An Overview of Identity Theft
Identity theft is a serious crime. It occurs when personal information, such as your name, Social Security number or credit card, is used without your knowledge to commit fraud or other crimes. Identity theft can cost you time and money, destroy your credit and ruin your good name.

Identity thieves may rent an apartment, obtain a credit card or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn’t make — or until you’re contacted by a debt collector.

While some identity theft victims can resolve their problems quickly, others spend hundreds of dollars and many hours repairing damage to their good name and credit record. Some consumers victimized by identity theft may lose out on job opportunities, or be denied loans for education, housing or cars because of negative information on their credit reports. In rare cases, they may even be arrested for crimes they did not commit.
To minimize your risk of becoming a victim of identity theft, simply remember SCAM.

**S**

Be STINGY when it comes to giving out your personal information, unless you trust the person asking.

Adopt a “need to know” approach to your personal information. For example, limit the information you have printed on your personal checks. Do not include your Social Security number or home telephone number.

If someone calls to offer you a credit card, a prize or other valuable item but asks for personal data such as your Social Security number, credit card number or mother’s maiden name, ask the person to send you a written application form. If he or she won’t do that, say you’re not interested and hang up. If you do receive an application, review it carefully to make sure it’s going to a company or financial institution that’s reputable. Check to see what businesses have received complaints with the Better Business Bureau.

**C**

CHECK your financial information regularly.

Monthly statements for bank and credit card accounts should list transactions for the most recent reporting period. Always check these statements carefully. This is the quickest way to find out if unauthorized debits or credits are being made to your accounts.

If you’re not receiving monthly statements for accounts you use, contact your financial institution or credit card company. If the statements are being mailed to another address that you didn’t provide, let them know right away that someone may be improperly using your accounts.

If someone is making withdrawals, charges or opening accounts in your name, contact your financial institution or credit card company immediately to report these transactions and to ask for the bank to take action.

**A**

ASK for a copy of your credit report routinely.

The Federal Trade Commission (FTC) encourages consumers to review their credit reports every year. Clear up misinformation as soon as possible to keep from jeopardizing your credit rating or stalling your application for any credit purchase.

You can get one free credit report a year from each of the three major credit bureaus by visiting AnnualCreditReport.com. This is a free site that will not ask for your credit card number or try to sell you additional services.

Your credit report should list all accounts under your name and will provide evidence if someone has opened or used any accounts wrongfully.

**M**

MAINTAIN careful records of your banking and financial accounts.

Retain monthly statements and checks for at least one year. This way, if you need to dispute any transaction, especially one that claims to bear your signature, your personal records will be more immediately accessible and useful to the institutions.
Tips to Keep Your Private Information Secure

**Keep your Social Security card secure.**
- Never carry your Social Security card in your wallet.
- Be cautious of anyone asking for your Social Security number. If they refuse to complete a transaction without it, consider taking your business elsewhere.

**Limit the information you put on checks.**
- Don’t preprint your Social Security number or your driver’s license number on your checks.
- Don’t pre-print your full name on checks. Use only your initials and last name. If someone takes your checks, they will not know if you sign your checks with just your initials or your full name, but your bank will know. If you have one, list a P.O. box on your checks instead of your home address.
- Don’t print your phone number on your checks.
- Unless required by the creditor, don’t write complete credit card numbers on the check when paying bills. Just use the last four numbers.

**Keep your credit cards safe.**
- Make sure new cards arrive in a timely manner and sign them as soon as you receive them.
- Keep a record of your account numbers, expiration dates and contact information of each company in a secure place.
- Consider cancelling cards that you haven’t used in the past six months.
- Never lend your card to anyone.
- Shred old cards when you dispose of them.
- Carry only cards you think you’ll need.

**Keep your mail safe.**
- Install a locking mailbox or a mail slot that goes directly into your house.
- Send your mail, especially payments, directly from the post office (don’t put it in the mailbox for the postal carrier to pick up).
- If your bank allows, pick up your new checks from the bank instead of having them sent to your home.
Guard your passwords and PINs.
- Change your passwords and PINs (Personal Identification Numbers) regularly.
- Don’t use common codes like birthdays or the name of your spouse, child or pet. Memorize passwords and your PIN and shred any piece of paper on which they are written.

Shred or tear up personal information when you throw it away.
- Always take your credit card receipts and never throw them away in public.
- Tear up or shred any offers for pre-approved credit cards you don’t intend to use and beware of offers from companies you don’t recognize.

Don’t give personal information over the phone unless necessary.
- Never give personal information unless you made the phone call.
- If someone calls and says they are calling from your bank or credit company, ask for a number to return the call. Make sure it’s an official number before calling back.

Guard your information online.
- Don’t put personal information on a computer home page or personal computer profile.
- Be careful about the type of information you put in social media.
- If you find your personal information posted on the internet, demand that it be removed.
- Update your virus protection software routinely. Use a firewall program and a secure browser.
- Don’t reply to pop-up or spam messages on your computer.
- Be cautious about opening attachments and downloads.
- Delete personal information when you dispose of a computer. Use a “wipe” utility program that overwrites the entire hard drive and makes the files unrecoverable.

Review credit card statements, phone, and utility bills monthly.
- Call the company if you don’t recognize a charge or phone call.
Take the following steps as soon as you suspect you may be a victim of an identity theft issue.

### What Do I Do If My Identity Is Stolen?

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1.   | **Place a fraud alert on and review your credit reports.** The alert tells creditors to follow certain procedures before they open new accounts in your name or make certain changes to your existing accounts. You can place an initial 90-day fraud alert by contacting one of the three nationwide credit reporting companies. (A call to one company is sufficient.)  
  - Experian: 888-EXPERIAN (397-3742) ([experian.com/fraudalert](http://experian.com/fraudalert))  
  - TransUnion: 800-680-7289 ([transunion.com/fraud](http://transunion.com/fraud))  
   Placing a fraud alert allows you to get free copies of your credit reports. Look for inquiries from companies you haven’t contacted, accounts you didn’t open and debts on your accounts you can’t explain. |
| 2.   | **Close any account you believe has been tampered with or opened fraudulently.** Call the security or fraud department of each company. It’s important to follow up in writing, and include copies of supporting documents. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Other tips include:  
  - Use the Identity Theft Affidavit at [identitytheft.gov](http://identitytheft.gov) to support your written statement.  
  - Ask the company holding your account to verify in writing that the disputed account has been closed and the fraudulent debts discharged.  
  - Keep copies of all documents and records of your conversations about the theft.  
  - When you open new accounts, use new PINs and passwords. Avoid using easily available information like your mother’s maiden name, your birth date, the last four digits of your Social Security number or your phone number.  
   **Tip!** Review other accounts you have, such as credit card and bank accounts or insurance policies: they may include identity theft benefits or services. |
   • Use the online complaint form at [ftccomplaintassistant.gov](http://ftccomplaintassistant.gov).
   • Call the FTC’s Identity Theft Hotline 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261

4. File a police report. This will provide proof of the crime to creditors who may request it. You may want to provide a printed copy of your online FTC complaint form to the police to incorporate into their police report.

5. Monitor your credit report quarterly, or even more frequently, if desired, until the problem is resolved. Then return to monitoring it annually.

Consider placing a credit freeze, which takes more stringent actions than a fraud alert, with the three major credit reporting bureaus — Equifax, Experian and TransUnion — until the problem is resolved.

**Tip!**

**What should I do if I’ve done everything advised and I’m still having problems?**

There are cases where people do everything right and still spend years dealing with problems related to identity theft. The good news is that most people can get their cases resolved by being diligent, assertive and organized. Remember:

- Don’t procrastinate on contacting companies to address the problems.
- Don’t be afraid to go up the chain of command or make complaints, if necessary.
- Keep organized files.
- If you haven’t filed a complaint with the FTC or updated it, you should do so and provide details of the problems that you are having.
- If your problems are the result from a failure of a party to perform its legal obligations, you may want to consult an attorney who specializes in such violations.
Take Control with ARAG

If you are the victim of identity theft and need an attorney or have questions about what to do, ARAG can help. Visit ARAGlegal.com to learn more about how ARAG legal coverage gives you an affordable way to manage legal matters.

Other Resources

Department of Justice
justice.gov

Federal Trade Commission
identitytheft.gov

Equifax Credit Information
Services Consumer Fraud Division
P.O. Box 740241
Atlanta, GA 30374-0241
888-766-0008
equifax.com/CreditReportAssistance/

Experian’s National Consumer Assistance
P.O. Box 2002
Allen, TX 75013
888-397-3742
experian.com/fraud/center.html

TransUnion’s Fraud Victim Assistance Department
P.O. Box 2000
Chester, PA 19022-2000 8
800-680-7289
fvad@transunion.com
transunion.com/fraud

This publication is provided as educational material only. While every effort has been made to ensure the accuracy of this publication, it is not intended as legal advice as individual situations will differ and should be discussed with an expert and/or lawyer.

By clicking on the links provided you are connecting to another website. We have provided links to these sites for information that may be of interest to you. These links and any opinions, products, services or any other sites contained therein are not endorsed by ARAG. ARAG is not responsible for the legality or accuracy of the information contained therein, or for any costs incurred while using this site.

© 2018 ARAG North America, Inc.