

# FRAUD PREVENTION NEWSLETTER

September 2009



## Counterfeit Money Orders

Inside This Issue

Counterfeit Money Orders

Visa® Check Card Safety

ATM Skimmers

MoneyGram offers an efficient and speedy way to send money throughout the world. Unfortunately, some fraud perpetrators use our services to fool or trick consumers with a variety of scams. Be very suspicious if you receive the following:

- A check or money order sent to you if you are asked to cash the item at your bank and to send a portion of the funds to someone else through MoneyGram. If the check is counterfeit your bank will make you cover the loss. Be warned that counterfeit checks look very real.
- A telephone call telling you that you have won money or a prize and that you need to send money to pay for taxes, customs fees, etc.
- A response to your newspaper ad for a lost pet or lost personal items, because fraud perpetrators use the classified ads to find people to contact and pretend that they have the lost item.
- A suggestion from a stranger that you send money to a friend or relative as a show of "good faith" because legitimate business is not conducted in this manner. They will tell you that by sending the money in the name of a friend that they will be able to collect the funds. That is not true. Con artists often use fake identification to pretend to be someone else.

Counterfeit Money Orders are normally obtained when a person gets involved in a "too good to be true" financial scheme, or is solicited by a beautiful woman (or man) needing to be rescued from a foreign locale. This normally occurs on the Internet.

Here are some examples of the lures used to pass these items along:

- Some of these lures include, but aren't limited to (new lures surface frequently), secret shopper, romance, lottery, work-at-home and auction scams.

A common denominator in most of the scams is that there will be a request to send the proceeds, minus your paltry cut (normally via wire transfer) back to the person sending you the instruments. That is (unless) they are buying goods from you. In this case, your property is what they want you to send to them.

In other words, if the item is cashed at a financial institution, when it comes back as a counterfeit — they will hold you and YOU ALONE liable.

More and more often, criminals pretend to be victims and pass the items. These people are called "reverse scammers" because they have no intention of wiring any money back to the original scammer.

The best way to avoid getting scammed is to call and verify the item at MoneyGram. This can be done by calling 1-800-542-3590. In almost all cases, this call will reveal the item as a counterfeit. **BE SURE THE PERSON OR COMPANY TO WHOM YOU ARE SENDING MONEY (OR AT WHOSE REQUEST YOU ARE SENDING MONEY) IS SOMEONE YOU KNOW AND TRUST. BE SURE TO KEEP INFORMATION RELATING TO YOUR TRANSACTION CONFIDENTIAL. ONCE THE MONEY HAS BEEN PAID OUT TO THE PERSON YOU NAME AS THE RECEIVER, CANCELLATION OR REFUND IS NO LONGER POSSIBLE. IF YOU NEED TO CANCEL OR CHANGE A TRANSACTION, PLEASE CONTACT MONEYGRAM.**

MoneyGram money orders aren't the only instruments being counterfeited. Counterfeit cashier's checks, money orders, gift and traveler's checks are also being counterfeited and used in these types of scams.

If you want to learn more about these scams, it is recommended you go to the Web site [fakechecks.org](http://fakechecks.org). There are some great videos illustrating the scams used to pass counterfeit items.

# FRAUD PREVENTION NEWSLETTER

## Visa® Check Card Safety

Using your Visa® Check Card is a simple, hassle-free way to get cash, make deposits, check account balances, transfer funds, make purchases and more. To enjoy the many conveniences a Visa® Check Card offers, make protecting your Visa® Check Card a priority. Here are some important safety tips.

**TREAT YOUR CARD LIKE CASH.** Always store your card in a safe place.

**KEEP YOUR PIN TO YOURSELF.** No company or individual needs to know your PIN ... not even us. Memorize your PIN, and never write it on your card or store it with your card. Never let a cashier, teller or other stranger enter your PIN for you.

**ALWAYS BE AWARE OF YOUR SURROUNDINGS.** When using an outdoor ATM such as in a parking lot, look for suspicious activity before you begin your transaction.

**SHOP CAREFULLY ONLINE.** If you initiate an online transaction and must provide personal data, look for indicators that the site is secure, like "https" in the Web address or the closed padlock icon in the bottom frame of your browser. It is also wise to conduct transactions on wired Internet connections only. Wireless connections can be more vulnerable to attack.

**PROTECT YOUR CARD'S MAGNETIC STRIP.** Exposing your card's magnetic strip to other magnetic objects can cause damage that will make your card unusable.

**REPORT A LOST OR STOLEN CARD AT ONCE.** Call us right away if your card is lost or stolen to reduce the chance that it will be used improperly. Immediate notice of lost or stolen cards also will limit your potential liability for unauthorized transactions. During business hours, call the Bank toll free at 866.770.3100. After business hours, call Visa's Lost or Stolen Card Hotline at 800.754.4128. Please have your card number ready.

**REVIEW ACCOUNT STATEMENTS REGULARLY.** The Internet is a common channel for fraud perpetration. Never provide your Visa® Check Card number, PIN or any other non-public information to anyone in response to an unsolicited e-mail, pop-up message or phone request. We will NEVER ASK you for your PIN.

## ATM Skimmers

The Illinois Department of Financial and Professional Regulation is warning consumers to be on the outlook for automated teller machine scams.

One method of scamming consumers is referred to as ATM skimming. ATM skimmers are devices that criminals install on ATM machines that steal unsuspecting consumers ATM account information. In addition, a small camera is installed in the skimmer or at another location near the ATM to capture the consumers PIN number. Once the information is captured, criminals are then able to make up their own ATM cards along with their associated PIN.

Following are tips that consumers can follow to help protect themselves from ATM skimmers:

1. Observe the ATM you are using, don't use the ATM if you see something that looks out of the ordinary such as wiring or an odd looking device.
2. Use the same ATM as much as possible. If you do this you will be familiar with the ATM and be able to spot if someone has tampered with the machine.
3. Be cautious if you see signs or stickers on the ATM that instruct you to "scan here first" or "no tampering". These are generally placed on the machine by the ATM thieves to divert your attention from the new piece of equipment.
4. Do not use the machine if someone offers to help you with your transaction. Criminals who install skimmers will often pose as another customer or technician working on the machine to assist users with their transactions.
5. Be wary of a jammed ATM machine that forces customers to use another ATM that has a skimmer attached.
6. You should always protect your PIN by not writing it down or giving it to anyone. Always cover the keypad while entering your PIN and never allow people to look over your shoulder while entering your PIN.
7. Use ATM machines where video cameras are installed. Criminals are less likely to install skimmers at such locations.
8. Consumers should monitor their account activity via monthly transaction statements or the Web and report any abnormal activity to the Bank as soon as possible (call toll free 866.770.3100).

## Websites for More Information

Internet Fraud (Federal) <http://www.ic3.gov>

Internet Crimes Unit (State) <http://www.isp.state.il.us/icu/>

The unit can be contacted by clicking on the bottom "Report an Internet Crime" or by calling the toll-free number 1-888-70-CRIME (1-888-702-7463).

Internet Crime Complaint Center <http://www.ic3.gov/crimeschemes.aspx>

Federal Trade Commission Identify Theft Website  
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

US Department of the Treasury Identity Theft Resource Page <https://www.treas.gov/offices/domestic-finance/financial-institution/cip/identity-theft.shtml>

FDIC Consumer Resources Website

<http://www.fdic.gov/consumers/consumer/index.html>

FDIC Consumer News

<http://www.fdic.gov/consumers/consumer/news/index.html>

The Federal Reserve Board Consumer Information Page

<http://www.federalreserve.gov/consumers.htm>

OnGuard Online, Your Safety Net <http://www.onguardonline.gov/spam.html>

AnnualCreditReport.com <http://www.annualcreditreport.com/cra/index.jsp>

Scam Victims United [http://www.scamvictimsunited.com/atm\\_scam.htm](http://www.scamvictimsunited.com/atm_scam.htm)