

What You Need to Know About Identity Theft

Identity theft is the fastest growing crime in America. Criminals who gain access to simply a few pieces of valid personal information can impersonate another and enable them to commit various types of fraud, including taking over a victim's financial accounts, opening new bank accounts, purchasing cars or opening credit cards and running up large debts. Your credit can quickly be damaged and efforts to correct these problems can become a nightmare.

The identity thief has many ways to gain access to your personal information. It can be obtained from uncollected mail sitting in your mail box, personal information carelessly thrown in the garbage, dishonest retail or restaurant employees or through the theft of your pocketbook or wallet. When thieves assume your identity they often rent a mailbox at a packaging center, fill out a change of address card using the new address, obtain new identification and open new charge or loan accounts.

There are several ways you can help prevent becoming a victim to identity theft and to minimize the damage if were to happen. The following tips should provide a guideline in minimizing risk and/or the effects of identity theft.

Identity Theft Prevention Tips

There are a number of things you can do to minimize the chances that you will become a victim of identity theft.

- Shred all bills, credit card charge receipts, credit applications, insurance forms, bank statements, expired charge cards, and pre-approved credit offers before throwing them into the garbage.
- Do not provide personal information simply because someone asks for it or because it is asked for on a form, questionnaire or product registration card.
- Do not carry your social security card in your purse or wallet or give out your social security number freely.
- **NEVER** have your social security number printed on your checks, drivers license or other financial documents. If a bank, health care provider or other entity uses your social security number for client or account identification, call or write that company and ask that a different identification number be issued. See "*Who can require my Social Security Number?*" section.
- Promptly remove mail from your mailbox. If going on vacation, make arrangements for someone to take the mail for you or call the U.S. Postal Service at 1-800-275-8777 and request a "vacation hold" for your mail.
- Place outgoing mail in post office collection boxes or at your local post office.
- **NEVER** provide personal identifying or financial information over the telephone when you did not initiate the call. This includes callers selling goods and services as well as charitable solicitors. Banks, credit card companies, telephone companies and other

legitimate creditors do not call to "verify" account numbers or to ask for your social security number or other personal information.

- **NEVER** provide personal identifying or financial information over the telephone to anyone claiming to represent a contest or sweepstakes promotion. It is illegal to market a foreign lottery in the United States. These calls are always fraudulent.
- Don't carry extra credit cards in your wallet or pocketbook. Cancel the ones you no longer use.
- Order credit bureau credit reports once a year to check for fraudulent activity, credit cards or loans you don't remember opening or other discrepancies. See "*Free Annual Credit Report*" section.
- Sign all new credit cards upon receiving them in the mail.
- Save all credit card receipts and match them against your monthly bill.
- Never leave receipts at an ATM, store counter, self-serve gas pump or in trash cans. Keep track of all paperwork and destroy those you no longer need.
- Memorize your social security number and passwords. *Never* write them down and carry them in your wallet or pocketbook.
- Keep track of when routine financial statements should arrive in the mail.
- Contact the issuing bank or company, if one doesn't arrive. Review statements to verify all charges.
- Never loan anyone your credit cards.
- If a credit card you applied for doesn't arrive in a timely fashion, notify the issuing bank. Also keep track of expiration dates on your cards. If the new card doesn't arrive notify the issuing bank.
- Notify all banks and credit card companies of any change of address.
- Never put bank account or credit card numbers on the outside of an envelope or postcard.
- Beware of telephone solicitations asking for personal information about your accounts or your social security number.
- When disclosing credit card, checking account or other financial data online, use caution. Make sure you receive a secured authentication key (lock icon) and a statement that indicates your transaction is secure.
- Be cautious of e- mails and instant messages that are unsolicited and request you to confirm credit card numbers, passwords or other personal information. Con artists often pose as agents of banks, on-line shopping services or internet providers attempting to obtain this information to commit fraud.
- Financial institutions may share your information with other companies. If you want, you can limit some of that sharing. Each year, your financial institutions should send you a privacy notice with instructions for "opting out." Read these notices carefully.

Also, when establishing accounts with new companies, ask about privacy policies and make your wishes known.

- The credit bureaus offer a toll- free number that enables you to “opt-out” of having pre-approved credit offers sent to you for two years. Call 1-888-5-OPTOUT (567- 8688) for more information.
- Remove your name from national direct mail advertising lists. To do this, send your name and address with a written request to: DMA Mail Preference Service, ATTN: Dept. 12059580, Direct Marketing Association, P.O. Box 282, Carmel, NY 10512.
- The Federal Government has created the National Do Not Call Registry. To register, or to get information, visit www.donotcall.gov, or call 1-888-382-1222 from the phone you want to register. You will receive fewer telemarketing calls within three months of registering your number. It will stay in the registry for five years or until it is disconnected or you take it off the registry. After five years, you will be able to renew your registration.

What to do if you become a victim

- Contact all creditors, by telephone and in writing, to inform them of the situation.
- Notify the local police department.
- Alert all banks to flag your accounts and to contact you for unusual activity. Change all passwords and PIN numbers.
- Document all contacts and keep copies of all correspondences.
- Contact the Social Security Administration Fraud Hotline at 1-800-269-0271.
- Contact the Department of Motor Vehicles to have a new license number issued in your name.
- Call the Federal Trade Commission's identity theft hotline at 1-877-438-4338 and file a complaint or go to their website www.ftc.gov .
- If you are the victim of identity theft, call each credit bureau with a national database and ask to have a “Fraud Alert/Victim Impact” statement placed in your credit files. Also request that all creditors contact you before they open any new accounts in your name. The following contact information is provided to assist identity theft victims:
 1. Equifax www.equifax.com 1-800-685-1111
 2. Experian www.experian.com 1-888-397-3742
 3. Trans-Union www.tuc.com 1-800-916-8800
- If you are a victim of check fraud, you should contact the following:
 1. Telecheck 1-800-710-9898
 2. Equifax 1-800-437-5120

Who Can Require Your Social Security Number?

Your SSN is probably the most frequently used record-keeping number in America. Many people assume that they are required to give their SSN whenever and by whomever asked.

That is not true.

The following is a list of who can require your SSN:

- **Government tax and welfare agencies.** For example:
 - The IRS
 - Other federal agencies (for health benefits and other entitlements)
 - State/local tax or revenue agencies
- **State motor vehicle departments.** Colorado law prohibits the recording of your SSN on your drivers license or state identification card.
- **State professional/occupational/recreational licensing agencies.**
- **Other governmental agencies.** Under federal law, they must tell you why your SSN is needed, whether giving your SSN is mandatory or voluntary, and how your SSN is to be used.
- **Employer.** They can require it for wage/tax purposes, but NOT from a job applicant.
- **Banks and securities brokerages.** Under the USA Patriot Act, 31 U.S.C. § 5318, financial institutions are required to establish minimum standards for properly identifying their customers opening new accounts (include checking, savings, loans, safe deposit boxes, and/or investments). Under federal regulations adopted in May 2003, banks, savings associations, credit unions, securities broker-dealers, futures commissions merchants, and mutual funds were required to have Customer Identification Programs (“CIPs”) in place by October 1, 2003. Information required to identify customers under a CIP includes name, date of birth, address, and a social security or federal tax identification number.

Requests by businesses. Federal law does not prohibit a merchant or other business from requesting your SSN. However, there is no state or federal law that requires you to provide your SSN to any entity not authorized by law to require it. Businesses, private agencies, etc., are free to request your SSN and use it for any purpose that does not violate state or federal law.

- For example, retail stores, prospective landlords, prospective employers, utility companies, and other service providers often ask you your SSN, but they do not need to and you are not required to give it. They can do a credit check or ID their customers by alternative means.
- Insurers, hospitals and doctors also typically request your SSN, although no law requires that you give it to them (except for Medicaid and Medicare recipients).

No obligation to provide SSN – or services. Again, you can refuse to give your SSN to any merchant or other business. However, that merchant or other business is free to decline your business if you refuse to disclose your SSN.

Giving your SSN to purchase goods or services is voluntary. Even if requested from a government agency, consider the following questions:

- Am I required by some law to provide my SSN?
- Why do they need my SSN?
- How will they use my SSN?
- Will they share my SSN with other businesses or agencies?
- What happens if I refuse to give them my SSN?
- Are there alternative means of identification they will accept?

Free Annual Credit Report

By law, you may now obtain free copies of your credit report from each of the three nationwide consumer reporting companies by calling 1-877-322-8228 or through their annualcreditreport.com website.

If you desire to send in your request by mail, you may download the request form from the site, complete it and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

You can receive a free report from each of the three national credit reporting companies every 12 months. Please do not contact the companies individually as they are providing free annual credit reports only as outlined above.

Annualcreditreport.com is the **ONLY** authorized online source for you to obtain this free credit report under federal law. Be aware that some other sites claim to offer "free" credit reports, but may charge you for another product if you accept a "free" report.

Additionally, if you choose to order your reports through the website, make sure you are not transmitting personal data on a publicly accessed computer. Also, your computer should have an up-to-date firewall and virus protection. Make sure that your operating system and web browser are updated as well.

For more information on Identity Theft, please visit the Federal Trade Commission's Website at www.FTC.Gov.