## CHECKLIST TO HELP PREVENT IDENTITY THEFT

**Help prevent all types of identity theft**

1. Use a paper shredder to destroy financial documents or other documents with personal information, including receipts, credit applications, and bank statements.
2. Don't carry your Social Security card with you or write it on a check. Place the card in a safe place, and only give your number out when absolutely necessary. Consider asking to use another identifier for accounts.
3. Don't share personal information with anyone you don't trust. Before sharing it with businesses or at the workplace, ask why they need it, how they will safeguard it, and the consequences of not sharing. If you aren't comfortable with their answer, take your business elsewhere.
4. Don't over-share on social networking sites. If you post too much information about your life, identity thieves can piece together enough information to answer "challenge" questions on your accounts, and possibly access your bank accounts or even construct a false identity that mirrors your life. Consider limiting access to your networking page to only a small group of people. Never post information that could identify you, like your Social Security number or even your full name, on websites that the public can access. Don't post the year of your birth if you decide to post your birthday.
5. Change your passwords every 60 days and make them "strong" (more difficult to "crack") by using a combination of upper case, lower case, numbers, and symbols. Avoid using your birth date, mother's maiden name, last four digits of your Social Security number, family names, or other obvious identifying words or numbers.
6. Order a free copy of your credit report from each of the three credit bureaus each year: Experian, Transunion, and Equifax. It contains information about what credit accounts have been opened in your name, as well as where you live and work, how you pay your bills, if you've been sued, arrested, or filed for bankruptcy. You are entitled to one free report each year from each of the three major bureaus, for a total of three free credit reports. Consider spreading these three reports out over the year so that you can review an up-to-date, free credit report once every few months.

7. Watch your billing cycles closely. If a bill is late, check with your creditors to see why it has not arrived, and watch for any unauthorized charges or unexpected account statements.
8. Have your mail sent to a post office box or get a locking mailbox. Also take outgoing mail to the post office. When you travel, have a trusted friend pick up your mail.
9. Only use a secure connection on the Internet when sending credit card numbers or other personal information. The website should begin with "https" instead of just "http," because the "s" means "secure."
10. Use virus protection and a firewall program to prevent your computer from being accessed by others, and keep them up to date. Run your virus scan on a regular basis. Don't download files or click on links from unknown sources. Instead, type in a web address you know. Also, unplug or close your Internet connection when you're not using it.
11. Keep your personal information in a secure place at home, especially if you have roommates, and employ only trusted outside help if you are having work done at your home.
12. Opt out of pre-approved credit card offers and receive fewer solicitations at home by calling 888-567-8688 or visiting www.optoutprescreen.com.
13. Destroy the labels on prescription bottles before you throw them away. Don't share your health plan information with anyone offering free health services or products.
14. Stay on the lookout for suspicious behavior and occurrences, such as unusual email or impersonators asking for your personal information. If you're not absolutely certain you're speaking with a real employee, do not give out any of your personal information. Instead, hang up and call them directly. These concepts also apply to email. Do not be tricked into sending personal information to a fake business or someone you do not know. Companies you do business with will not ask you for personal information by email. Do not open email from people or companies that you do not recognize.
15. Password protect your cell phone and other devices. It's easy to lose your cell phone. And if a criminal gets it, your cell phone provides an easy way to commit identity theft with the apps and other information it stores.
16. Before you sell or dispose of a computer or mobile device, get rid of all the personal information it stores. For computers, use a wipe utility program to overwrite the entire hard drive. For mobile devices, check your owner's

manual, the service provider's website, or the device manufacturer's website for information on how to delete information permanently, and how to save or transfer information to a new device. Remove the memory or subscriber identity module (SIM) card from a mobile device. Remove the phone book, lists of calls made and received, voicemails, messages sent and received, organizer folders, web search history, and photos.

17. Read any notices that are sent to you by mail that describe the way your data might have been exposed in a data breach.

**Extra steps to help prevent medical identity theft**

18. Make sure you've taken all steps above to "Help prevent all types of identity theft."
19. Remember that your medical and insurance information are very valuable to identity thieves, so do not hand it out unnecessarily.
20. Don't share medical or insurance information by phone or email unless you initiated the contact and know who you're dealing with.
21. Be suspicious of people offering "free" health services or products, especially if they ask you to provide your health plan ID number or other insurance information. Medical identity thieves may pretend to work for an insurance company, doctor's office, clinic, or pharmacy to try to trick you into revealing your personal information.
22. Keep paper and electronic copies of your medical and health insurance records in a safe place. Shred outdated health insurance forms, medical statements, receipts, and the labels from prescription bottles before you throw them out.

**Extra steps to help prevent tax fraud identity theft**

23. Make sure you've taken all steps above to "Help prevent all types of identity theft."
24. File your tax returns as early as possible.
25. Request a Personal Identification Number, or PIN, from the IRS. This can help prevent scammers from filing a federal return in your name. Other PIN numbers help consumers make secure payments on amounts owed to the IRS.

26. Consumers with questions about whether a contact from the IRS is authentic should call the IRS toll-free number (1-800-829-1040) to confirm.
27. Keep copies of all your tax records in a secure location.
28. Check your credit reports and other records for accuracy. Check your banking records daily or weekly.
29. Report the improper use of your Social Security number to the Social Security Administration at their fraud hotline (1-800-269-0271).

This information was adapted from the Federal Trade Commission by the Office of the Missouri Attorney General.