# Suggested Steps to Reduce Your Vulnerability to Identity Theft

## Protect Your Personal Information

- **At home and at work, secure important documents that contain your personal information where they are protected from unwanted view or access.**
- **Carry only the necessary cards and identifying information in your purse or wallet. Limit the number of credit cards and checks that you carry. Don't carry PIN numbers with your cards.**
- **Sign your credit and debit cards when you receive them.**
- **Pick up receipts from ATMs, restaurants, stores, and gasoline pumps. Don't leave them lying around.**
- **Watch out for shoulder surfers watching you type in your PIN number at the cash register or ATM.**
- **Safeguard your Social Security number.**
  - **Do not carry your Social Security card in your wallet.**
  - **Do not pre-print your Social Security number on your checks or driver license, and do not use it on an unsecured web site.**
  - **Ask why someone wants your Social Security number and how it will be protected before deciding to give it out. (Financial institutions will require it before they can provide products and services.)**
- **Protect your mail.**
  - **Deposit outgoing mail that contains personal information in a U.S. Postal Service blue collection box, hand it to a letter carrier, or take it to the Post Office if you can. If you place outgoing mail in your own mail box for the letter carrier to pick up, don't use the red flag to draw attention to the waiting mail.**
  - **Remove incoming mail promptly from your mail box and consider some kind of lock mechanism to keep thieves out. Have the Post Office hold your mail if you are going away.**
- **Use strong passwords to protect access to your sensitive information and financial accounts.**
  - **Don't create passwords using easy to guess or easy to obtain personal information, like birthdates or a pet's name. Make the passwords unique – e.g., mix letters with numbers and symbols. Change your passwords from time to time.**
- **Outsmart the "dumpster diver" by shredding documents containing sensitive information before throwing them out.**
- **Destroy expired or unneeded credit, debit, or ATM cards so that the numbers and magnetic strip cannot be read.**

# Suggested Steps to Reduce Your Vulnerability to Identity Theft

## Be Alert, Be Careful

- **Check your consumer reports (i.e., credit reports) annually at least, and before making a major purchase like a home or car. Dispute and remove errors or unknown accounts in the reports.**
- **Check bank and credit card statements and bills regularly. Report unauthorized transactions immediately and then in writing.**
- **Contact your financial institution if your regular statements or bills don't arrive on time to see whether they were mailed, or possibly intercepted or diverted to another address.**
- **Be cautious about sharing your information. Generally, refrain from giving personal information and account information out to others – via phone, fax, mail, or e-mail -- if you have not initiated the communication in the first place.**
- **Choose your tax preparer very carefully, if you don't prepare your own tax return.**
- **If the Internal Revenue Service (IRS) sends you a letter that leads you to believe someone may have used your Social Security number fraudulently, contact the IRS immediately as directed.**
- **Read a company's privacy and security policy in order to understand how your personal information will be used, disclosed, and protected.**

## Added Tips for Online Safety

- **Install a firewall on your computer.**
- **Use anti-virus, anti-spam, and anti-spyware software. Keep the software updated.**
- **Use parental controls to protect children from unwanted spam and phishing e-mails.**
- **Keep your browser updated.**
- **Don't respond to requests for personal information from unsolicited e-mails or pop-up windows.**
- **Visit a web site by entering the web address – or "URL" – yourself into your web browser, not by clicking a link in an e-mail.**
- **When downloading a program, game, etc., reading the provider's statement of terms will let you know what else you might be downloading that you may not want.**
- **Check that you use secure web sites for sensitive communications or transactions. When entering the URL, look for the "s" in the "https" and the lock icon in the bottom right of the screen.**
- **Clean the hard drive before discarding any personal computer.**

# What To Do If You Are, Or Think You Are or May Become, a Victim of Identity Theft

## What the Experts Recommend

- **Report lost or stolen credit, debit or ATM cards to financial institutions immediately and then in writing.**

- **Report unauthorized card transactions that show up on your monthly statements immediately; however, you also must write to the creditor at the address given for "billing inquiries," not the address for sending your payments, and include your name, address, account number, and description of the billing error.**

- **Contact your or the pertinent financial institution if you find that a thief has taken over an existing account, like a checking account, or established new accounts in your name without your knowledge. Follow up the complaint in writing.**

- **Contact the three nationwide consumer reporting agencies (i.e., credit bureaus) – Equifax, Experian, and TransUnion – to place a fraud alert in your file.**

  - **One call to any one of them will be sufficient. The company you call is required to contact the other two, which will place an alert in their versions of your file, as well.**

- **Obtain a free copy of your credit report from each of the three nationwide consumer reporting agencies once you place the fraud alert. Check it carefully and dispute any errors or unauthorized accounts promptly.**

- **Keep good records of all of your communications and any evidence of identity theft that you obtain.**

- **Contact law enforcement and file a police report. You will be able to use the report to help clear up the record from the identity theft.**

- **Active duty military personnel deployed away from their regular duty station may place an Active Duty Alert in their file for 12 months (renewable). This signals lenders to take a little extra care before issuing credit to someone claiming to be the deployed service man or woman. One call to Equifax, Experian, or TransUnion is sufficient. The company you call is required to contact the other two, which will place an alert in their versions of your file, as well.**

- **Report the incident(s) to the Federal Trade Commission (FTC), which keeps track of reported crimes and shares the information with law enforcement throughout the country. The FTC also has information and materials that may help victims of identity theft in their efforts to restore their identity. www.consumer.gov/idtheft**