First Line of Defense

As an Agent, you are our first line of defense. Looking for these key red flags and asking additional questions prior to sending or receiving a transaction may help to deter the fraudster.

When **SENDING** money, be alert to consumers who:

- Are elderly and sending money internationally
- That send frequent transactions within a day, week, etc.
- Appear to be agitated, upset, or nervous, or overly excited
- Inquires about procedure for a refund or to reverse transaction

When **RECEVING** money, be alert to consumers who:

- Receive frequent transactions within a day, week, etc.
- Have come to your location using different names or various forms of ID

MoneyGram International

We strongly urge each of our Agent locations to continue to be vigilant in watching for suspicious activities.

- **If you suspect fraud, do NOT complete the transaction. Advise the consumer that there is a problem with their transaction and to contact MoneyGram**
- **Contact MoneyGram by phone at 1-800-866-8800 or e-mail fraudalert@moneygram.com**
- **Advise potential victims to visit MoneyGram's Money Transfer Fraud Education Center at:**

www.moneygram-preventfraud.com

2012 MoneyGram Agent *Holiday Fraud Awareness and Determent Guide*

1-800-866-8800

Email:
fraudalert@moneygram.com

www.moneygram-preventfraud.com

Fraudsters never take a holiday, so it's important for Agents and consumers to be alert to signs of possible fraud, keeping the consumer's shopping and charitable dollars out of the hands of these criminals.

During the holiday season, there is a historic increase in fraud activity. Scam artists are out to turn the season of giving into the season of taking, by attempting to defraud people out of their hard-earned money.

MoneyGram wants to assist you in deterring any opportunities the thieves may have to get their hands on consumers' money through illegal methods, and help consumers learn their tricks before they become victims.

This brochure is intended to raise awareness and allow you to help consumers protect themselves from becoming victims of scams typically on the rise this time of the year.

Holiday Notes!

70% of Americans plan on shopping online during the 2012 holiday season.

Source: Mashable.com

In December 2011, online scams increased almost 13% from previous month.

Source: Securelist.com

Consumer Victimization Scams

Everyday, consumers worldwide receive offers sounding too good to be true. Scammers do not discriminate and will target people of all backgrounds, ages, and income levels. Below are the top scams trending recently:

Internet Purchases

Fraudsters use online auctions and internet shopping to target potential victims. Consumers shopping for high end merchandise such as automobiles, concert and sporting event tickets, and new family pets are likely victims. Consumers should protect themselves by:

- *Never buying from sellers with poor ratings*
- *Being wary of sellers who ask you to send funds internationally*
- *Only making purchases through a reputable website and/or company*

Emergency Scams

This scam typically involves a grandparent who receives a phone call from a scammer claiming to be a grandchild in trouble needing money immediately. The caller indicates they have been in an accident and are having trouble returning from a foreign country or they need bail money. To protect themselves consumers should:

- *Never send money to anyone they don't know and trust*
- *Verify the story with the child's parent or friends*
- *Ask the person on the phone questions only their loved one know the answer*

Romance Scams

These scams involve dating and romance websites where the scammer will try to defraud a person by sending emails with talk of need, love and/or desire. Individuals should:

- *Use legitimate and reputable dating websites*
- *Never provide personal information or details about banking accounts when chatting online*
- *Be concerned of someone who declares their love after only a few letters or emails*

Agent Targeted Computer Crimes

Cyber criminals target employees at Agent locations and cause the targeting individuals to spread malicious software or "malware) to steal MoneyGram log-in credentials. Then the fraudsters are able to remotely log-in and complete unauthorized transactions. To protect yourself from this type of scam:

- *Don't respond to or open attachments or click on links in unsolicited emails.*
- *Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem.*
- *Log/turn off computers when not in use.*
- *Install and maintain real-time anti-virus and anti-spyware desktop firewall and malware detection and removal software.*
- *Do not use the same computer that's being use to send/receive MoneyGram transactions for checking email, accessing the Internet, or on-line banking.*

Agent Targeted Social Engineering

Agents receive phone calls from people alleging to be from MoneyGram Customer Service or the Agents IT department. They state that there is a system error and transactions are not being sent/received correctly. The caller instructs the Agent to send transactions to "test" a fix that was recently implemented. Remember:

- *MoneyGram will never call Agents and ask them to perform a Money Transfer of any kind*
- *Never send a transaction for anyone WITHOUT first having cash in hand*
- *Do not perform any transactions initiated over the phone*
- *Never share your log-on and PIN information with anyone*