

***** SAFEGUARD YOUR INFORMATION AGAINST IDENTITY THEFT *****

Unfortunately, it's impossible to prevent identity theft and credit fraud entirely, but by managing your personal information carefully - and with a full understanding of its importance - you can substantially reduce the chances that it will happen to you.

There is some awesome information available at the Federal Trade Commission web site on ID Theft called "When bad things happen to your good name". <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>

1. BE CAREFUL ABOUT GIVING OUT PERSONAL INFORMATION. Never give anyone your credit card number, Social Security number, banking information or other personal information for a purpose you don't understand - ask to use other types of identifiers when possible. Always be very wary of calls made to you at home, work or on your cell phone requesting information. I would typically only give out sensitive information on calls that I have initiated.

2. PROTECT YOUR MAIL. Don't let a thief "dumpster dive" to get your personal information - tear or shred your charge receipts, bank statements, expired charge cards, and preapproved credit offers. Promptly remove mail from your mailbox after it's delivered. Think about getting a secure mailbox at home. If you plan to go away, call the Post Office and request a vacation hold on your mail. Possibly use a PO Box for all accounts that you have set up. I shred anything that has my name and address on it from any source. You never know what account information is on the address label from catalog companies, magazine subscriptions.

3. GUARD YOUR CREDIT CARDS. Minimize the information and the number of cards you carry in your wallet. If you lose a card, contact the fraud division of the credit card company. If you apply for a new credit card and it doesn't arrive in a reasonable period, contact the issuer. Also, when you receive a new card, sign it in permanent ink and activate it immediately. 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 won't have access to it. Make sure to not leave credit card receipts unattended when leaving a business. You don't want your credit card number and expiration date out there in any hands that it is not supposed to be.

4. PAY ATTENTION TO BILLING CYCLES. Contact creditors immediately if your bills arrive late or not at all. A missing bill could mean an identity thief has taken over your credit card account and changed your billing address or used other account information to gain another account or service using your information as reference.

5. SAFEGUARD PERSONAL INFORMATION IN YOUR HOME. Guard your personal information if you are having service work done in your home, employ outside help or have a roommate. Use a fire-proof lock box or safe. If you have information stored on your computer make sure it is encrypted (PGP) or remove it and store on a CD/Floppy for storage. I always recommend having a safety deposit box at your bank.

6. FIND OUT WHO HAS ACCESS TO YOUR INFORMATION AT WORK. Be sure to verify that records are kept in a secure location, and are accessible only to employees who have a legitimate reason to access them.

7. BE SMART ABOUT PASSWORDS AND PINS. Memorize your passwords and personal identification numbers instead of carrying them with you. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.

Password is NOT a 4-Letter Word:

Get more information at <http://www.user-groups.net/InfoManager/password.html>

8. COPY THE CONTENTS OF YOUR WALLET. Photocopy the front & back of all information and keep in a secure location. I actually have all of my information on my Palm in an encrypted password protected application. Have the account numbers, Expiration Dates, Customer Service phone numbers, secure CID number from the back of your credit cards. Think about if you ever lost your wallet! What information would

you need.

9. REMOVE YOUR SSN FROM YOUR DRIVER'S LICENSE. Have this removed the next time you get your license renewed. You will need to have your SS Card when you have anything done at the BMV.

10. ONLINE ACTIVITY AND EMAIL. Phishing – a growing Internet scam technique that tricks a user, per an e-mail notice, to visit a seemingly legitimate website and input personal information. Information is then used for fraudulent purposes, such as identity theft. Have you started to receive emails from various reputable institutions, asking you to visit a website that requests personal information, even if you don't have an account or services with that institution that supposedly sent the e-mail? Familiar companies like Citibank, USBank, PayPal, Ebay or even CoreComm. If so, then you've met the Internet's latest threat, called "phishing." The following tips can help you identify and avoid phishing scams:

- Never supply personal information via email request. If you get an email from a reputable organization that you believe may be fake, contact the organization using a telephone number you know to be genuine.
- Do not supply personal information on a website if the address does not start with "https:". The "s" indicates a secure connection to the website, however this method is not foolproof as some con artists may have fake security certificates. You also can look for the "Padlock" in your browser to know if it is a secure web site.
- Keep antivirus software current, and do not open attachments that you are not expecting. Some phishing emails contain viruses or software that is meant to track your Internet activities in secret.

You can get more details at the Anti-Phishing web site: <http://www.antiphishing.org/>

11. CHECK YOUR CREDIT REPORT REGULARLY. Checking your credit report can help you catch mistakes and fraud before they wreak havoc on your personal finances. Make sure your report is accurate and includes only those activities you've authorized. It's also a good idea to review your credit report from each of the three major credit reporting agencies every year -- it's possible that information is reported to one but not the others.

Equifax - <http://www.equifax.com>

Experian - <http://www.experian.com>

TransUnion - <http://www.transunion.com>

12. USE A CREDIT MONITORING SERVICE. I use Equifax Credit Watch™ for my monitoring service. Now there's a simple, automated way to help detect and protect against the impact of identity theft. Regularly checking your credit report for changes you did not make is one of the best ways to combat identity theft. Equifax Credit Watch™ makes monitoring your report easy by automatically alerting you within 24 hours of key changes in your Equifax Credit Report™ – like when someone tries to get credit in your name – so you can act before serious damage is done. And with credit card fraud being the most common type of identity theft, Equifax Credit Watch™ can now alert you to sudden changes in your credit card balances. Your service also includes your Equifax Credit Report™, identity theft insurance and access to live customer support.

RESOURCES ONLINE

Federal Trade Commission - Your National Resource for ID Theft

<http://www.consumer.gov/idtheft/>

Privacy Rights Clearinghouse - Identity Theft Resources

<http://www.privacyrights.org/identity.htm>

Identity Theft - Get free tips, tools and information

<http://www.fightidentitytheft.com/>

Identity Theft Resource Center

<http://www.idtheftcenter.org/index.shtml>

Identity Theft Prevention and Survival

<http://www.identitytheft.org/>

When Identity Crime Strikes You - Compliments of Ohio State Highway Patrol
<http://www.bmv.ohio.gov/IdentityFraud.html>