

Steps to Safeguard Your Identity

Your identity is one of your most valuable assets. Identity Theft is the misuse of another individual's personal information to commit fraud. Today, 1 out of every 10 Americans is the victim of identity theft, many of them unsuspecting senior citizens.

Just the Facts

Your personal information criminals are most interested in:

- ✓ Name, address, & phone number
- ✓ Date of Birth
- ✓ Social Security Number (perhaps the most valuable piece of information for a thief)
- ✓ Driver's license number
- ✓ Credit card information
- ✓ Bank account information
- ✓ Mother's maiden name

Travel Light

- ✓ Do not carry your Social Security card in your wallet. Only carry identification you absolutely need when you go out.
- ✓ Never carry more than two credit or debit cards
- ✓ Keep a list of all your credit cards, bank accounts, and investments in a secure place. Include account numbers, expiration dates and phone numbers for customer services departments so you can contact them quickly, if necessary.

Just Say No

- ✓ Be wary of unsolicited telephone calls. Unless you have a relationship with the person, business or agency, and you initiated the call and have verified the other party's authenticity, NEVER offer any personal information. This includes your Social Security Number, credit card number, and other personal data.
- ✓ To avoid unwanted telephone offers, add your name to the National Do-Not-Call registry at www.fcc.gov/cgb/donotcall.

Shred It

- ✓ A large majority of identity theft is the result of stolen mail or items found in the trash. Shred any solicitations that contain your name, address, or other sensitive data.
- ✓ When away from home for more than a few days, have your mail held at the postoffice.

- ✓ Always shred pre-approved credit card offers. You can remove your name from these permanent offer lists by visiting www.optoutprescreen.com or calling 1-888-567-8688.
- ✓ Do not leave outbound mail that contains personal check in an unsecured mail box

Don't Bank On It

- ✓ Review your credit card statements, bank statements, and phone bills frequently for unauthorized use.
- ✓ If using online banking or an app, review your accounts at a minimum of once a week to check for unauthorized use. The quicker you spot it and contact the appropriate company, the quicker you can protect yourself.
- ✓ Never let merchants write your Social Security Number on your checks.
- ✓ Do not print your Social Security Number, driver's license number, or home phone number on your check. A P.O. Box is preferable.
- ✓ Check your Social Security statement each year for signs of fraud.
- ✓ Cut up expired credit cards before you dispose of them.
- ✓ Check your credit reports, at least once a year. You are entitled to 1 free report a year. Details can be found at www.annualcreditreport.com.

Internet Precautions

- ✓ Use email alerts for your online banking to notify you of account activity such as transactions, balance thresholds, and account transfers
- ✓ Do not provide credit card numbers or personal information on any website unless you are positive it is authentic
- ✓ Never open spam or other email from unknown sources as they can contain viruses. If you aren't sure if it's spam, err on the side of caution and delete it without opening.
- ✓ Never use the last 4 digits of your Social Security Number, your mother's maiden name, your birth date, your child's name, or your pet's name for your password.
- ✓ If an institution uses the last 4 digits of your Social Security Number as a PIN, change it.
- ✓ Use a combination of capital letters, small letters, numbers, and special characters to create your passwords
- ✓ Change your passwords on a regular basis

6 Easy Steps If Your Identity Is Stolen

1. Contact the 3 major credit bureaus. Ask them to place a fraud alert on your credit report. Order copies of your credit reports and review for fraud activity.

A. Equifax

www.equifax.com

To order your report: 1-800-685-1111

To report fraud: 1-800-525-6285

TDD: 1-800-255-0056

B. TransUnion

www.transunion.com

To order your report: 1-800-888-4213

To report fraud: 1-800-680-7289

TDD: 1-977-553-7803

C. Experian

www.experian.com

To order your report: 1-800-EXPERIAN (397-3742)

To report fraud: 1-800- EXPERIAN (397-3742)

TDD: 1-800-972-0322

2. Notify your bank(s) and credit card companies & follow up in writing. If your checks are stolen, stop payment at once. Call SCAN at 1-800-262-7771 to determine if bad checks have been passed in your name. If your accounts have been compromised, close them immediately.
3. Keep a record of the names and phone numbers of the people with whom to you discuss your case, as well as all the reports and supporting documents.
4. File a report with your local police department. Request a copy of the police report as it is one of the two documents that comprise what is known as an Identity Theft Report. Some creditors will request this report in order to remove the debts created by the theft.
5. File a complaint with the Federal Trade Commission at 1-877-438-4338. The completed complaint is called an FTC Affidavit and is the 2nd document needed for your Identity Theft Report. The FTC also has counselors to help you resolve financial and other problems that can result from this crime.
6. Visit <https://www.identitytheft.gov/> to create a detailed personal recovery plan

Other Helpful Federal Agencies

U.S. Postal Service: www.usps.com/postalinspectors; 1-877-876-24553

U.S Department of Justice: <https://ojp.gov/programs/identitytheft.htm>

Federal Deposit Insurance Corporation: www.fdic.gov/consumers; 1-877-275-3342