

PROTECT YOUR IDENTITY

IDENTITY THEFT NEWSLETTER

Don't become a victim.

JULY 2010 / VOL. 7

ATM SKIMMING FRAUD WARNING

There has been a large increase in the number of ATM skimming devices being deployed in this part of the country. This involves criminals placing a device over the area of the ATM where the card is inserted so that information from the card is captured and then used later for fraudulent transactions. Please look carefully before using an ATM to ensure that the area where you insert your card does not look unusual or appear to have anything attached to it. If you are unsure do not use the ATM. Also, consumers should not try to remove a suspected skimming device, but rather report any fraudulent activity to the police and the financial institution immediately.

Shielding the entry of the PIN with your hand and body is just one way you can prevent someone from viewing it via electronic or human means.

Consumer tips to help reduce ATM skimming incidents:

1. Be wary of anything about the ATM machine that looks out of the ordinary, such as odd-looking equipment or wires attached to the device.
2. Look for a "no tampering" sign. Crooks often place these to stop anyone curious about a new piece of equipment.
3. Steer clear of a jammed ATM machine that forces customers to use another ATM that has a skimmer attached. Often, the criminal will disable other ATMs in the area to draw users to the one that has the skimming device on it.
4. Customers should check their bank accounts regularly to make sure there are no unusual or unauthorized transactions. Federal law limits loss from ATM fraud, and many banks offer additional protection. Consumers should check with their financial institution for details.
5. If you see anything unusual or suspicious around an ATM, or if you find unauthorized ATM transactions on your bank account, immediately notify local law enforcement, as well as your financial institution and/or the establishment where the ATM is located.
6. Always protect your PIN: Don't give the number to anyone, and cover the keypad while you are entering your PIN.

FRAUDSTERS TAKE AIM AT MOBILE BANKING

Best Practices for Securing Your Mobile Phone

Beyond phishing concerns, there are some best practices that cell phone users should keep in mind when using their phone, whether for business or for personal use.

- **Make No Assumptions** - Never assume that voice calls are confidential (like fax or email), especially when calling internationally where some countries' phone operators have no encryption security in place at all. Check your signal, calls on 3G are more secure than 2G but often falls back to 2G when 3G is unavailable.
- **Ensure Physical Security** - Keep your phone safe and do not leave it lying around. Skilled attackers can take just a few moments to install a malicious program, compromise the security of the SIM card or install a special battery with a bug in it, all of which can later be used to help intercept calls.
- **Protect PINs** - Use and protect your phone and voicemail PINs in the same way as your bankcard PIN. Never leave confidential messages in voicemails or send confidential texts. Texts in particular are easy to read on the phone and mobile phone voicemails can often be accessed from any phone with the PIN.
- **Be Mindful of Malware** - Be vigilant to prevent malicious software on your phone. Be wary of texts, system messages or events on your phone that you did not ask for, initiate or expect. Turn off Bluetooth if you are not using it.
- **Take Precautions** - Consider installing antivirus/antimalware software. And if you strongly suspect your calls are being listened to, then turn off the phone when you don't need it and remove the battery as an extreme precaution. Also, use voice call encryption software on your phone to secure your sensitive calls that works worldwide and is as easy to use as making a normal phone call.



Beware of the "Census Taker"

Identity protection firms have partnered with the Census Bureau in an effort to get the word out that thieves will attempt to use the current Census to steal identities.

Those homes that did not fill out a census form by mail will receive a visit to their home address from a Census taker. According to LifeLock, identity thieves may take advantage of this fact and begin targeting unsuspecting victims.

The company reports that Census scams range from fraudulent emails to attempts to impersonate Census takers. Many consumers don't think twice about sharing personal information with a Census taker, which is why the scams can be very effective, LifeLock reports. The company warned that a real Census taker will have a government badge and picture ID, as well as a confidentiality notice. These can be faked, however, so LifeLock also suggested that people consider that **census takers:**

- Do not ask for Social Security numbers or financial information such as bank account numbers.
- Never ask for money or say that a household owes money.
- Will not harass or intimidate.
- Will not contact a household by email, only by phone, mail or in person.

This newsletter is brought to you by


Chelsea Groton
Feel good about your bank.™

860-448-4100 • 860-823-4800

Member
FDIC

860-599-2406



Visit our website to view our latest Customer Notices

www.chelseagroton.com

MYSTERY SHOPPERS: *The Latest Fraud Scheme*

The latest alert from the **Internet Crime Complaint Center (IC3)** says **mystery, or "secret shopper," schemes are rampant.**

This employment offer comes via email or regular mail, and promises to hire the person to perform secret or random checks on a retailer or its competition. They are really slick; these fraudsters are even asking for resumes and performing background checks on the victims before accepting them as a mystery shopper, which opens the victim to further identity theft problems.

HOW THE SCAM WORKS:

The IC3 says victims are contacted via e-mail or U.S. mail to apply to be a mystery shopper. Applicants are asked to send a resume and are purportedly subject to an extensive background check before being accepted. The employees are sent a check with instructions to shop at a specified retailer for a specific length of time and spend a specific amount on merchandise from the store.

The employees receive instructions to take note of the store's environment, color, payment procedures, gift items and shopping/carrier bags, then report back to the employer. The second evaluation is the ease and accuracy of wiring money from the retail location. The money to be wired is also included in the check sent to the employee.

The remaining balance is the employee's payment for the

completion of the assignment. After merchandise is purchased and money is wired, the employees are advised by the bank the check cashed was counterfeit, and they are responsible for the money lost in addition to bank fees incurred.

TIPS TO AVOID BECOMING A VICTIM:

- Do not respond to unsolicited (spam) e-mail.
- Do not click on links contained within an unsolicited e-mail.
- Be cautious of e-mail claiming to contain pictures in attached files, as the files may contain viruses.
- Only open attachments from known senders. Virus scan all attachments, if possible.
- Avoid filling out forms contained in e-mail messages that ask for personal information.
- Always compare the link in the e-mail to the link you are actually directed to and determine if they match and will lead you to a legitimate site.
- There are legitimate mystery/secret shopper programs available. Research the legitimacy on companies hiring mystery shoppers. Legitimate companies will not charge an application fee and will accept applications online.
- No legitimate mystery/secret shopper program will send payment in advance and ask the employee to send a portion of it back.
- People who believe they have information pertaining to mystery/secret shopper schemes are encouraged to file a complaint at www.IC3.gov.

**SHRED!
SHRED!
SHRED!**

"Dumpster Divers" can steal your identity and rack up thousands of dollars against you just by quickly browsing through your trash. Shred the following to protect your identity:

- Expired credit cards
- Physician statements
- Insurance forms
- Charge receipts
- Checks and account statements
- Copies of credit applications
- Credit offers that you receive in the mail

*Protect yourself.
Buy a paper shredder
and use it often.*

Tips for Using Social Networking Sites Safely:

While social networking sites can increase a person's circle of friends, they also can increase exposure to people with less than friendly intentions.

- Understand what information should be private.
- Post only information that you are comfortable with others seeing.
- Use privacy settings to restrict who can access and post on your website.
- Once you post information online, you can't take it back.
- Trust your gut if you ever feel uncomfortable or threatened by anything online.



What to do if you fall victim to identity theft:

- Contact your financial institution immediately and alert it to the situation.
- If you have disclosed sensitive information in a phishing attack, you should also contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file, which will help prevent thieves from opening a new account in your name.

Below is the contact information for each bureau's fraud division:

Experian

888-397-3742
P.O. Box 1017
Allen, TX 75013

Equifax

800-525-6285
P.O. Box 740250
Atlanta, GA 30374

TransUnion

800-680-7289
P.O. Box 6790
Fullerton, CA 92634

- Report all suspicious contacts to the Federal Trade Commission through the Internet at www.consumer.gov/idtheft, or by calling 1-877-IDTHEFT.