CREDIT CARDS

Guarding Against Fraud

- Do's:

- Sign your cards as soon as they arrive.
- Carry your cards separately from your wallet, in a zippered compartment, a business card holder, or another small pouch.
- Keep a record of your account numbers, their expiration dates, and the phone number and address of each company in a secure place.
- Keep an eye on your card during the transaction, and get it back as quickly as possible.
- Void incorrect receipts.
- Destroy carbons.
- Save receipts to compare with billing statements.
- Open bills promptly and reconcile accounts monthly, just as you would your checking account.
- Report any questionable charges promptly and in writing to the card issuer.
- Notify card companies in advance of a change in address.

- Don'ts:

- Lend your card(s) to anyone.
- Leave cards or receipts lying around.
- Sign a blank receipt. When you sign a receipt, draw a line through any blank spaces above the total.
- Write your account number on a postcard or the outside of an envelope.
- Give out your account number over the phone unless you're making the call to a company you know is reputable. If you have questions about a company, check it out with the Better Business Bureau.

If you think you've been the victim of fraud or a scam, immediately follow these steps. The faster you contact the proper authorities, the more likely you are to minimize the damage a scammer can do to your identity, your credit, and your bank account.

Step 1: Close any affected accounts

Contact the genuine company or organization if you believe you've given sensitive information to an unknown source masquerading as that real company or organization. If you contact the real company immediately, they might be able to lessen the damage to you and others. Then:

- **Speak with the security or fraud department** about any fraudulently accessed or opened accounts at every bank or financial institution you deal with, including credit card

companies, utilities, Internet service providers, and other organizations that have your personal information.
- **Follow up** with a letter and save a copy for yourself. When you open new accounts use strong passwords, not passwords such as your mother's maiden name, along with a new account number.

Step 2: Change the passwords on all of your online accounts

When you change your passwords or open new accounts, use strong passwords.

Step 3: Place a fraud alert on your credit reports

- In the United States, contact these three credit bureaus:
  - Equifax (800) 525-6285
  - Experian (888) 397-3742
  - TransUnion (800) 680-7289
- For each of the credit bureaus:
  - **Get a copy of your report** (victims of ID theft can receive copies of their credit reports for free) and ask that no new credit be granted without your approval.
  - **Make sure your account is flagged** with a "fraud alert" tag and a "victim's statement," and insist that the alert remain active for the maximum of seven years.
  - **Send these requests in writing** and keep copies for yourself.
  - **Review the reports carefully**. Look for things like inquiries you didn't initiate, accounts you didn't open, and unexplained debts.

Outside of the United States, you can contact your bank or financial institution, who can direct you to the relevant organization or agency.

Step 4: Freeze your credit reports

A credit freeze is a way to block your credit reports to make it a lot tougher for an identity thief to get a loan or open a credit account in your name. While a freeze is in place, no one - not even you! - can open an account in your name. Lenders, insurers and even employers doing background checks are not able to access your credit file.

You can have the freeze lifted, or "thawed," if you need to get new credit, but you have to give the bureaus a specially issued personal identification number and a few days' notice to do so.

You probably need to freeze your credit if:

- You've already been the victim of "new account" fraud. If someone stole enough information about you to open a credit card account or get a loan in your name, then you need to make sure such fraud doesn't happen again.

On the other hand, if the thief just swiped your credit card or credit card number, a freeze is definitely overkill. Just report the theft to your credit card issuer, fill out its paperwork and go on your way with your new card.

- You've been told that your personal identifying information has been compromised. More than 200 million personal records have been stolen, hacked into or otherwise compromised since the Privacy Rights Clearinghouse started keeping track in 2005. You probably don't need to bother with a freeze if thieves accessed a database that contained just your credit card number. Credit card fraud is relatively easy to catch and fix without long-term damage to your credit reports.

If you want to institute a credit freeze, follow the links to Equifax, Experian and TransUnion to find instructions on how to go about it.

Although several companies offer to place fraud alerts or freezes for you, it doesn't make much sense to pay others to do what you could do yourself for less (or for free, in the case of fraud alerts). Don't institute a freeze if you're about to be in the market for credit, and make sure your PIN is kept in a safe place so you can thaw the freeze when you want.

For more information, go to
http://www.consumersunion.org/campaigns//learn_more/003484indiv.html.

Step 5: Contact the proper authorities

In the United States, contact the Federal Trade Commission (FTC).

- **File a complaint.** If you are a victim of any type of identity theft, you can report the theft by calling the FTC's toll-free Identity Theft Hotline at (877) ID-THEFT or (877) 438-4338. Counselors will advise you on how to deal with the credit-related problems that can result from identity theft.
- **Download and print the FTC's Identity Theft affidavit.** Fill it out and send it to all the financial institutions at risk to help minimize your responsibility for any debts incurred by those who stole your identity. Your case will be entered in the FTC's nationwide "Consumer Sentinel" database of ID theft cases, which helps law enforcement agencies find criminal patterns and catch the thieves.
- **File a report with your local police department.** Get a copy of the police report to notify your bank, credit card company, and other creditors that you are a victim of a crime, not a credit abuser.

Step 6: Record and save everything

As you complete all these steps to clear up the wrongdoing, always make print copies of documents for yourself, including e-mail messages, written correspondence, and records of telephone calls, and file them somewhere safe.

For telephone or in-person conversations, follow up with dated confirmation letters to the organization, and save a copy for yourself. State in the letter what was covered in the conversation, and list any follow-up items that you or the representative have committed to in the conversation.

Source: http://www.ftc.gov/bcp/edu/pubs/consumer/credit/cre07.shtm and http://www.microsoft.com/protect/yourself/personal/fraud.mspx

Click on the links to below for the most information on Credit Cards.

- Avoid Credit Card Fraud
- 21 Ways to Protect Yourself from Credit Card Fraud
- Tips for Seniors to Protect Themselves from Credit Card Scams