PROTECT YOURSELF FROM IDENTITY THEFT!

Identity theft occurs when someone wrongfully uses your personal identification to obtain credit, loans, services, even rentals and mortgages in your name. They may even commit crimes while impersonating you! It is a frightening and overwhelming experience if it does happen to you. You may not know it is happening for months or years!

USEFUL PRIVACY INFORMATION

1. The next time you order checks, have only your initials (instead of first name) and last name put on them. If someone takes your checkbook, they will not know if you sign your checks with just your initials or your first name, but your bank will know how you sign your checks. Do not put your telephone number on your checks.

2. Get all of your checks delivered to your bank - not to your home address.

3. Do not put checks in the mail from your home mailbox. 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.

4. Do not sign the back of your credit cards. Instead, put “PHOTO ID REQUIRED”.

5. When you are writing checks to pay on your credit card accounts, DO NOT put the complete account number on the “For” line. Instead, just put the last four numbers. The credit card company knows the rest of the number and anyone who might be handling your check as it passes through all the check processing channels will not have access to it.

6. Do not put your credit card account number on the Internet (unless it is encrypted on a secured site.) Don't put account numbers on the outside of envelopes.

7. Never have your Social Security number printed on your checks. You can add it if it is necessary but if you have it printed, anyone can get it.

8. Memorize your Social Security number and take your original Social Security card out of your wallet.

9. Photocopy both sides of all licenses, credit cards, etc. that you carry in your wallet. If your wallet is stolen, you will know what you had in your wallet and all of the account numbers and phone numbers to call to cancel. Keep the photocopies in a safe place. The key is having this information handy so you can contact providers immediately.

10. Empty your wallet of all extra credit cards. Do not carry any identifiers you do not need. Don't carry your birth certificate, Social Security card, or passport, unless necessary.

11. If your wallet is stolen, do the following IMMEDIATELY:

a. File a police report in the jurisdiction where the wallet was stolen. This proves to credit companies you were diligent, and is the first step toward an investigation (if there ever is one).

b. MOST IMPORTANT: Call the three national credit reporting organizations immediately to place a fraud alert on your name and Social Security number. Also call the Social Security fraud line number. The alert means any company that checks your credit knows your information was stolen and they have to contact you by phone to authorize new credit.

Attached is a sample letter to send to the three credit reporting agencies. You may copy it for all three, fill in the blanks as applicable to you, and keep a copy for yourself. Make sure that you send it Return Receipt Requested and keep the postal receipt with your copy. It cannot be guaranteed that the three credit reporting agencies will honor these requests.

The Social Security Administration fraud line number is 1-800-269-0271.

Please also know that these protective measures will not guarantee that a criminal will not get access to your credit from a "less than cautious" credit grantor. 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 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.

In addition, here are some other things that you should do to protect your privacy, which will help to reduce the risk of identity theft.

1. Buy a cross-cut type shredder (you can purchase a cross-cut type shredder very cost effectively for approximately $60 - $70.) Shred all your important papers and especially pre-approved credit applications received in your name and other financial information that provides access to your private information. Don't forget to shred your credit card receipts.

2. Be careful of "Dumpster Diving." Make sure that you do not throw anything away that someone could use to become you. Anything with your identifiers must be shredded (cross-cut) before throwing away.

3. Be careful at ATM's and using Phone Cards. "Shoulder Surfers" can get your "Pin Number" and get access to your accounts.

4. When you order new credit cards in the mail, or your previous ones have expired, watch the calendar to make sure that you get the card within the appropriate time. If it is not received by a certain date, call the credit card grantor immediately and find out if the card was sent. Find out if a change of address was filed if you don't receive the card or a billing statement.

5. Cancel all credit cards that you do not use or have not used in 6 months. Thieves use these very easily - open credit is a prime target.

6. Put passwords on all your accounts and do not use your mother's maiden name. Make up a fictitious word.

7. Get a post office box or a locked mailbox, if you possibly can.

8. Ask all financial institutions, doctors' offices, etc., what they do with your private information and make sure that they shred it and protect your information. Tell them why.

9. When a person calls you at home or at work, and you do not know this person, never give out any of your personal information. If they tell you they are a credit grantor of yours call them back at the number that you know is the true number, and ask for that party to discuss personal information. Provide only information that you believe is absolutely necessary.

10. Do not put your Social Security number on your checks or your credit receipts. If a business requests your Social Security number, give them an alternate number and tell them why. They do not need that to identify you. If a government agency requests your Social Security number, there must be a privacy notice accompanying the request.

11. Get credit cards and business cards with your picture on them.

12. 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. Unfortunately, your health insurance carrier often uses your Social Security number as your identification number. Try to change that if you can.

13. In conjunction with a credit card sale do not put your address, telephone number, or driver's license number on the statement.

14. Monitor all your bank statements from every credit card every month. Check to see if there is anything that you do not recognize and call the credit grantor to verify that it is truly yours.

15. Order your credit report at least twice a year (The addresses are enclosed for you on the sample letter.) Review it carefully. If you see anything that appears fraudulent, immediately put a fraud alert on your reports by calling the numbers below.

16. Immediately correct all mistakes on your credit reports in writing. Send those letters Return Receipt Requested, and identify the problems item by item with a copy of the credit report back to the credit reporting agency. You should hear from them within 30 days.

17. Take your name off all promotional lists. Call the three credit reporting agency numbers to opt out of pre-approved offers.

Experian: (888) 397-3742
Equifax: (800) 525-6285
TransUnion: (800) 680-7289

Write to the following to get off promotional lists:

Direct Marketing Association Mail Preference Service P. O. Box 9008 Farmingdale, NY 11735	Direct Marketing Association Telephone Preference Service P. O. Box 9014 Farmingdale, NY 11735

18. Write to your State and Federal Legislators to demand stronger privacy protection. Also, ask that identity theft be considered a crime in your State. Demand that the State Finance and Banking Committees pass legislation to protect consumers from negligent bank and credit reporting practices.

19. Consider making your phone an unlisted number or just use an initial.

20. Make a list of all your credit card account numbers and bank account numbers (or photocopy) with customer service phone numbers, and keep it in a safe place. (Do not keep it on the hard drive of your computer if you are connected to the Internet.)

CREDIT LETTER

Date

CERTIFIED MAIL
RETURN RECEIPT REQUESTED

EQUIFAX Equifax Credit Information Services, Inc P.O. Box 740241 Atlanta, GA 30374	Order Report# (800) 685-1111 Fraud # (800) 525-6285
EXPERIAN (formerly TRW) P.O. Box 2104 Allen, TX 75013-2104	Order Report# (888) 524-3606 or (888) 397-3742 Fraud # (888) 397-3742
TRANS UNION CORPORATION TransUnion LLC Consumer Disclosure Center P.O. Box 1000 Chester, PA 19022	Order Report# (800) 888-4213 Fraud # (800) 680-7289

Re:	First, Last, Middle Name: Social Security No: Date of Birth:	Spouse Name: Social Security No: Date of Birth:

Dear Gentleperson:

In accordance with the Fair Credit Reporting Act and protection of my credit information, I respectfully request that you do the following immediately:

1. Provide me with my current credit report. (Enclosed is $_____.)
2. Please add a consumer alert to my credit file: **"Do not issue credit without calling me first at this phone number _____."**
3. Remove my name from any and all marketing mailing lists and promotions to <u>any</u> entity.
4. Do not change my mailing address or phone number without verification from me in writing.
5. My current address is:
6. My former address is:
7. My current phone number at my office is:
8. My current phone number at my home is:
9. Enclosed is a current utility bill to confirm.
10. Do not provide my credit report to anyone without my prior permission by phone, fax, or in writing. Please provide me whatever information is necessary to set up a secret password that I may use for telephonic communications.

If I do not hear from you otherwise in writing within ten (10) business days of receipt of this letter, I will assume that you unconditionally agree to all of the above.

Thank you for your prompt attention to this matter.

Yours truly