Why am I Responsible for Compliance in my Business?

Because you sell money orders and/or money transfers, you are subject to the compliance requirements of various anti-money laundering and anti-fraud laws and other compliance related regulations such as the:

- **Bank Secrecy Act (BSA)**
- **USA PATRIOT Act**
- **Dodd–Frank Wall Street Reform and Consumer Protection Act**
- **Gramm–Leach–Bliley Act**
- **Office of Foreign Assets Control (OFAC)** and other sanctions lists

Bank Secrecy Act (BSA)

Requires U.S. financial institutions to assist U.S. government agencies to detect and prevent money laundering. Specifically, the act requires financial institutions to keep records of cash purchases of negotiable instruments, file reports of cash transactions exceeding $10,000 (daily aggregate amount), and to report suspicious activity that might signify money laundering, tax evasion, or other criminal activities. It was passed by the Congress of the United States in 1970.

USA PATRIOT Act

Title III of the USA PATRIOT Act is intended to facilitate the prevention, detection and prosecution of international money laundering and the financing of terrorism. The title's sections primarily amend portions of the Money Laundering Control Act of 1986 and the Bank Secrecy Act of 1970.

The provisions of Title III are divided into three subtitles. The first deals primarily with strengthening banking rules specifically against money laundering, especially on the international stage. Communication between law enforcement agencies and financial institutions, as well as among institutions, is expanded by the second subtitle, which also increases record keeping and reporting requirements. The final portion of the title deals with currency smuggling and counterfeiting, including quadrupling the maximum penalty for counterfeiting foreign currency.

Dodd–Frank Wall Street Reform and Consumer Protection Act

This act required the Consumer Financial Protection Bureau to issue new rules to protect consumers who send money electronically to foreign countries. All money transmitters, as well as any banks, thrifts or credit unions offering international remittance transfers in the normal course of business must comply with the new rules. The rules impact all remittance transfers that are made by a consumer in the United States, and sent to a foreign country. The act was signed into law on July 21, 2010

You have specific, required responsibilities as a MoneyGram Agent under this act. Please regularly review these requirements in Section 10 - Dodd-Frank of this resource binder.

Gramm–Leach–Bliley Act

This act prompted the Federal Trade Commission (FTC) to issue a final Safeguards Rule to establish standards relating to administrative, technical and physical information safeguards for financial institutions to ensure the security and confidentiality of consumer records and information, protect against any anticipated threats or hazards to the security or integrity of such records, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any consumer.

Your additional responsibilities as a MoneyGram Agent under this act are detailed further on ***Page 18*** of this resource guide.

Your Compliance Program must align with the requirements of these and other government regulations as outlined in this Compliance Resource.

Office of Foreign Assets Control (OFAC)

OFAC is part of the U.S. Department of the Treasury and is responsible for enforcing U.S. government sanctions programs against countries, organizations and individuals. Sanctions programs typically involve blocking assets to further national security. Many of the sanctioned individuals, commonly referred to as Specially Designated Nationals (SDNs), are known or suspected drug dealers and terrorists. All U.S. entities are prohibited from conducting any financial transactions with SDNs even if transactions with the SDN originate or terminate outside of the United States.

As a U.S. company, MoneyGram must comply with the U.S. sanctions regarding Cuba. MoneyGram and its agents cannot process any transactions where a sender or receiver is a Cuban National. All such issues MUST be referred to MoneyGram's AML Compliance Department by calling **1-800-444-3010**.

You can learn more about OFAC by visiting the Treasury Department's website at:

www.ustreas.gov/offices/enforcement/ofac.

The site also includes an extensive list of questions and answers to common questions regarding OFAC.

Code 4 Message Potential

MoneyGram reviews *all* money transfer sender and receiver names against *multiple* sanctions lists, including the OFAC SDN list, *regardless* of the dollar amount of the transaction. If a name is a potential match to any monitored sanctions list, agents must follow MoneyGram's instructions in order to prevent any unauthorized payout or refund.

If you receive a **Code 4** message on an attempted transaction, the following steps should be followed:

1. You will be instructed to contact MoneyGram at **1-800-444-3010** and select **Option 2** BEFORE completing single or multiple transactions
2. You must contact MoneyGram *before* refusing OR completing the transaction.
3. The MoneyGram representative will request additional information to validate whether the consumer's name is a true match to the sanctions list.

Your cooperation is critical!

Transactions CANNOT be paid out or refunded until MoneyGram has reviewed and released possible OFAC SDN matches.

Civil and Criminal Penalties

The government can impose harsh civil and criminal penalties against anyone who violates the BSA, USA PATRIOT Act, OFAC, Dodd Frank or other anti-money laundering and anti-fraud laws and regulations. Civil and criminal fines can quickly reach into the hundreds of thousands or even millions of dollars. The criminal penalty for violating a BSA requirement is a fine of up to $500,000, a jail term of up to 10 years, or both. In addition, the government can seize any property involved in criminal violations of these laws. This includes your business, your bank account or any other assets the government can link to criminal violations.

Under certain circumstances, businesses can be held criminally liable for the acts of their employees; it is important for your employees to be trained in these matters and for your business to have a system in place to ensure employees' compliance with the laws and regulations. If you or your employees do not comply, you may be subject to large fines and/or imprisonment.

The government requires strict compliance with these laws and regulations.

MoneyGram will immediately cancel the contract of any agent who knowingly or negligently fails to comply with the laws and regulations.

Non-compliance just isn't worth the risk.

What is Money Laundering?

Money laundering is the attempt to hide or disguise the nature, location, source, ownership or control of illegally obtained money.

This definition covers a wide range of activity and is not limited to cash or currency transactions. Money laundering can involve any type of money, including money orders, money transfers and other financial transactions. You need to understand how people launder money so that you can identify and report money laundering and also know how to help prevent it from happening.

The money laundering cycle begins when criminals place money into the financial system by, for example, buying money orders or sending money transfers. Once the money has entered the financial systems, the source of illegal funds is further disguised by transferring them through layers of financial institutions, such as bank or investment accounts. Finally, the money enters the everyday economy and appear to be legitimate by purchasing items or investing in legitimate investments such as real estate, real property, stocks and bonds or by buy addition money orders or sending additional money transfers.

Terrorist Activity and Money Laundering

Money laundering is most commonly associated with drug dealing and tax evasion, however, ***terrorists*** often attempt to launder money in order to hide their identity and finance their illegal operations. It is critical that anyone processing money related transactions, like those for MoneyGram, should remain alert for any such activity, and take appropriate and immediate action if detected.

The **Financial Action Task Force (FATF)** and the U.S. Treasury's **Financial Crime Enforcement Network (FinCEN)** have both issued guidance on financial transactions that may be indicative of terrorist financing at www.fatf-gafi.org and www.fincen.gov.

Some examples include, *but are not limited to:*

- Movement of funds through a country designated by FinCEN or the FATF as "non-cooperative," that are identified as specially designated nationals by OFAC, or that appear on the United Nation's list of blocked accounts
- Multiple transactions conducted by group of nationals from countries associated with terrorist activity
- Individuals acting on behalf of another money transmitting business that use MoneyGram to transfer funds to multiple locations. This may actually be unlicensed money transmitters wanting to avoid using the banking system to conduct foreign money transfers

If you suspect terrorism financing, you should immediately report the incident to the FinCEN hotline at 1-800-556-3974, which is operated 24 hours a day, seven (7) days a week. You should also E-File a **Suspicious Activity Report (SAR-please see below)** on any suspected terrorism activity.

To help prevent the laundering of cash and to help obtain documentation that could be used to prosecute money launderers, the government requires you to save and store records on certain cash transactions. Some transactions also require that reports be electronically filed and stored. Please see Section 1 Page 14-16 and Sections 7 and 8 in this resource binder for additional information on E-Filing these types of reports.

What is Fraud?

Fraud is the potential or actual theft of information and funds from both you as an Agent and from consumers by means of *deceit, trickery, counterfeit, manipulation*, or other *illicit* means.

Be Aware!!!

There are three critical areas of fraud that MoneyGram agents should recognize and assist in preventing by monitoring day-to-day transactions:

- **Agent Fraud**
- **Counterfeit Fraud**
- **Consumer Fraud**

Agent Fraud

Agents and their employees are often targeted by individuals attempting to steal agent or consumer information that can be used to commit fraud. These attempts usually fall under one of the following categories, but are not limited to: ***Computer Crimes or Social Engineering (Phishing).*** *Please see the* ***Fraud Prevention Counter Express Resource****, located in the pocket of this resource binder, for additional information on these types of Agent Fraud.*

Following the guidelines below will help stop many of these attempts on your employees and business from being successful:

- Do not share confidential information with ANYONE.
- Install and maintain real-time anti-virus/spyware/malware desktop detection and removal software.
- Log off or turn off computers when not in use.
- Do not check email, access the internet, or use online banking on the computer processing MoneyGram send/ receive transactions.
- Don't respond to or open attachments or click on links in emails from ANY sender you do not know, while using any computer.
- Realize pop-up messages claiming your machine is infected and offering software to scan or fix the problem may not be legitimate. Confirm with an expert before clicking pop up. Cancel if at all possible.
- **Never send a "test" or "training" transaction. NEVER.**
- **Never** send a transaction without having the cash in your hand and a consumer in your location
- Do not attempt to start a transaction that initiates over the phone
- Remove or restrict call forwarding features on your business telephone
- *Regularly test your employees on these guidelines and train on illicit techniques*

Protect your PIN

- Do not share your PIN with ANYONE
- Change the PIN every time an employee leaves
- Change the PIN periodically
- NEVER state your PIN or agent number in front of a consumer
- Do not post or write your PIN where a consumer can see it
- Do not provide your PIN over the phone unless you initiate the call to MoneyGram

Counterfeit Financial Instruments/Money Orders Fraud

A new type of fraudulent money alteration or counterfeiting appeared when computerized color laser copiers became capable of high-resolution copying. They can easily produce documents whose quality is difficult to distinguish from real documents. Such documents include, but are not limited to: *commercial/personal checks, counterfeit cash, traveler's checks* and *money orders.*

Use the guide below to avoid fraudulent money order transactions:

When Selling Money Orders

- Collect cash for the purchase of the money order **BEFORE** you print and give the money order to the consumer
- Be sure the cash you collect does not contain any counterfeit bills.
  Please visit www.secretservice.gov/money_detect.shtml for additional help on detecting counterfeit bills.

When Cashing Money Orders

- The warning band at the top of the money order will list security features you should confirm before trying to cash
- Check the money order for alterations. Look closely at the dollar amount, date, payee, and purchaser to make sure none of these have been changed
- Check the money order for erasures or thin spots, discolorations, distortions, or any damage
- Have the consumer endorse the money order exactly as the name appears on the front of the money order
- Obtain the same identification you would when cashing a check

Call MoneyGram IMMEDIATELY at 1-800-542-3590 if you have any doubts about a money order, to confirm dollar amount or stop payment status. You can also visit www.moneygram.com and click on the **Money Order** link under **"Products and Services"**.

REMEMBER

MoneyGram will NEVER call Agents and ask them to process a money transfer of any kind or to process a money order for ANY reason!!!

Consumer Fraud

MoneyGram works every day to prevent consumers from becoming victims of fraud. MoneyGram is committed to educating you so you can educate your consumers to build a safer and more reliable money transferring network. ***The key is to be conversational...not confrontational.***

Preventing fraudulent transactions from being completed protects you, our consumers, and MoneyGram's global brand. Fraud can occur during **Send AND Receive** transactions. Below is a guide for some of the more common consumer fraud type scams and directions on how to investigate further before completing the transactions.

Relative in Need:

Often, the "relative in need scam" begins with a phone call from the fraudster posing as a loved one, or even posing as law enforcement or a lawyer, asking for money to help with medical care, car repair, bailed out of jail, etc. **If you suspect you are processing a transaction for someone who has fallen victim to this scam, ask a few simple, conversational questions like:**

What is your relative doing in (name of place)? Is this normal for them to be here?

Have you sent money to (receiver's name) or used MoneyGram before? For what reasons?

Have you confirmed with other relatives or family members that the receiver is in another country?

Lottery or Sweepstakes:

A victim of the "lottery or sweepstakes scam" would likely be sending money to a company/organization instead of a single person. Typically they received notification of their "winnings" via email or letter, so keep an eye out for printed copies of emails or an envelope containing the letter that the sender may be referring to while filling out the form. **Ask questions like:**

I have never heard of that lottery/sweepstakes organization, where did you hear about them?

I have never heard of someone having to send money to cover the taxes or customs fees, do you know why they have asked you to do so?

Online Purchase:

Sending money for an online purchase should ***always be considered a red flag***. Most internet sites provide a different payment option that offers a greater level of protection for both buyer and seller than a money transfer. If you learn someone is paying for something online consider the following:

Do they use a Test Question and Answer related to the item? A definite red flag something may not be legitimate.

Did they mention they are sending money to pay for a service or an item purchased from the Internet?

Often, they will send within the United States.

Romance:

In many cases, the consumer may indicate they have met, or been contacted by, someone online and believe they are in a "romantic" relationship. Taking advantage of your consumer's emotional state, the fraudster will ask them to send money so they may visit/move to start a life together. You should not hesitate to inquire about their romantic interest by asking questions and remembering tips like:

"How long have you known (the receiver)?"

"How did you two meet?"

"Did you discuss alternate trip plans where you are not the one having to pay?"

"What is the urgency?"

Are they sending to a different country, such as Nigeria, Jamaica, or Canada?

Other types of consumer fraudulent scams include, but are not limited to:

- Check or Money Order Scam
- Disaster Scam
- Vehicle Purchase Scam
- Fake Loan Scam
- Newspaper Ad Scam
- Mystery Shopper Scam

To learn more about these and other types of fraudulent activity, please regularly visit:
www.moneygram-preventfraud.com

If you suspect a fraudulent transaction, even if in doubt, you should IMMEDIATELY report it to MoneyGram by phone at 1-800-866-8800 or by e-mail at fraudalert@moneygram.com.

Financial Crimes Enforcement Network (FinCEN)

The Financial Crimes Enforcement Network (FinCEN) is a bureau within the U.S. Department of the Treasury that administers the federal government's anti-money laundering laws and regulations. FinCEN has created materials to assist Money Services Businesses (MSBs) with compliance with these laws and regulations.

MSBs should familiarize themselves with information provided by FinCEN and should regularly review FinCEN's MSB website, www.fincen.gov, (select *Information for Money Services Businesses*) for updates or new information related to anti-money laundering compliance.

Below is a list of some of the information available on FinCEN's website*:

MSB Home Page – This section provides important information MSBs including MSB registration information, MSB materials in English and seven foreign languages, and additional contacts, including appropriate State contacts. Recent news for MSBs is also provided.

Guidance – This section is intended to clarify issues or respond to general questions about FinCEN regulations that are applicable to MSBs.

E-Filing – This section contains instructions and links for E-Filing

Advisories/Bulletins/Fact Sheets – This section contains FinCEN advisories relating to money laundering and other financial crimes. It also contains helpful bulletins and fact sheets for MSBs.

Quick Links – There are quick links to general information for MSBs, MSB Frequently Asked Questions (FAQs) and MSB Useful Tools/Information.

The Quick Links section provides access to a very important and informative document titled, "MSB Examination Manual". This document provides a summary of Bank Secrecy Act / Anti-Money Laundering (BSA/AML) compliance requirements and exam procedures to the MSB industry. It contains an overview of AML program requirements, BSA/AML risk and risk management expectations, sound industry practices and examination procedures.

**FinCEN owns and manages the content on this website. Information/Location could change without notice.*

Do I Need to Register as a Money Services Business (MSB)?

If you engage in MSB activities as defined by the **BSA**, you should work with your MoneyGram Representative to determine your requirement to electronically register (E-file) via the internet as an **MSB** with the **U. S. Department of the Treasury**.

Please review **Section 6 - MSB Registration** *of this resource binder for additional guidance.*

Creating an Anti-Money Laundering Compliance Program

The **BSA** and **USA PATRIOT Act** regulations require that all **MSB's** adopt a formal and written anti-money laundering ***Compliance Program*** that is reasonably designed to ensure proper recordkeeping and reporting of certain transaction and to prevent your business from being used to launder money. At a minimum, your anti-money laundering compliance program must include:

A. The designation of a Compliance Officer who is responsible for assuring that:

- Policies and procedures are followed
- Procedures are updated as needed
- Training and education are provided
- Reports are properly filed

B. Internal policies, procedures and controls for:

- Verifying consumer identification
- Transaction Monitoring
- Filing reports
- Creating and retaining records of all transactions
- Responding to law enforcement requests

C. An ongoing employee training program that:

- Explains policies and procedures
- Teaches how to identify suspicious activity
- Identifies how and where training records are filed and permanently kept

D. An independent review of your anti-money laundering program:

- How often and how much of your anti-money laundering program should be reviewed must depend on the compliance risks specific to your business. A "best practice" is to have a review at least once a year. However, more reviews may be required, if applicable.
- The review may be performed by one of your employees, but **cannot** be performed by your Compliance Officer, anyone that reports to the Compliance Officer, or by a MoneyGram Representative.

Section 2 - Compliance Program *of this Resource provides addition guidelines for establishing your Compliance Program.*

What Are the Consumer Identity (ID) Confirmation Requirements?

Money Transfers

Before completing any **Send** money transfer that is for the amount of $900.00 or more, you must **confirm** the consumer's identity by **asking for and looking at** a valid government issued photo identification that contains the person's name and address, such as a valid (non-expired) driver's license or other government-issued ID card. *If the consumer **is not** a resident of the U.S., a passport, an alien identification card or other official document must be presented that will provide evidence of the consumer's nationality or residence.*

For all RECEIVE money transfers, *regardless of amount*, you **MUST CONFIRM THE CONSUMER'S IDENTITY.** The use of test questions and acceptable answers are permitted for money *transfers* **up to $899** if the beneficiary does not have acceptable photo identification. Identification details or the answer to the test question **must be recorded** for **RECEIVE** transactions.

Additional Money Transfer Consumer ID Requirements

Both money transfers sending and receiving agents must obtain and **RECORD** specific consumer ID information for money transfers, *depending* on the amount, regardless of the method of payment. The consumer must be physically present in your location when conducting a transaction so that you can obtain and verify the consumer's identifying information. Use the following table to determine what information needs to be recorded: *(See next page for Third Party (On Behalf) transactions.)*

	$0.01 - $899.99	$900.00 - $2,999.99	$3000.00 - $10,000.00*
Name	X	X	X
Address	X	X	X
Transaction Amount	X	X	X
Transaction Date	X	X	X
Valid Government Issued Photo ID. *(See above if Non-US Resident)*		X	X
Social Security # or Tax ID #. *(See above if Non-US Resident)*			X
Date of Birth			X
Specific Occupation			X

Before* completing single or multiple transactions that total **more than $9,100, you **MUST** contact MoneyGram Anti-Money Laundering Operations at 1-800-444-3010 (Select Option 7).*

Maximum Aggregated Transactions

The maximum allowable send amount **per transaction** is $10,000. However, before proceeding with any amount of $9,100 or more, you must call 1-800-444-3010 and select Option 7 for a sender interview. This process could take 30 - 45 minutes.

MoneyGram limits consumers to a maximum aggregated send total of $20,000 per day, subject to the same process detailed above.

Transaction Record Retention Requirement

You must retain the physical documents for all money transfers of $3,000 or more for five (5) years.

Money Order Consumer ID Requirements

If the same consumer purchases $3,000 or more in money orders, using cash, in the same day, you **MUST** obtain and record the following consumer transaction information on a Money Order Log **BEFORE** completing the transaction(s):

- Name and Address of **location** where money order was purchased
- Name and Address of **consumer** purchasing the money order
- Date the consumer purchased the money order
- Occupation/Job of consumer purchasing money order
- Social Security Number or Tax ID. Number of consumer purchasing money order

  *If the consumer **is not** a resident of the U.S., a passport, an alien identification card or other official document must be presented that will provide evidence of the consumer's nationality or residence.*
- Date of Birth of person purchasing the money order
- Type of valid government issued photo ID provided *(i.e. TX Drives License)* and number on ID
- *TOTAL amount of ALL money order purchased by the consumer*
- Serial number(s) of **EACH** Money order

  (Has to be all digits. Using characters such as "XXX" to bypass this requirement is not allowed.)
- Amount of **EACH** money order purchased

A Note About Third Party (On Behalf) Transactions

If you know that your client is sending/receiving a money transfer or purchasing a money order on behalf of someone else, then you must also obtain the same information on that other person. Examples of this could be a relative of an elderly person receiving money for the elderly person (both MUST BE physically at your location) or an employee of a business conducting the transaction for the business.

What Are Currency Transaction Report (CTR) E-File Requirements?

Cash transactions that are greater than $10,000 conducted in one day, by any person, or on behalf of another person **REQUIRE** a ***CTR*** to be electronically filed with the federal government via the FinCEN E-File* system. The $10,000 threshold includes both the face amount of the transaction and all fees paid by the consumer.

You must treat multiple cash purchases of money orders or money transfers in aggregate if you have knowledge that the transactions are conducted by or on behalf of the same person and total more than $10,000 during one business day.

CTR E-File Requirements (US Code of Federal Regulations Title 31)

- You must E-File the CTR within 15 days of the transaction using the FinCEN E-File System
- DO NOT send the CTR to MoneyGram
- You must print and keep, or have access to a copy of each E-File CTR for at least five (5) years

Please reference Section 7 - CTR E-FILE for FinCEN CTR E-File procedures.

NOTE: *CTRs and other records and reports are only as good as the information you provide. Therefore, it is very important that the information you provide on such reports is accurate and complete. This is your responsibility. The government and law enforcement agencies depend on this information as they fight against money laundering, fraud, and terrorism.*

What is Suspicious Activity?

"Suspicious Activity" can vary from one transaction to another based on the circumstances surrounding the transaction or group of transactions.

For example, the transactions by one consumer may be normal because you are familiar with the consumer's transactions through repeat business, while similar transactions by another less frequent consumer may be suspicious. Many factors are involved in determining whether the transactions are suspicious, including:

- Amount of the transaction(s)
- Locations of your business
- Comments and/or behavior of your consumer

It is important for you and all of your employees to read and know the material in this resource to help you detect any suspicious activity related to all money services transactions.

Examples of Various Suspicious Activity:

Example 1: A consumer says that he wants to send $5,000 and wants to pay in cash. When you tell the consumer that you need to collect his personal identification information, he asks what amount he can send without showing his ID. You should E-File a SAR on the transaction or attempted transaction.

Example 2: A consumer purchases money orders with cash just below $3,000 over the course of several days. The consumer may be structuring his purchases. You should consider E-Filing a SAR.

Example 3: You see Jim hand cash to Bill and Susan outside your store. Bill and Susan each give you cash and purchase money orders that total less than $900 each, but total more than $900 together. This appears to be a structured transaction and may require the E-Filing of a SAR and the entry of the purchase in the Money Order Log.

Example 4: A consumer picks up a money transfer from your location. After the consumer has left, you discover that the consumer also picked up money transfer at some of your other offices on the same day. The consumer may be attempting to avoid recordkeeping and reporting requirements. If you suspect that structured or suspicious activity has occurred, you must E-File a SAR for the total of all the transactions. If the total amount of currency paid the consumer exceeds $10,000 in one day, you must also E-File a CTR.

Example 5: A consumer picks up a money transfer at your location that is along the U.S. border and is accompanied by another person. The other person appears to be telling the consumer what to do. After the transaction is completed the consumer gives the money to the other person. The consumer may be paying to have a family member or friend smuggled across the border. You should E-File a SAR on the transaction or attempted transaction.

Note:

The above examples are a few of several possible situations or transaction types that could be suspicious and should not be considered a rule for all. Additional examples can be found at www.fincen.gov. If you ever have any concerns regarding what appears to be suspicious activity, please do not hesitate to contact MoneyGram at 1-800-444-3010 and select Option 7.

What Are Suspicious Activity Reporting (SAR) E-File Requirements?

ANY transaction that appears to be suspicious does **REQUIRE** a ***SAR*** to be *electronically filed* with the federal government via the FinCEN E-File* system. These types of transactions include, but not limited to, the conditions below:

1. Involves funds that you suspect are from illegal/criminal activity or are intended to hide funds derived from illegal/criminal activity
2. Appear to be structured to avoid recordkeeping or reporting requirements
3. Appear to have no legitimate business or apparent lawful purpose

SAR E-File Requirements

- You must E-File a **SAR** with FinCEN within **30 days** of detection of the suspicious activity
- DO NOT send the report to MoneyGram
- You must print and keep, or have access to a copy of each E-File **SAR** and all supporting documentation for at least five (5) years
- **Never tell your consumer that you E-Filed a SAR**

  Note: It is illegal to tell your consumer that you are E-Filing a SAR-MSB. If MoneyGram believes that some of your consumers may be misusing its money orders or money transfers our compliance staff may contact you as part of an investigation. You must not tell your consumer about this type of inquiry either.

Please reference Section 8 - SAR E-FILE for FinCEN SAR E-File procedures.

NOTE: *SARs and other records and reports are only as good as the information you provide. Therefore, it is very important that the information you provide on such reports is accurate and complete. This is your responsibility. The government and law enforcement agencies depend on this information as they fight against money laundering, fraud, and terrorism.*

SAR or CTR?

E-Filing a **SAR** is a separate requirement from E-Filing a **CTR**. Even if you have E-Filed a CTR on a transaction or set of transactions, you must also E-File a SAR if you believe the activity is suspicious.

What is Structuring?

Many money launderers are familiar with the dollar thresholds that require recordkeeping and reporting. Therefore, in order to remain anonymous and avoid the detection of law enforcement officials, they will "structure" their transactions so that the recordkeeping or reporting requirements will not be triggered. Structuring is the act of breaking up a potentially large transaction into several smaller ones to avoid reporting or recordkeeping requirements.

What if I Suspect Structuring?

It is illegal for you or your clients to structure transactions in order to avoid the recordkeeping or reporting requirements.

For example, if a client sends a $1,500 money transfer in the morning and another $1,500 money transfer send transaction in the afternoon, he may be structuring his purchases in order to avoid the $3,000 recordkeeping requirements.

It is illegal for you or your employees to assist anyone in structuring transactions to avoid recordkeeping or reporting requirements. For example, you may not tell or even imply to a client that they can avoid providing information by conducting a smaller transaction. Some criminals may attempt to trick you or your employees into allowing them to structure transaction by splitting up their activity with several accomplices or by trying to "con" you with a hard luck story. You need to be on the lookout for structuring so that you prevent it from occurring.

Are all multiple transactions considered structuring?

No.

For example, a client sends two money transfers to separate receivers, one for $2,000 and another for $1,500. Each transfer is less than $3,000, but the total of the transactions exceeds $3,000. You learn that the consumer is sending money to her children who are attending two different schools.

This is also an example of the transaction review documentation you would make and retain as part of your **MONITORING** program.

Data Policy

As an agent, you must safeguard nonpublic personal information. You may only ask for and collect the personally identifying information that is necessary to complete the transaction.

In accordance with the *Federal Trade Commission's Gramm-Leach-Bliley Act Safeguards Rule*, you are required to maintain appropriate safeguards for nonpublic personal information, including having written policies in place regarding the collection and disclosure of consumer information considered to be "nonpublic personal information" and designating an employee or employees to coordinate your information security program. Please reference the **FTC website** for additional help to create your information security program: www.business.ftc.gov/privacy-and-security

Other tips include, but are not limited to:

- Avoid loudly referencing identification data such as addresses, telephone numbers, social security number, etc. where others can hear what you are saying
- Never show the MoneyGram system monitor screen to any consumer.
- Any notes, forms, logs or other documents containing a consumer's nonpublic personal information must be shredded before disposing of the documents.

Record Retention

All record keeping and reporting documentation required by the Bank Secrecy Act (BSA) and state specific regulations will be maintained for a minimum of five (5) years and they will be made readily available to the U.S. Treasury Department and/or representatives from other government officials upon legitimate request.

Receipts for all transactions of $3,000 or more are required by law to be stored and accessible for a minimum of five (5) years.

Consumer Privacy
In accordance with the Privacy Act, you must protect consumers' personal and private information. All documents that contain consumers' private and personal information will be stored in a secure location. If you wish to legally discard any MSB/MoneyGram related documents, the documents must be completely destroyed prior to disposal.

Personal Use of Services

As a MoneyGram Agent, you should not initiate, process, or complete any personal MoneyGram money service on behalf of yourself or immediately family members.