Useful Tips to Protect Your Identity

To minimize your risk of becoming a victim of identity theft, be very careful with your personal information.

Here are a few important suggestions regarding common circumstances faced throughout the day:

You're Bank Statement

- Review your bank and credit card statements monthly for signs of suspicious activity. Immediately contact the company if an item looks suspicious.
- If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.

You're Car

- Do not leave any personal information in your car.
- If your car is broken into, report it to the police immediately.
- When buying a new car from a private individual, make sure the title and registration match the name and address of the person selling the car.
- Be cautious of a seller with no fixed address, place of employment, or phone number.

You're Computer

- Do not keep computers online when not in use. Either shut them off or physically disconnect them from Internet connection.
- Use anti-virus software and a firewall, and keep them up to date. Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them. These files can contain viruses or other software that can weaken your computer's security.
- If you get an email or pop-up message that asks for personal or financial information, do not reply. And don't click on the link in the message, either.

You're Credit Cards

- Do not hand over your ATM/Debit Cards or Credit Cards to anyone.
- Cancel all unused credit card accounts. Even though you do not use them, their account numbers are recorded on your credit report.
- Avoid paying by credit card if you think the business does not use adequate safeguards to protect your personal information.

You're Credit Report

- Check your credit reports from the three major credit bureaus, Equifax, Experian and TransUnion, at least twice a year and correct any inaccuracies.
- Order a copy of your credit report. An amendment to the federal Fair Credit Reporting Act requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit reports, at your request, once every 12 months. To order your free annual report from one or all the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through www.annualcreditreport.com
- Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, and Vermont already have free access to their credit reports.

You're Financial Accounts

- When you open new accounts, place passwords on them.
- Add passwords to your credit card, bank and telephone accounts that are not the typical passwords, such as the last four digits of your Social Security number, your birth date, your mother's maiden name, your phone number, or a series of consecutive numbers. If you are opening a new account that requests your mother's maiden name, use a password instead.

You're Home

- Secure personal information in your home, especially if you have roommates, employ outside help, or are having work done.
- If your house or car was broken into, report it to the police immediately.

Mail

- Deposit your outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox.
- If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.
- When ordering new checks, pick them up from the bank instead of having them mailed to your home mailbox.
- Remove your name from mailing lists by contacting the Direct Marketing Association at:

Mail Preference Service
Attention: Dept.9301235
Direct Marketing Association
P.O. Box 643
Carmel, NY 10512

- Opt out of receiving offers of credit in the mail by calling: 1-888-5-OPTOUT (1-888-567-8688) or through the following website: www.optoutprescreen.com. The three nationwide consumer reporting companies use the same toll-free number to let consumers choose not to receive credit offers based on their lists.
- Note: You will be asked to provide your Social Security number which the consumer reporting companies need to match you with your file.

Phone Offers

- Be cautious when responding to promotions. Identity thieves may create phony promotional offers to get you to give them your personal information.
- Be wary of anyone calling you to "confirm" personal or financial information. Often, these are criminals trying to obtain those facts under the guise of "confirmation".
- Stop receiving unsolicited calls. You may do so by contacting the National Do Not Call Registry either by phone at 1-888-382-1222 or online at https://www.donotcall.gov/. The registration is free of charge and is effective for five years.
- Never give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact or you are sure you know who you're dealing with. Identity thieves are clever, and have posed as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information.
- Before you share any personal information, confirm that you are dealing with a legitimate organization. Call the company back using a phone number from a statement or from the telephone book (not a phone number the person who is calling gives you). You may check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly.

You're Social Security Number

- Before providing identifying information, especially your Social Security number, ask if the information is required. Give your Social Security number only when absolutely necessary and ask to use other types of identifiers.
- Remove your Social Security number from any identification you carry, such as checks, a driver license or your health insurance card. Both your health insurance company and the Department of Motor Vehicles will give you a new number if you request it.
- If you ask, only the last four digits of your Social Security number will appear on your credit reports.

You're Trash

- Treat your trash carefully.
- To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, tear or shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail. Preferably use a crosscut shredder, which cuts paper into confetti like pieces instead of strips.

You're Wallet

- Carry only one or two credit cards in your wallet.
- Carry only the identification information that you'll actually need when you go out.
- Do not carry your Social Security card in your wallet; leave it in a secure place.
- If your purse or wallet is stolen, report it to the police immediately.

You're Workplace

- Secure personal information in your workplace. Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information such as your paycheck.
- Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information.
- Find out who has access to your personal information and verify that records are kept in a secure location. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.
- Ask about the disposal procedures for those records as well.

Four Biggest Myths about Identity Theft

- Internet use puts you at greater risk for identity theft. Actually, 90% of data compromise takes place offline, meaning most victims can pinpoint the source of the identity compromise. The #1 source for identity theft is still lost/stolen wallets or purses, credit cards, and checkbooks, comprising 30% of identity theft cases.
- You are helpless to protect yourself. In over 60% of identity theft cases, the point of compromise is by someone the victim knows (coworker, acquaintance, employee, etc.). The thieves get the information from home computers, mail, wallets/purses, or credit cards. These sources are easy to protect, and you can fairly easily control whom you grant access to this information.
- Identity theft is rare; it won't happen to me. Identity theft is not so rare anymore. With 10 million victims per year, the chances are higher and higher that identity theft could happen to you.
- The elderly have to worry the most about identity theft. Although vulnerable populations like the elderly and minors do have to guard against identity theft, the demographic with the highest identity theft rates is actually the 25-34 year old bracket. This age range also has a higher average fraud amount compared to the elderly, meaning identity theft is more severe with this age demographic.

Identity Theft Safety Tips

Supplement your identity theft protection investment by following these safety tips:

- Don't give out your social security number or account information
- Carry in your wallet or purse only the credit cards you need
- Shred all documents containing sensitive information before discarding
- Store documents with identifying information in a secure, locked location
- Replace paper bills with paperless options
- Make passwords to accounts complicated and change them often
- Don't place checks in your mailbox-take them directly to the post office
- Review your bank and credit card statements regularly
- If you do not receive bills or statements on time, contact your lender immediately
- Talk to your creditors about their zero-liability policies, if they have them
- Immediately report any suspected fraud

How to Guard Against Identity Theft - Tips and Advice

Identity theft occurs when somebody steals vital pieces of personal information, e.g. your social security, credit card numbers, etc. and uses that information for financial gains by taking your identity. The most common form of identity theft involves credit card and mortgage frauds. But it can also be used for vicious crimes like drug dealings, terrorism, etc.

You may be surprised to know that many minor identity thefts are committed by someone you know. So, don't make it an easy job for a person to steal your personal information from your wallet, checkbook, etc. Avoid leaving things containing your personal information lying around for others to have easy access to that information.

How you can guard against Identity Theft

It must be stated here that there are no guarantees that the steps you take will prevent your identity from being stolen. Personal information is available from sources (including government, employment and other business records) that we are not in a position to personally protect. However, there are things you can do to guard against identity theft, such as:

1. **Don't carry your SSN in your wallet or purse.** Social Security Numbers, birth certificates, passports or any other personal identification should not be carried in your wallet. The same goes for extra credit cards and store or gas credit cards. The less you carry the less risk if your wallet is stolen or lost.
2. **Stop pre-approved credit offers.** You can stop the mailing of pre-approved credit offers by calling toll-free 888-5OPTOUT (888-567-8688). Ask to have your name removed from the list as pre-approved credit offers can be easily abused by thieves.
3. **Put passwords on your credit cards.** Credit card companies like Visa offer added protection by allowing you to create a password along with the card number when making a purchase. Even if your card is stolen you can prevent thieves from using it by having it password protected.
4. **Shred, shred, shred.** Buy a cheap paper shredder from an office supply store and shred all your paid bills, used check books, etc. before tossing those into the trash. Put aside 30 minutes every Saturday morning for shredding anything that contained your personal information and you intend to trash. Make it a habit.
5. **Pick up the mail EVERY day.** Don't allow mail to sit overnight in the mail box or you give thieves an easy target. Credit card offers, bank statements and possibly information with your SSN can be used to open new credit in your name or steal from you.
6. **Never give out your personal information like your social security number; birth date etc. over the phone when the call you received is unsolicited.** Your financial institutions have those information and they will not ask you for that. Sometimes, for verification purposes, they make ask you the last four digits of your social security number.
7. **Don't pay to get anybody to get a copy of your credit report.** Because of a congressional mandate, all three-credit report bureaus will give you a copy of your credit report for free every year. Go to AnnualCreditreport.com to obtain your free credit report every year from TransUnion, Equifax, and Experian. While obtaining your free credit report, these bureaus will push some paid services. Just ignore those.
8. **Don't get your free credit reports from the three bureaus all at the same time.** Then you have to wait one year before you can get your reports again for free. In the mean time, some unwanted stuff may show up in your report. Get your free report every four months from each bureau. If you are using a PDA, password protect it to prevent others from accessing it.
9. **Phishing is a popular method to steal sensitive information by email. Don't be a phishing victim. Avoid clicking on any link that comes to your way through e-mails or IM.** The e-

mail will disguise itself coming from your financial institutions (your bank or PayPal accounts) and will urge you to click a link to verify your accounts or resort to such other tricks. Sometimes, it can be outright threatening. If you click the link you will end up in the thief's website. And if you enter your user name and password, the thief will have enough information to log into your actual account.

10. **Open online accounts for all your credit cards and financial accounts.** Online accounts are not only convenient for faster bill paying, paperless transactions, etc.; they also help monitor your accounts frequently, instead of waiting for the monthly bill or statement to arrive. Monitor your accounts online every week and if you see any suspicious charges, checks, etc., call you banks immediately. Also setup e-mail based account alerts, if available, to alert you when charges are made to your accounts.
11. **If possible, avoid putting your outgoing mails containing bills and checks in your mailboxes for easy access by a thief**. Drop them in mailboxes located in the post office or street corners. Better yet, setup online bill payment with your bank and avoid the snail mail for bill paying.
12. **You also need to keep your computer safe.** Thieves can get into computers through spyware and unsecured wireless or network connections. **Use anti-spyware programs and turn on your Windows default personal firewall program.** To prevent viruses infecting your computer, use an anti-virus program. Setup accounts for each user of your computer and ask them to use strong passwords that include a combination of letters and numbers. Also, when you dispose of your computer, always destroy the hard drive.
13. **Another way to prevent anybody, including you, from opening any credit in your name is to freeze your credit.** This option is not available in all states. If it is available in your state and you opt for this option, you need to lift the block before you allow anybody, e.g. an employer for a new job, creditor for a car loan, etc., to access your credit information. Though it is almost like a foolproof system to prevent identity theft, it is the also the most inconvenient method.

What Steps Can Individuals Take to Avoid Becoming a Victim?

To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps you can take. These steps correspond to the acronym SCAM. This acronym stands for "**Stingy**, **Check**, **Ask**, and **Maintain**".

- **STINGY**: Be stingy about giving out your personal information to others unless you have a reason to trust them, regardless of where you are. Adopt a "need to know" approach to your personal data. If you are traveling, have your mail held at your local post office or ask someone you know well and trust to collect and hold your mail while you're away. Shred and destroy unwanted documents that contain personal information. Furthermore, deposit mail in U.S. Postal Service collection boxes.

- **CHECK**: Check your financial information regularly. Look for what should be there and what should not. You should be receiving monthly statements. If you're not, call the financial institution or Credit Card Company immediately and inquire. If you are told that your statements are being mailed to another address, tell them you did not authorize the change of address and that someone may be improperly using your accounts. Obtain copies of all statements since the last statement you received to help in determining whether or not some of those transactions were fraudulent. Review your statements closely

to make sure there are no unauthorized transactions. Contact your financial institution or Credit Card Company immediately if there are any unauthorized transactions.

- **ASK**: Periodically ask for a copy of your credit report from credit reporting ureaus such as Equifax, Experian, or TransUnion. Your credit report should list all bank and financial accounts under you name.

- **MAINTAIN**: Maintain careful records of your banking and financial accounts. You should retain your monthly statements and checks for at least one year, if not more. If you need to dispute a particular transaction, your original records will be more immediately accessible and useful to the institutions that you have contacted.

Other steps you can take to avoid identity theft include the following: Sign new credit cards immediately and write “Ask for ID” on them. Watch cashiers closely. Watch anyone who handles your checks or plastic cards. Memorize your social security number and passwords. Do not use your date of birth as your password and do not record passwords on papers you carry with you. When using an ATM, be aware of your surroundings, i.e., someone attempting to get your PIN number. Also, be wary of the machine itself. Check to make sure that the machine has not been retrofitted with a skimming device that would capture the details of the transaction. Never leave transaction receipts at ATM machines, gas stations or points of sale.