Protect Yourself and Your Identity

Your identity is a valuable commodity – you should make these and other basic precautions a part of your daily routine to help preserve the privacy of your personal information and protect yourself against identity theft.

Identity theft occurs when someone acquires and uses another person's personal information (such as their name, date of birth, Social Security number, driver's license number, residential address, credit card number, insurance information, employment information, or other identifying information) to take on their identity. Identity thieves may use your personal information to fraudulently obtain money, property, or services, or to commit other crimes falsely in your name.

By consistently protecting the privacy of your personal information, you can greatly reduce your risk of becoming a victim of identity theft. Here are some simple, basic suggestions to help protect yourself and your identity:

Keep your Social Security Card in a safe, private place and protect your Social Security number. Your Social Security number is a key to unlocking your identity. Keep your Social Security card and any other cards or documents that display your SSN in a safe, secure, and private location. Avoid providing your SSN to anyone that you don't know or trust or that does not have a true "need to know" that personal information.

Keep your personal information private. Think carefully and ask questions before you agree to provide your personal information to anyone, especially if you aren't certain who you are dealing with. Identity thieves may contact you by phone, email, text or postal mail and pretend to work for your bank, a utility company, a store, an internet services provider, or even a government agency – all in order to get access to your personal information. If you didn't initiate the communication or if you aren't sure who you are communicating with, don't divulge your personal information to them. Even if you do know who you're dealing with, you should only disclose the minimum amount of personal information that is necessary to conduct your personal business. You should ask how your personal information will be protected, used or shared. If you don't like the answers, don't provide your personal information. And remember, reputable businesses and institutions will not ask for sensitive personal information such as your social security number or credit card information over the phone, by email or text.

Check yourself on Social Media Sites, Apps, and Chats. Identity thieves troll the internet for personal information – including social media sites, apps, and chats. Think of public internet outlets, sites and apps as the front page of a national newspaper – your posts may inadvertently expose your personal information to identity thieves around the world. Check and limit all of your privacy settings and take the time to understand what personal information you may be divulging inadvertently through the sites and apps you use. Ask yourself, what could the wrong person do with this information before you post or upload a photo or video on social media.

Review your Credit Report Regularly. You should check your credit report at least annually for problems or for new accounts that you did not open. Every year you are entitled to a free copy of your credit report from each of the three credit reporting agencies: Equifax, Experian, and TransUnion. To get your free reports, visit: www.annualcreditreport.com or www.freecreditreport.com.

It's not trash to everyone. Identity thieves often root through trash to obtain personal information. Make sure you shred or destroy any documents containing your personal information before disposing of them. This includes credit card offers and unused "convenience checks."

Check your bills and bank statements. Review your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call your bank

or credit card issuer if your bills or statements fail to arrive on time. It may mean that someone has stolen your identity and changed your contact information on the accounts to hide fraudulent charges.

Stop pre-approved credit offers. Pre-approved credit card offers and “convenience checks” are prime targets for identity thieves. You can have your name removed from credit bureau marketing lists by calling 888-5OPTOUT (888-567-8688).

Limit your online shopping to stores you know well. Some retail websites are fronts for identity thieves. Make sure you know the company you are dealing with when you shop online. Stick to online retailers you can trust. Carefully check out a shopping site before entering your personal information. Read the privacy policy for the site and take opportunities to opt out of information sharing. Only enter personal information on secure Web pages that encrypt your data in transit. You can often tell whether a page is secure if "https" is in the URL or if there is a padlock icon on the browser window.

Protect your devices and email accounts. Protect personal information on your electronic devices and in your email accounts by following good security practices. Use strong, non-easily guessed passwords (for example, do not include things like birth dates, nicknames, or pet names in your passwords). Use regularly-updated firewall, anti-virus, and anti-spyware software on your devices. Download software, pictures, videos and other files only from sites you know and trust and only after reading all the terms and conditions. Delete suspicious emails or other messages without opening them first. Don't click on links in pop-up windows or in spam or other suspicious emails.