Identity Theft Prevention

Karp Capital Management
Registered Investment Advisor

1. Don't publicly post anything you may use as a password such as your birth date, pet's name, mother's maiden name, or your alma mater. Identity thieves can use the information you post to guess your password.
2. Review your credit card statements. Make sure all the purchases are transactions you actually authorized.
3. Carefully watch your credit card when handing it to the clerk. Make sure you are given back your card and not a different card.
4. Pay attention to your monthly bills and follow up with creditors if one does not arrive on time. A missing credit card bill could mean an identity thief has changed your billing address to cover his or her tracks.
5. Put a fraud alert on your account. This will notify creditors to verify your identification before issuing credit in your name. A security freeze prevents potential creditors from accessing your credit report without your consent. The credit reporting company may charge a fee to place or remove a security freeze.
6. If you are moving, notify credit card companies and financial institutions in advance of any change of address or telephone number. Contact the sender if your statements are not received in the mail at the usual time.
7. Watch your mail. When a breach occurs and you were exposed, the company is required to send you a notification letter with an explanation and information on what to do. It may also offer a free credit monitoring service to help check your account and pay for the initial cost of a security freeze. These letters are easy to miss because they look like junk mail and may come from an unfamiliar third party service.
8. Several times a year, order your credit report from one or more of the national credit reporting agencies (Equifax, Experian, TransUnion.) You may obtain a free copy of your credit report once a year at www.freeannualcreditreport.com
9. If you use a wireless router, enable the encryption to scramble the data you send online.
10. Shred information containing sensitive information such as receipts, copies of credit applications, insurance forms, physician statements, bank checks and statements, expired charge cards, convenience checks, and credit offers. Clean the receipts out of your wallet and car several times a week.
11. Mail anything with personal information or payment at the post office, not from your mailbox.

If you suspect identity theft, there are a number of steps you should take:

* Notify the company about the data breach, as well as law enforcement authorities, all three credit reporting agencies, and the FTC.
* Keep up with all paperwork that involves your fraud case. You will probably be asked to provide corroborating evidence of the unauthorized transaction or identity theft. This includes a signed affidavit, law enforcement or governmental agency reports, receipts of expenses, and insurance declaration forms.