- Customer uses false ID.
- Two/more customers use similar IDs.
- Customer alters transaction upon learning that he/she must show ID.
- Customer alters spelling or order of his/her full name.

Transactions Below Reporting or Recordkeeping Thresholds

Customer conducts transactions just below relevant thresholds:

- Currency exchanges just under \$1,000.
- Cash sales of money orders or traveler’s checks of just under \$3,000.

MSBs Can Help Fight Money Laundering

Multiple Persons or Locations

- Two or more customers working together to break one transaction into two or more transactions in order to evade the BSA reporting or recordkeeping requirement.
- Customer uses two or more locations or cashiers in the same day in order to break one transaction into smaller transactions and evade the BSA reporting or recordkeeping requirement.

Overt Illegal Customer Conduct

- Customer offers bribes or tips.
- Customer admits to criminal conduct.

An MSB that correctly verifies and documents a customer's identity is more likely to recognize suspicious activity that should be reported.

What Should MSBs Look For?

Money laundering schemes can vary widely. Federal action to curtail money laundering activities once focused heavily on identification and documentation of large currency transactions. More recently, anti-money laundering efforts have focused on the use of money transfers, both through bank and non-bank money transfer systems, and other means of moving funds. Today, as money launderers become more sophisticated, all types of financial transactions are facing greater scrutiny.

The following situations may indicate money laundering or other illegal activity. These lists are not comprehensive, but they may help MSBs recognize ways launderers and other criminals may try to use them to launder money.

Attempts to Evade BSA Reporting or Recordkeeping Requirements

Customers may try to keep their transactions

MSBs Can Help Fight Money Laundering

What Should MSBs Look For? (Cont.)

just below the reporting or recordkeeping thresholds, such as:

- A customer or group of customers who attempt to hide the size of a large cash transaction by breaking it into multiple, smaller transactions by, for example, conducting the smaller transactions—
 - At different times on the same day.
 - With different MSB cashiers on the same day or different days.
 - At different branches of the same MSB on the same or different days.
- A customer or group of customers who conduct several similar transactions over several days, staying just under reporting or recordkeeping limits each time. For example, the customer may:
 - Purchase money orders with cash just under \$3,000 over several days.
 - Purchase traveler’s checks with cash just under \$3,000 over several days.
 - Initiate multiple money transfers to the same receiver, each transfer in an amount under \$3,000, over several days.
- A customer who is reluctant to provide information needed for a reporting or recordkeeping requirement, whether required by law or by company policy.
- A customer who is reluctant to proceed with a transaction after being informed that a report must be filed or a record made.

MSBs Can Help Fight Money Laundering

- A customer who breaks down a single large transaction into smaller transactions after being informed that a report must be filed or a record made.
 - A customer who presents different identification each time a transaction is conducted.
 - A customer who spells his/her name differently or uses a different name each time he/she initiates or receives a money transfer or purchases traveler's checks.
 - Any individual or group that bribes or attempts to bribe an MSB employee not to file any required reporting forms or not to create a record entry required by law or company policy.
 - Any individual or group that forces or attempts to force an MSB employee not to file any required reporting forms or create a record required by law or company policy.
- A customer who receives payment of multiple money transfers that appear to have been purchased in a "structured" manner – organized in a way to evade reporting and recordkeeping requirements.
 - By the same send customer, each transfer in an amount just under \$3,000 (or other relevant threshold).
 - By multiple send customers initiated at one MSB location within minutes of each other, each transfer in an amount just under \$3,000 (or other relevant threshold).
 - A customer cashing multiple instruments (money orders, traveler's checks, cashiers' checks, foreign drafts) that appear to have been purchased in a structured manner (e.g. each in an amount below \$3,000).

MSBs Can Help Fight Money Laundering

What Should MSBs Look For? (Cont.)

Customers Who Provide Insufficient and/or Suspicious Information

Individual and business customers may try to evade providing required identification, such as:

- An individual customer who is unwilling or unable to provide identification or information.
- An individual customer who provides different identification or information each time he or she conducts a transaction.
 - Different name or different spelling of name.
 - Different address or different spelling or numeration in address.
 - Different identification types.
- An individual customer without a local-address, who appears to reside locally because he or she is a repeat customer.
- A legitimate ID that appears to have been altered.
- An identification document in which the description of the individual does not match the customer's appearance (e.g. different age, height, eye color, sex).
- An expired identification document.
- An individual customer who presents any unusual or suspicious identification document or information.
- A business customer that is reluctant to provide complete information regarding: the type of business, the purpose of the transaction, or any other information requested by the MSB.
- A prospective business customer that refuses to provide information to qualify for a business discount (or other preferred customer program offered by the MSB).

MSBs Can Help Fight Money Laundering

Activity Not Consistent With the Customer's Business or Occupation

Look for examples of inconsistent customer activity, such as:

- An individual customer conducts MSB transactions in large amounts inconsistent with the income generated by the individual's stated occupation.
 - A business customer engages in transactions that frequently use large bills when the nature of the customer's business activity does not justify such use.
 - An individual or business customer cashes large numbers of third party checks.
- A customer makes cash purchases of money orders, traveler's checks, or other instruments inconsistent with the customer's business or occupation.
 - A business customer uses a means of payment inconsistent with general business practices (e.g., pays for MSB services with traveler's checks, money orders, or third party checks).
 - A business customer sends or receives money transfers to/from persons in other countries without an apparent business reason or gives a reason inconsistent with the customer's business.
 - A business customer sends or receives money transfers to or from persons in other countries when the nature of the business would not normally involve international transfers.

MSBs Can Help Fight Money Laundering

What Should MSBs Look For? (Cont.)

Unusual Characteristics or Activities

Notice any unusual characteristics, such as:

- An individual customer purchases products/services on a regular basis but seems neither to reside nor work in the MSB's service area.
- A customer pays for MSB products/services using musty bills that have an unusual or chemical-like odor.
- A customer pays for MSB products/services using money orders or traveler's checks without relevant entries on the face of the instrument. (e.g., for money orders – *no payee, and for traveler's checks – no signature or countersignature*).
- A customer pays for MSB products/ services using money orders or traveler's checks with unusual symbols, stamps or written annotations (such as initials) that appear either on the face or on the back of the instruments.
- A customer purchases money transfers, money orders, traveler's checks, etc., with large amounts of cash when the MSB does not require payment in cash.
- An individual or business customer asks to purchase traveler's checks or money orders in large bulk orders.
- A customer purchases a number of money transfers, money orders, or traveler's checks for large amounts or just under a specified threshold without apparent reason.
- A customer starts frequently exchanging small bills for large bills, or vice versa, when the customer does not normally use cash as a means of payment.

MSBs Can Help Fight Money Laundering

- A customer sends and receives money transfers in equal amounts at or about the same time.
- A customer receives a number of small money transfers and the same day, or within several days, initiates one or more send money transfers to a person in another city or country in about the same amount.
- A customer sends or receives frequent or large volumes of money transfers to or from persons located in foreign countries, especially countries listed as non-cooperative jurisdictions.
- A customer receives money transfers and immediately purchases monetary instruments prepared for payment to a third party.

Changes in Transactions or Patterns of Transactions

Be alert for changes in activity, such as:

- Major changes in customer behavior, for example:
 - An individual money order customer begins to make weekly purchases of money orders in the same amounts (when previously he or she only purchased money orders on pay day for rent, utilities, etc.).
 - An individual customer begins to bring in large amounts of cash (when previously he or she cashed his or her paycheck to purchase instruments or transfers).
- Sudden and inconsistent changes in money transfer send or receive transactions.

MSBs Can Help Fight Money Laundering

What Should MSBs Look For? (Cont.)

- Rapid increase in size and frequency of cash used by a particular customer.

Employees

Watch out for employee behavior, such as:

- An MSB employee whose lifestyle cannot be supported by his/her salary, which may indicate receipt of tips or bribes.
- An employee who is reluctant to take a vacation, which may indicate he/she has agreed, or is being forced, to provide services to one or more customers in violation of law or company policy.
- An employee who is associated with unusually large numbers of transactions or transactions in unusually large amounts, which may indicate he/she has agreed, or is being forced, to provide

services to one or more customers in violation of law or company policy.

Situations like those described in this section often will be found, upon further examination, to be completely legitimate. By the same token, other situations not mentioned here might be suspicious if they are inconsistent with the normal activity of a particular customer or employee. As an MSB or MSB employee, you must make a reasonable judgement.

MSBs Can Help In Other Ways

MSBs must comply with other BSA reporting and recordkeeping regulations. The following outlines certain of these requirements.

File Currency Transaction Reports (CTRs)

An MSB must file a report of each currency transaction involving cash-in or cash-out of more than \$10,000 conducted by, through, or to the MSB on any one day by or on behalf of the same person.²

Therefore, a CTR is required when a transaction meets all of the following conditions:

- In currency,
- Greater than \$10,000 in either cash-in or cash-out,
- By, or on behalf of, the same person, and
- Occurs on one business day.

² See 31CFR103.22

Aggregation

Multiple transactions conducted by or on behalf of the same person on the same day are considered to be one transaction for CTR purposes. In other words, the MSB must file a CTR if it knows the customer's aggregate cash-in or cash-out transactions total more than \$10,000 in one day.

Cash-in and Cash-out

Cash-in transactions must be added together with cash-in transactions and cash-out transactions must be added together with cash-out transactions to determine whether the CTR threshold (greater than \$10,000) has been met in any one business day.

CTR Filing

The CTR is IRS Form 4789, Currency Transaction Report, and is available on www.msb.gov or by calling the IRS Forms

MSBs Can Help In Other Ways

File Currency Transaction Reports (CTRs) (Cont.)

Distribution Center at 1-800-829-3676.
The form must be filed within 15 days from the date of the transaction(s).

The CTR requirement requires an MSB to:

- Verify and record customer ID,
- Obtain transaction information,
- Complete and file the CTR,
- Retain a copy of the CTR for five years from the date of filing the report.

Keep Records

Monetary Instrument "Log" – for Cash Purchases of Money Orders, Travelers Checks, Other Instruments

An MSB that sells money orders, traveler's

checks, or other instruments for cash must verify the identity of the customer and create and maintain a record of each purchase when the purchase involves cash between \$3,000 and \$10,000, inclusive.³ Thus, a record is required when:

- Cash-in of \$3,000-\$10,000, inclusive, and
- Cash-in is for the purchase of money orders, traveler's checks, or other monetary instruments.

The Monetary Instrument "Log" requirement requires an MSB to:

- Verify and record customer ID,
- Record transaction information (for each money order, traveler's check, or other instrument purchased: amount, serial number, and date sold),
- Retain the record for five years from the date of the transaction.

³ See 31CFR103.29

MSBs Can Help In Other Ways

Funds Transfer Rules For Senders of Money Transfers

An MSB that accepts an instruction to send a money transfer of \$3,000 or more must verify the identity of the send customer and create and maintain a record of the money transfer, regardless of the method of payment.⁴

In addition, certain information must "travel," that is, the MSB must send on certain information, to the next MSB or financial institution processing the transfer.

For Receivers of Money Transfers

An MSB that accepts an instruction to pay a money transfer of \$3,000 or more must verify the identity of the receiving customer and create and maintain a record of the money transfer, regardless of the method of payment.

The requirement to record funds transfers requires a money transmitter to:

- Verify customer ID,
- Record customer information,
- Record transaction information,
- Send information to receiving MSB,
- Retain the record for five years from the date of the transaction.

Currency Exchange Record

Each currency exchanger must create and maintain a record of each exchange of currency in excess of \$1,000.⁵ The currency exchange may be either domestic or foreign currency, or it may be both. Thus, a currency exchange record is required when:

- Currency-in greater than \$1,000, or
- Currency-out greater than \$1,000.

⁴ See 31CFR103.33(f)

⁵ See CFR103.37

MSBs Can Help In Other Ways

Keep Records (Cont.)

Example. A customer wishes to exchange \$3,000 in Canadian dollars for its equivalent in U.S. dollars, or a customer wishes to exchange \$1,500 in \$20 bills for \$1,500 in \$100 bills.

In each case, the transaction must be recorded.

The requirement to record currency exchanges includes the following – the currency exchanger must:

- Record customer ID and information,
- Record transaction information,
- Retain the record for five years from the date of the transaction.

Reports That Can Help MSBs Identify Suspicious Transactions

The following list of reports can be used to look for possible money laundering activity in MSBs.

Cash-In and Cash-Out of Large Transaction Reports

Many MSBs prepare, or have systems that generate, reports of cash-in and cash-out. Often these reports include transactions that exceed a certain threshold. Many money transmitters, for example, have established identification requirements at levels below the \$3,000 threshold. Such reports can help identify customers who may be structuring transactions to evade BSA reporting and recordkeeping requirements or who are engaging in other unusual activity.

Kiting Reports

Issuers of traveler's checks and money orders and money transfer companies often prepare, or have systems that generate, reports that identify transactions that may involve kiting. Kiting is depositing and drawing checks between accounts at two or more banks and thereby taking advantage of the float – that is, the time it takes the bank of deposit to collect from the paying bank. Reports that indicate kiting may also disclose other unusual patterns of activity possibly associated with money laundering.

Money Transfer Reports

Money transfer companies prepare, or have systems that generate, daily transaction reports and other reports that identify different groupings of transfer activity processed through their systems (e.g., corridor reports showing all transfers from

Reports That Can Help MSBs Identify Suspicious Transactions

Money Transfer Reports (Cont.)

country A to country B in a specific time period). These reports can help identify unusual patterns that may suggest possible money laundering.

Depending on the type of report and the frequency, these reports can help identify unusual customer behavior. Such reports also may help identify unusual behavior of businesses serving as agents of money transfer companies.

\$3,000 Instrument "Log"

Reports of cash sales of instruments between \$3,000 - \$10,000, inclusive, required by BSA regulations, can help MSBs identify possible currency structuring patterns. Recorded information can, for example, help identify customers who may be structuring transactions to evade the BSA reporting and recordkeeping requirements.

Clearance Records/Receipts

Issuers of money orders and traveler's checks prepare, or have systems that generate, daily records of items that have been presented for payment against the issuer's bank account. Many issuers have designed programs to identify unusual patterns of cleared instruments. Such reports can be extremely useful in the identification of items that may have been used for illicit purposes.

\$3,000 Funds Transfer Records

These records, required by BSA regulations, can help money transmitters identify possible structuring patterns. Records of \$3,000 or more in money transfers regardless of the method of payment may help identify customers who could be structuring transactions to evade BSA reporting and recordkeeping requirements.

Reports That Can Help MSBs Identify Suspicious Transactions

Customer Activity Reports

Some MSBs use customer reward programs to encourage repeat use by customers. Reports generated to monitor individual customer responses or general customer activity can be useful in identifying unusual transactions or patterns of transactions.

Some Money Laundering Schemes

The following descriptions are intended to help MSBs identify activities that criminals use to launder money. They are also intended to reinforce the need for strict customer identification programs. Finally, although these examples are of landmark investigations that primarily involve banks, they provide lessons to be learned by MSBs as well.

Operation Polar Cap

Two banks reported suspicious activities related to changes in operations by customers. Those two reports and an analysis of CTRs by the U.S. Customs Service helped bring together a national investigation.

At one bank, an employee noticed that a customer, a jewelry broker, was making large cash deposits (\$25 million over three months) that did not seem commensurate with his usual business. In addition to filing

the CTRs required for cash transactions by this customer of more than \$10,000 in a business day, one bank also notified the IRS Criminal Investigation Division (IRS-CID).

At the other bank, an observant employee became suspicious when a customer, who ran a grocery store and check cashing service, stopped taking cash back for the checks he deposited in the bank. This change led the banker to notify law enforcement authorities.

Together, these two suspicious banks helped uncover and disrupt an operation that had laundered about \$1.2 billion over two years. More than 127 people were arrested, a foreign bank was indicted, and one ton of cocaine was seized. Numerous convictions resulted.

Some Money Laundering Schemes

Operation C-Chase

A Luxembourg-based bank, two of its subsidiaries, nine bank officials, and 75 other individuals in several countries were indicted for possible involvement in a worldwide money laundering scheme. Convictions were obtained in a significant number of cases. The operation relied on the launderers' associates picking up cash from drug activities in cities around the

United States and, either through funds transfers or by physically transporting the cash, depositing it into undercover accounts in a U.S. bank.

The associates signed blank checks drawn on the undercover accounts, and after a cash pickup occurred, the head of the laundering operation would enter the amount onto one of the blank checks and forward it to the owner of the funds or sell it on the currency black market.

As the operation expanded, the head of the operation developed several variants on that process. Some funds from the undercover accounts were wired to similar accounts in a Central American bank to further disguise their origin. Others were transferred through another U.S. bank to a foreign bank.

In both instances, the funds transferred to the foreign bank were placed in 90-day certificates of deposit and used as collateral on loans made by the Central American bank to its associates. The loan proceeds were then deposited in undercover accounts in the bank and forwarded through the chain as before.

At a later date, funds wired through two foreign banks were used to purchase certificates of deposit at a second foreign bank. The certificates were then used as collateral on loans made at a third foreign bank, the proceeds of which were wired

Some Money Laundering Schemes

Operation C-Chase (Cont.)

back to the undercover accounts at the U.S. banks, and transferred from there to the owner's account in South America. The organizers of this ring were careful to warn participants that transactions should be handled in varying combinations to avoid developing a pattern. They used many legitimate businesses, such as hotels and restaurants, to originate funds transfers to the undercover accounts. Together, the network was able to absorb about \$10 million per month in drug proceeds.

Bank of Credit and Commerce International (BCCI)

Established in the 1970s, the Bank of Credit and Commerce International emerged in the 1980s as one of the world's largest privately owned financial institutions, with operations in over 70 countries. During the

years of its operations, BCCI employees were found to have engaged in a number of illicit activities, including money laundering. BCCI was financially distressed in the 1970s because of troubled shipping loans, but through an intricate shell game, it shuttled assets and liabilities among its subsidiaries, giving the appearance of being a well-capitalized financial institution.

Investigations resulted in the 1991 seizure of BCCI's operations by regulators in seven countries. BCCI points out a number of important issues for financial institutions: financial institutions should be careful about knowing other institutions with which they do business. They should carefully screen potential major owners or shareholders, pay attention to the quality and extent of supervision that foreign institutions receive in their home countries, and be aware that asset

Some Money Laundering Schemes

forfeiture laws put institutions at risk of having assets, including bank accounts and outstanding instruments and money transfers, frozen or seized.

Operation Green Ice

Law enforcement agencies in eight nations cooperated in a sting operation which resulted in the arrest of 167 people and the seizure of \$54 million in cash and other assets. Operation Green Ice led to the arrest of several high-ranking financial officers of cocaine cartels, and ultimately their conviction. Accounts at banks around the world were frozen after receiving transfers and cash deposits of laundered funds. In the United States, bank accounts were frozen and seized in San Diego, Los Angeles, Chicago, Houston, Miami and New York.

The U.S. banks that received the cash deposits in this case cooperated with agents of the Drug Enforcement Agency and continued to file detailed CTRs, which provided further evidence. Intermediary banks had less access to information and were more at risk of unwittingly being used as part of the money laundering chain.

This case points out the need for institutions to be aware of such risks and to protect themselves by noting frequent transfers of substantial sums sent to persons or accounts in drug source countries.

Legislation

Over the years, Congress has passed many laws to combat money laundering. Perhaps the most significant of these are the Bank Secrecy Act of 1970, the Money Laundering Control Act of 1986, the Anti-Drug Abuse Act of 1988, the Annunzio-Wylie Act of 1992, the Money Laundering Suppression Act of 1994, the Money Laundering and Financial Crimes Strategy Act of 1998 and the USA PATRIOT Act of 2001.

The **Bank Secrecy Act of 1970 (P.L. 91-508)** was designed to:

- Prevent tax evasion and provide tools to fight organized crime.
- Create an investigative "paper trail" for large currency transactions by establishing reporting standards and requirements (e.g. the Currency Transaction Report requirement).

- Verify the identity of customers and keep certain basic records of customer transactions, including cancelled checks and debits, signature cards, and statements of account.
- Impose civil and criminal penalties for noncompliance with its reporting requirements.
- Improve detection and investigation of criminal, tax, and regulatory violations.

The **Money Laundering Control Act of 1986 (P.L. 99-570)**, part of the Anti-Drug Abuse Act of 1986, made money laundering a federal crime. It created three new criminal offenses for money laundering activities by, through, or to a financial institution. These offenses are:

- Knowingly helping launder money derived from criminal activity.

Legislation

- Knowingly (including being willfully blind) engaging in a transaction of more than \$10,000 that involves property or funds derived from criminal activity.
- Structuring transactions to evade BSA reporting requirements.

The **Anti-Drug Abuse Act of 1988 (P.L. 100-690)** reinforced anti-money laundering efforts in several ways. The Act:

- Significantly increases in civil and criminal penalties for money laundering and other BSA violations, including forfeiture of any property, real or personal, involved in a transaction or attempted transaction in violation of laws relating to the filing of Currency Transaction Reports, money laundering or structuring transactions.
- Requires strict identification and recording of cash purchases of certain

monetary instruments, including money orders and traveler's checks between \$3,000 and \$10,000, inclusive.

- Permits the Department of the Treasury to require certain financial institutions in specific geographic or "target" areas to file additional BSA reports of currency transactions in amounts less than \$10,000 by use of "Geographic Targeting Orders."
- Directs the Department of the Treasury to negotiate bilateral international agreements covering the recording of large U.S. currency transactions and the sharing of such information.
- Increased the criminal sanction for tax evasion when money from criminal activity is involved.

Legislation

The **Annunzio-Wylie Anti-Money Laundering Act of 1992 (P.L. 102-550)**

strengthened penalties for financial institutions found guilty of money laundering. Annunzio-Wylie required the Secretary of the Treasury to:

- Adopt a rule requiring all financial institutions, both banks and non-banks (including MSBs), to maintain records of domestic and international funds transfers, which can be used in law enforcement investigations.
- Establish a BSA Advisory Group (BSAAG), comprised of representatives from the Department of the Treasury and Department of Justice, Office of National Drug Control Policy and other interested persons and financial institutions, including MSBs. The BSAAG, established in 1994, meets twice per year and informs representatives of

the financial services industry about new regulatory developments and how reported information is used.

Annunzio-Wylie also permitted the Secretary of the Treasury to:

- Require any financial institution, or any financial institution employee, to report suspicious transactions relevant to any possible violation of law or regulation.
- Require any financial institution to adopt an anti- money laundering program.

In addition, Annunzio-Wylie:

- Makes it illegal for a financial institution, or an employee of a financial institution, to disclose to anyone involved in a suspicious transaction when a Suspicious Activity Report (SAR) has been filed.

Legislation

- Protects any financial institution, and any director, officer, employee, or agent of a financial institution, from civil liability for reporting suspicious activity.
- Makes it a federal crime to operate an illegal money transmitting business (i.e. operating a money transmitting business without a state license in a state where such license is required under state law.)

The **Money Laundering Suppression Act (MLSA) of 1994 (P.L. 103-325)**

specifically addressed MSBs. The MLSA:

- Requires each MSB to be registered by an owner or controlling person of the MSB.
- Requires every MSB to maintain a list of businesses authorized to act as agents in connection with the financial services offered by the MSB.
- Makes operating an unregistered MSB a federal crime.

- Recommended that states adopt uniform laws applicable to MSBs.

The **Money Laundering and Financial Crimes Strategy Act of 1998 (P.L. 105-310)**

requires:

- The President, acting through the Secretary of the Treasury and in coordination with the Attorney General, to develop a national strategy for combating money laundering and related financial crimes and to submit such strategy each February 1st to Congress.
- The Secretary of the Treasury, upon consultation with the Attorney General, to designate certain areas—by geographical area, industry, sector or institution—as being vulnerable to money laundering and related financial crimes. (Certain areas were subsequently designated as High Intensity Financial Crime Areas (HIFCAs).

Legislation

The **USA PATRIOT Act of 2001 (P.L. 107-56)**, which is the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, requires:

- Establishment of anti-money laundering compliance programs by all financial institutions. At minimum each program must include: policies procedures and controls; designation of a compliance officer; training; and an independent audit function.
 - Establishment of a confidential communication system between government and the financial services industry.
 - Implementation of customer identification procedures for new accounts.
 - Enhanced due diligence for correspondent and private banking accounts maintained for non-U.S. persons.
- Establishment of a highly secure network by FinCEN for electronic filing of BSA reports.

International Money Laundering Efforts

The United States is not alone in the fight against financial crimes. Many countries have enacted significant anti-money laundering legislation. A number of international organizations and regional groups have adopted anti-money laundering rules and regulations as well.

Basel Committee

The Basel Committee consists of representatives of central banks and supervisory authorities of Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, the Netherlands, Spain, Sweden, Switzerland, the United Kingdom and the USA. In 1988 the Basel Committee published a "Statement of Principles" on money laundering, which generally recommended obtaining proper identification from customers and complying with laws and regulations governing financial transactions.

United Nations (UN)

The UN Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances (the Vienna Convention) calls on signatories to criminalize money laundering, to assure that bank secrecy is not a barrier to criminal investigations, and to promote removal of legislative barriers to investigation, prosecution, and international cooperation.

Financial Action Task Force (FATF)

FATF was created at the Economic Summit of the major industrialized countries in 1989. It issued a report in which it made 40 recommendations, consistent with the Vienna Convention, for implementing and coordinating money laundering laws in member countries. They also formed the basis of money laundering rules and regulations established by the Caribbean Financial Action Task Force and the Organization of America States.

International Money Laundering Efforts

Financial Action Task Force (FATF) (Cont.)

Another report FATF has issued on non-cooperative countries and territories identifies countries with detrimental rules and practices that obstruct international cooperation in the fight against money laundering.

European Union (EU)

In 1991, the EU issued a directive on money laundering, compatible with the original 40 FATF recommendations. It requires mandatory reporting of suspicious transactions and identification of beneficial owners and customers of financial transactions and accounts.

Country Advisories and Economic and Trade Sanction Lists

FinCEN Advisories

FinCEN has issued country advisories urging enhanced scrutiny of financial transactions with countries that had deficient anti-money laundering controls. Advisories can be viewed at: www.fincen.gov under [Publications/Advisories](#).

Office of Foreign Assets Control (OFAC) List

The U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC) issues the Specially Designated Nationals and Blocked Entities List (SDN List). OFAC regulations require businesses to identify and freeze the assets of targeted countries, terrorists, drug cartels and other specially designated persons. For these lists and specific instructions regarding what businesses may or may not do under OFAC regulations, refer to the OFAC website at: www.ustreas.gov/ofac.

Glossary

Agent

A business that an issuer authorizes, through written agreement or otherwise, to sell its instruments or, in the case of funds transmission, to sell its send and receive transfer services.

Aggregation

Adding together multiple transactions that an MSB knows have been conducted by or on behalf of the same person on the same day, for BSA reporting and recordkeeping purposes. For example, the MSB must file a CTR if it knows a customer's aggregate cash-in or cash-out transactions during one day totals more than \$10,000.

Branch

An owned location of either an issuer or agent at which financial services are sold.

Issuer

The business ultimately responsible for payment of money orders or traveler's checks as the drawer of such instruments, or a money transmitter that has the obligation to guarantee payment of a money transfer.

Money Laundering

A process by which criminals seek to disguise the true source of their illegally obtained funds or proceeds of crime. It involves three different, and sometimes overlapping, stages:

Placement – Physically placing criminal proceeds into the financial system.

Layering – Separating the proceeds of criminal activity from their origins through layers of financial transactions.

Integration – Moving the proceeds of crime into a "final" form that provides an apparently legitimate explanation for the illegally obtained funds.

Glossary

Money Services Business (MSB)

Any person doing business, whether or not on a regular basis or as an organized business concern, providing one or more of the following services:

- money orders
- traveler's checks
- check cashing
- currency dealing or exchange
- stored value

-AND-

- Conducts more than \$1,000 in money services business activity
 - with one person
 - in one or more transactions (in one type of activity)
 - on any one day.

OR

- Provides money transfers in any amount.

Money Transmitter

A person that engages as a business in the transfer of funds through a financial institution is a money transmitter and an MSB, regardless of the amount of transfer activity. Generally, the acceptance and transmission of funds as an integral part of a transaction other than the funds transmission itself (for example, in connection with a sale of securities or other property), will not cause a person to be a money transmitter.

Redeemer

A business that accepts instruments in exchange for currency or other instruments for which it is not the issuer is a redeemer. For example, a hotel that provides a customer with \$1,500 in cash in exchange for the customer's \$1,500 money order (issued by another MSB) is a redeemer. The MSB definition in 31 CFR 103.11(u)(4) extends to "redeemers" of money orders and

Glossary

Redeemer (Cont.)

traveler's checks only insofar as the instruments involved are redeemed for monetary value – that is, for currency or monetary or other negotiable or other instruments. The taking of the instruments in exchange for goods or general services is not redemption under BSA regulations.

Structuring

A term used in reference to any conduct engaged in to evade a reporting or recordkeeping threshold and the corresponding BSA reporting or recordkeeping requirement (e.g. \$1,000 for currency exchange and \$3,000 for funds transfer records or more than \$10,000 in currency for filing CTRs). Structuring is a federal crime.

Examples of Structuring

1. One person breaks a large transaction into two or more smaller transactions –

A customer wishes to conduct a \$10,500 cash transaction on one day. However, knowing that the threshold for filing a CTR (more than \$10,000 cash transaction) would be met, he conducts two \$5,250 cash transactions, thereby trying to evade the CTR reporting requirement/threshold.

2. A large transaction is broken into two or more smaller transactions conducted by two or more persons –

A customer wishes to send \$10,000 to a friend in London. The customer and three others each purchase a \$2,500 money transfer to London, thereby evading the Funds Transfer Rule recordkeeping requirement/threshold of \$3,000.

Request More Information

BSA Forms

To Download:

FinCEN website at: www.fincen.gov

MSB website at: www.msb.gov

IRS website at: www.irs.gov

To Order:

IRS Forms Distribution Center at:

1-800-829-3676

Free MSB Information and Guidance Materials

To Order:

MSB Web site at: www.msb.gov

Money Services Business Outreach Office at:

1-800-386-6329

Answers to Questions about Filing BSA Forms

IRS-Detroit Computing Center

Hotline

1-800-800-2877

Interpretation of BSA Regulations

Financial Crimes

Enforcement Network

Regulatory Helpline

1-800-949-2732

Report Terrorist Related Financial Activity

Financial Institutions Hotline

1-866-556-3974



The Campaign **AGAINST**
Financial Crimes

Financial Crimes Enforcement Network
U.S. Department of the Treasury
Washington, DC

*A publication of the Financial Crimes Enforcement Network (FinCEN)
U.S. Department of the Treasury*