protect yourself FROM IDENTITY THEFT!

IDENTITY THEFT OCCURS when someone wrongfully uses your personal identification to obtain credit, loans, services, mortgages, or a job in your name. They may even commit crimes while impersonating you! Anything you can do with your identity can be done by the impostor.

IDENTITY THEFT is a frightening and overwhelming experience if it does happen to you. You may not know it is happening for months or years! It is my desire to help other people prevent the nightmare I have had to go through myself.

Please also know that the following protective measures will not guarantee that a criminal will not get access to your credit from a "less than cautious" credit grantor, an unscrupulous employee or a hacker. As you know, there are many ways to steal private information about you (i.e., anyone who has access to your social security number and other identifying information.) All of these offices have your information: Your bank, the IRS, your doctor, accountant, lawyer, loan officer, health insurance, schools, courts, etc. A shady employee of these people could steal your identity! Remember, you don't have to lose your wallet or have it stolen to become a victim of identity theft.

Here are some things you should do to protect your privacy, which will help to reduce the risk of Identity Theft.

PREVENTION:

1. Buy a cross-cut type shredder (Average cost $60-$70.) Shred all your important papers, pre-approved credit applications received in your name and other financial documents that provide access to your private information. Don't forget to shred your credit card receipts.
2. Be aware of "Dumpster Divers." Do not throw anything away that someone could use to become you. Anything with your identifiers must be shredded (cross-cut) before being thrown away.

womens FOCUS wichita

3. Be careful at ATM's and when using Phone Cards. "Shoulder Surfers" can get your pin number and gain access to your accounts. Don't use a debit card since you are not as protected as when you use a credit card. The money can be siphoned out of your bank account without your knowledge. With a regular credit card you receive a statement and have the opportunity to dispute fraud BEFORE it's paid.
4. If you use checks, have them delivered to your bank - not zyour home address. Use your initials, not your full name. Do not pay bills from your home. Drop them off at a U.S. Mailbox or the U.S. Post Office. Mail theft is common. It's easy to change the name of the recipient on the check with an acid wash.
5. Better yet – don't use checks! Your account and routing number can be copied to make up new checks, and the bank releases funds by using an automatic reader- so check fraud is rampant. It is better to pay on-line from your checking account directly to all your creditors (using at least 10-12 numbers and letters for your password).
6. When you order new credit cards, or your previous ones have expired, watch the calendar to make sure that you receive the card within the appropriate time. If it is not delivered by a certain date, call the credit card grantor and ask if the card was sent. Ask if a change of address was filed if you don't receive the card or a billing statement.
7. Cancel all credit cards that you do not use or have not used in 6 months. Thieves use these easily. Open credit is a prime target.
8. Put passwords on all your accounts and do not use your mother's maiden name. Make up a fictitious word that uses 10-12 letters and numbers
9. Get a post office box or a locked mailbox.
10. Ask all financial institutions, doctors' offices, etc., what they do with your private information and make sure that they shred it for your protection. Tell them you are concerned with privacy and ID theft. Don't give them your social security number unless they have a need for some IRS purpose.
11. Empty your wallet of all extra credit cards and social security numbers, etc. Do not carry your birth certificate, social security card, or passport, unless necessary. If you have an ID with your SSN, (you are in the military or have a Medicare card), copy your ID and blacken all but the last 4 numbers of your SSN and put the copy in your wallet.
12. Memorize social security numbers. Lock passwords in locking drawers. Encrypt sensitive data on your hard drive and portable electronic devices.
13. When anyone calls you at home or at work, (or you receive e-mail or regular mail which is unsolicited) and you do not know the person (even if you are told it is your bank), never give out any of your personal information. If they say they are a credit grantor of yours look the number up on your statement then call them back and ask for that party before discussing personal information. Provide only the facts that you believe are absolutely necessary.
16. Get credit cards and business cards with your photograph on them.
17. Do not put your credit card account number on the Internet unless it is encrypted on a secured site. (Your browser should have a padlock present and the address bar will read https://)

Never use a debit card on-line and don't give your checking account number on-line. Never put account numbers on the outside of envelopes, or on your checks.

18. When you are asked to identify yourself at schools, employers, or any other kind of institutional identification, ask to have an alternative to your social security number.
19. In conjunction with a credit card sale do not put your address, telephone number, or driver's license number on the receipt.
20. Monitor all your bank and credit card statements monthly, or more often if you do on-line banking. If there is anything that you do not recognize call the credit grantor to verify that it is truly yours.
21. Order your credit reports for free at www.annualcreditreport.com from each of the 3 major credit reporting agencies, Equifax, Experian, TransUnion. Review each line very carefully. If you see anything that appears fraudulent or erroneous, immediately put a fraud alert on your reports.
22. Immediately correct all mistakes on your credit reports in writing. Send those letters Return Receipt Requested. Include a copy of the report identifying the problems item by item. You should hear from them within 30 days.
23. Call the three credit reporting agency numbers to opt out of pre-approved promotional offers. (888) 567-8688 (888 5 opt out).

~ MARI FRANK, ESQ.

Author of Safeguard Your Identity (Porpoise Press). To learn more visit www.identitytheft.org. To listen to Mari's radio show visit www.kuci.org/privacypiracy

womens FOCUS wichita