Credit Card and Identity Theft
October 2010

On the list of things you'd hate to lose, your identity and credit cards rank high on the list, somewhere between your kids and car keys. Losing either one of these things has the potential to cause a lot of damage. The last thing you want is damage to your credit at someone else's hand, it's crucial that you know what to do when your identity or other important card has been lost or stolen. If you become a victim, here are steps you might want to take.

Identity theft victims can get detailed advice by calling the Federal Trade Commission's ID Theft Clearinghouse toll-free at 877-438-4338 or going to *www.consumer.gov/idtheft*. The FTC will send you a free booklet, "ID Theft: When Bad Things Happen To Your Good Name," or you can get it online. Do not use a complaint to the FTC as an official identity theft report

The first thing you should do **NOW is **make copies of all your credit cards, ID cards and licenses -- everything in your wallet.** Make sure you photocopy both sides of all your cards, and/or list your account numbers, and the toll free phone numbers you'd need to call to report them missing. **Keep this photocopy in a separate, safe place.** Be sure to update this information as needed.

Step 1. Call the companies/banks that issued your credit cards, debit card, ATM card, or checks to report the theft. Use the toll free number as soon as you discover the problem. Have your account number, the date you noticed your card missing and the date and amount of your last purchase ready when you call. Write down the name of each person you speak with. It's a good idea to follow up each of your phone calls with a letter. In the letter, summarize your phone conversation, including your name, account number, when you noticed that your card was missing, the date you first reported the loss via phone, and the name of the person you spoke with, include the date and amount of last authorized purchase, if known.

Alternatively, you can purchase a credit card registration service for an annual fee and register your account numbers with this service. Then, you only have to make one phone call to report all card losses (rather than calling each individual issuer). Many services also will request replacement credit cards on your behalf. Be careful. These services can be pricey for what they offer. If you go this route, compare offers since they do vary. Unless you're a victim of serious and ongoing identity theft, buying a service that alerts you to certain activities in your credit files probably isn't worthwhile, especially if it costs hundreds of dollars a year. In any event, you do need to make sure you keep your info up to date with the registration service, or it won't help you.

Step 2. Call the three national credit-reporting agencies to report the theft, and ask them to attach a 'fraud alert' to all your credit cards. This will oblige creditors to take extra precautions if someone applies for credit in your name to verify that it's really you. There are two kinds of fraud alerts. An "initial fraud alert" stays on your credit records

for at least 90 days. This is the kind of alert to use if you think you might be a victim but you're not sure – for instance, if you lost your wallet or you find out that someone has gotten access to the customer records at a place you do business. An "extended fraud alert" should be placed when you have reason to believe that someone has illegally used your identity. You must provide a copy of an official "identity theft report" to request an extended fraud alert, which will stay on your credit records for 7 years. Just contact one of the three major credit bureaus to place the fraud alert; it will be shared automatically with the other two. When you file a fraud alert, the credit bureaus will contact you with information about how to get free copies of your credit reports. Here are the three agencies and their numbers: Equifax: 1-800-525-6285, Experian (formerly TRW): 1-888-397-3742, Trans Union: 1-800-680-7289. You are entitled to free copies of your reports once in every 12-month period. ***Do not contact the credit bureaus directly for these free annual reports.*** They are only available by calling 877-322-8228 or going to *www.annualcreditreport.com*.

Step 3. Call the Social Security Administration if your social security card is missing. Fraud line is 1-800-269-0271. Also, be sure to contact the Department of Motor Vehicles about your driver's license, as well as any other organizations from which you lost cards.

Step 4. Call the police in the jurisdiction where your credit card(s) was stolen to report the theft and obtain an "official identity theft report".

Step 5. Know your payment rights. The Fair Credit Billing Act (FCBA) protects you when fraudulent charges are made with your lost or stolen credit card. Under federal law, if unauthorized charges are made with your credit card, the maximum amount you can be liable for is $50, if the charges are made before you report the loss. If the charges are made after you report the card lost or stolen, you have no liability. That's why it's important to report your missing credit card as soon as possible.

Step 6. Review your billing statement for a few months after, to catch any unauthorized charges. If you see any charges that you did not make, report them to your creditor as soon as possible.

Step 7. Respond quickly to debt collectors. If debt collectors contact you about accounts opened in your name or unauthorized charges made to your existing accounts, respond immediately *in writing*, keeping a copy of your letter. Explain why you don't owe the money and enclose copies of any supporting documents, such as an official identity theft report.

FRAUD PREVENTION TIPS:

***Lock up important documents** in a safe deposit box or in a hidden place at home. Thieves don't need your credit card in order to steal your identity. Sometimes all thieves need is one piece of information about you and they can easily gain access to the rest. Don't make it easy for them.

***Pay attention at the checkout line.** Try not to let your card out of your sight. Your card can be scanned using a "skimmer". This is an electronic device that captures your credit card information when you swipe it. Or a clerk can take a picture of the front and back of your card with a cell phone or merely swap out cards. Be sure to look at your card when they hand it back and make sure it's yours, and not a card that looks like yours.

***Don't give out your information** over the phone or internet (emails) unless you initiate the contact and you know the company is reputable. Be very careful to whom you give your credit card or social security number to. Never give your info out when you receive a phone call. (For example, if you're told there has been a 'computer problem' and the caller needs you to verify information.) Legitimate companies don't call you to ask for the numbers over the phone.

***Never respond to emails that request you provide your credit card info via email --** and don't ever respond to emails that ask you to go to a website to verify personal (and credit card) information. These are called 'phishing' scams.

***Make sure the website is secure** prior to providing your information.(i.e. address may start with **https**…)

***Sign your credit cards** as soon as you receive them. You can sign your credit card with a Sharpie so your signature can't be erased and written over. You can also add "See ID" to encourage cashiers to request your driver's license. Another suggestion is leaving the "please activate" sticker on. Since the card has to be activated from the phone number listed with the credit card company, some thieves won't bother with them.

***Be careful with your snail mail. Go paperless in as many ways as possible.** Try to cut back on the mail you receive by discontinuing paper bills and statements. Bills being sent to your home can be taken by an identity thief. They can get a hold of your account and change your billing address. It is recommended that you take outgoing mail to the post office or other secure receptacle. Stolen checks are another way thieves take your identity. With your routing and checking account number, a thief can create new checks and use them to make purchases. If possible, it is recommended that you pick up new checks at your bank rather than having them mailed to your home. Shred all credit card applications you receive.

***Each month, review all bank and credit card statements.** Watch for significantly small charges from unfamiliar companies or individuals. Most people don't notice small charges. Thieves will often "test" an account to check that the accounts haven't been canceled prior to purchasing a block of stolen credit card numbers. Once confirmed active, they will make a much larger charge. In addition, many of the fraud alerts you can set on your accounts aren't triggered by small dollar amounts. Reviewing your credit report on a regular basis is also a good idea, although by the time a fraudulent transaction reaches your credit report, it's often too late.

***Don't write your PIN number on your credit card** -- or have it anywhere near your credit card.

***Shield your credit card number** so that others around you can't copy it or capture it. People are using devices like cell phone cameras and other electronic equipment to capture your information. There is a scanning device that is being used to scan the information from your pocket/purse. This process is called "electronic pick pocketing". Cards or passports that contain a new technology called "RFID" (radio frequency identification technology) can be targeted. This technology allows you to simply wave your card in front of a device to pay. Secure sleeves and specially-lined wallets are available to protect yourself. Aluminum foil will also block the scanners. Lastly, if you carry two cards with RFID embedded in them, those signals could cancel each other, and possibly protect you from electronic pickpockets.

***Only carry around credit cards that you absolutely need**.

***Promptly report any charges** that you don't have a receipt for or recognize. This should also be done in writing to the credit card company.

***Shred** anything with your credit card number written on it like receipts, carbon paper and even incorrect receipts.

***Never sign a blank credit card receipt.** Carefully draw a line through blank portions of the receipt where additional charges could be fraudulently added.

***Don't write your credit card account number on a postcard** or so that it shows through the envelope payment window.

***Ideally, carrying your credit cards separately from your wallet** -- perhaps in a zippered compartment or a small pouch.

***Never lend a credit card to anyone**.

***If you move, notify your credit card issuers in advance of your change of address.**

***The nonfinancial personal information you reveal online is often enough for a thief.** Beware of seemingly innocent personal facts that a thief could use to steal your identity. For example, never list your full birth date on Facebook or any other social-networking website. Don't list your home address or telephone number on any website you use for personal or business reasons, including job-search sites.

*B**e alert to strangers** hovering around whenever using a credit card at an ATM or phone, and to avoid public wireless Internet connections unless their laptops or PDAs have beefed-up security protection.

***If an ATM or store terminal looks funny, don't use it.** As a general rule, the mouth of a card receptacle on an ATM machine should be flush with the machine or have only a very slight lip. If it looks or feels different when you swipe your card, or has an extra piece of plastic sticking out from the card slot, it may be a "skimmer". If you notice it after you've already inserted your card, you should alert your bank so they can watch for any fraudulent charges to your account.

***Identity theft insurance can pay off, but you need to read the fine print.** Several companies offer identity theft insurance, which covers the money you shell out to repair your identity. This includes whatever you spend on phone calls, making copies of documents and mailing them, hiring an attorney, and in some cases, lost wages. However, the insurance -- which costs about $50 a year -- does not reimburse you for funds you lost. Your current homeowner's policy may include identity theft insurance in your package, so check first before signing up with an outside company. Also, some companies are starting to offer identity theft insurance as an employee benefit.

No one is immune to identity or credit card theft, but a little knowledge about how thieves operate can help you stay a step ahead.

Joyce Gibson
Oklahoma State
2nd Vice President/Educational Director

Resources:
*Latoya Irby – About.com; *National Consumers Leagues Internet Fraud Watch;
*Audri and Jim Lanford - SCAMBUSTERS.ORG; *Lisa Rogak - CreditCards.com;
*Scott Stevenson, the founder and CEO of Eliminate ID Theft;
*Mark Cravens, the "anti-scam doctor"; *Sandy Shore, training manager with Novadebt;
*Justin Yurek, the president of ID Watchdog; *Lucy Duni, the VP of consumer education at TrueCredit; *Echo Montgomery Garrett, a writer; *Sarah Browne - Consultant