FRAUD PREVENTION
COUNTER EXPRESS RESOURCE

Contact MoneyGram IMMEDIATELY if you suspect ANY transaction to be fraudulent:

1-800-866-8800

Recognize 3 Common Types of Fraud

Agent Fraud

Occurs when your employees are targeted by individuals attempting to steal Agent or consumer information to commit further fraud. Below are two common categories of Agent Fraud:

***Computer Crimes*:** Attempting to "take over" Agent computer by installing illegal software that will allow Agent and consumer information to be stolen. **FIGHT BACK!**

- Log/turn off computers when not in use
- Don't respond to or open attachments or click on links in unsolicited emails
- 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
- Be wary of pop-up messages claiming your machine is infected and offering software to scan and fix the problem. Ask someone first before responding to these types of computer messages

***Social Engineering*:** Someone claiming to be from MoneyGram calls and wants you to help fix a system problem or run a test. They might try to get you to run a test transaction. STOP IT, NOW!

- MoneyGram will NEVER call Agent employees and ask them to perform a Money Transfer of any kind
- Do not perform any transactions initiated over the phone or without cash in hand
- NEVER share your log-on and PIN information with anyone
- Tell the caller you will call them back, get a phone number. Then, IMMEDIATELY call **MoneyGram Agent Services** at **1-800-444-3010** and inform the representative of the request.

Counterfeit Financial Instruments/Money Order Fraud

Modern printing technology makes it easier for individuals to give you counterfeit cash, various types of checks, and money orders. Take extra time to verify suspicious looking items.

- Collect cash for the transaction order BEFORE you proceed completing the transaction
- Confirm cash collected does not contain counterfeit bills. Please visit www.secretservice.gov/money_detect.shtml for additional help on detecting counterfeit bills.
- For 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, erasures, thin spots, discoloration, or any damage. Look closely at the dollar amount, date, payee, and purchaser to make sure none of these have been changed
- Have the consumer endorse any item exactly as the name appears on the front and confirm
- Obtain the same identification for money orders as you would when cashing a check

REMEMBER

MoneyGram will NEVER call Agent employees and ask them to perform a Money Transfer of any kind

Turn this resource over for Consumer Fraud prevention and contact information.

/moneygram @moneygramMe

moneygram.com

MoneyGram bringing you closer

MG0913-33F

FRAUD PREVENTION
COUNTER EXPRESS RESOURCE

Contact MoneyGram IMMEDIATELY if you suspect ANY transaction to be fraudulent:

1-800-866-8800

Consumer Fraud:

Everyday, consumers worldwide receive offers sounding too good to be true. Scammers do not care who the person is and will target people of all backgrounds, ages, and income levels. Below are the top fraud scams to be on the look out for:

- ***Relative in Need*:** Consumer is told to immediately send money to help a "relative" or friend to pay for airline ticket, bail, medical care, etc.
- ***Lottery or Sweepstakes:*** Consumer has received an email or phone calling tell them they won money in a lottery or sweepstakes and must send funds to cover service, transfer, legal, or administrative fees.
- ***Online Purchase:*** Consumer is paying for something they "bought" online for a "really good deal." 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.
- ***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. The fraudster will ask them to send money so they may visit/move to start a life together.
- ***Other:*** Other types of fraudulent scams include, but are not limited to: Fake Check/Money Order, Disaster Relief, Vehicle Purchase, Fake Loan, Newspaper Ad, or Mystery Shopper.

GET INVOLVED. ASK QUESTIONS

You can help ***PREVENT*** fraud by simply asking the consumer questions regarding the situation requiring them to send money. ***The key is to be conversational...not confrontational.***

When suspecting fraud, ask the following types of questions, depending on the situation, to help you make an informed decision regarding the transaction.

- *How do you know the person you are sending the money to?*
- *Where did you meet them?*
- *What is the location of the person?*
- *Have you ever sent money to this person (or this location) before?*
- *How did you hear about this offer?*
- *Have you ever bought anything from them before?*
- *Did you actually enter this sweepstakes?*
- *How did you hear about the sweepstakes?*

If you expect 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.

Turn this resource over for AGENT and COUNTERFEIT fraud type information.

/moneygram @moneygramMe

moneygram.com

MoneyGram bringing you closer