

Free Credit Report:

Consumers are entitled to one free credit report from each of the three major credit reporting agencies each year. These reports can be obtained:

- www.annualcreditreport.com
- 1-877-322-8228

Do Not Call Registry

Eliminate most unwanted solicitation calls by registering your phones on the Do Not Call List:

- www.donotcall.gov
- 1-888-382-1222

If you have an established business relationship with an organization they are exempt from the Do Not Call List. However if you specifically request that the organization remove you from their call list, then the company may be subject to a fine up to \$11,000 if they call you again.

Political organizations, charities and telephone surveyors are also exempt from the Do Not Call List. However if you specifically request that the organization remove you from their call list, then the organization may be subject to a fine up to \$11,000 if they call you again.

Opt Out of Pre-Approved Credit Card Offers:

Consumer Reporting Agencies (credit bureaus) regularly provide your information to insurers and creditors for the purpose of sending you (the consumer) pre-approved insurance and credit offers. Under the Fair Credit Reporting Act (FCRA), you have the right to have your name removed from these lists or “Opt Out.”

- www.optoutprescreen.com
- 1-888-567-8688

DETER

While nothing can guarantee that you won't become a victim of identity theft, you can minimize your risk, and minimize the damage if a problem develops, by making it more difficult for identity thieves to access your personal information.

Protect your Social Security number

Don't carry your Social Security card in your wallet or write your Social Security number on a check. Give your Social Security number only when absolutely necessary, and ask to use other types of identifiers. If your health insurance company uses your Social Security number as your policy number, ask to substitute another number.

Your employer and financial institutions will need your Social Security number for wage and tax reporting purposes. Other businesses may ask you for your Social Security number to do a credit check if you are applying for a loan, renting an apartment, or signing up for utilities. Sometimes, however, they simply want your Social Security number for general record keeping. If someone asks for your Social Security number, ask:

- Why do you need my Social Security number?
- How will my Social Security number be used?
- How do you protect my Social Security number from being stolen?
- What will happen if I don't give you my Social Security number?

If you don't provide your Social Security number, some businesses may not provide you with the service or benefit you want. Getting satisfactory answers to these questions will help you decide whether you want to share your Social Security number with the business. The decision to share is yours.

Treat your trash and mail carefully

To thwart an identity thief who may pick through your trash or recycling bins to capture your personal information, always shred your charge receipts, copies of credit applications, insurance forms, physician statements, checks and bank statements, expired charge cards that you're discarding, and credit offers you get in the mail.

To opt out of receiving prescreened offers of credit in the mail, call: 1-888-5-OPT-OUT (1-888-567-8688).

Note: You will be asked to provide your Social Security number which the consumer reporting companies need to match you with your file.

Deposit your outgoing mail containing personally identifying information in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox. If you're planning to be away from home and can't pick up your mail, contact the U.S. Postal Service at 1-800-275-8777 or online at www.usps.gov, to request a vacation hold. The Postal Service will hold your mail at your local post office until you can pick it up or are home to receive it.

Be on guard when using the Internet

The Internet can give you access to information, entertainment, financial offers, and countless other services but at the same time, it can leave you vulnerable to online scammers, identity thieves and more. For practical tips to help you be on guard against Internet fraud, secure your computer, and protect your personal information, visit www.OnGuardOnline.gov.

Verify an on-line merchant's authenticity and reputation by visiting the Better Business Bureau's website, www.bbbonline.org

Select intricate passwords

Place passwords on your credit card, bank, and phone accounts. 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, a series of consecutive numbers, or a single word that would appear in a dictionary. Combinations of letters, numbers, and special characters make the strongest passwords. When opening new accounts, you may find that many businesses still ask for your mother's maiden name. Find out if you can use a password instead.

Verify a source before sharing information

Don't give out personal information on the phone, through the mail, or on the Internet unless you've initiated the contact and are sure you know who you're dealing with. Identity thieves are clever, and may pose as representatives of banks, Internet service providers (ISPs), and even government agencies to get people to reveal their Social Security number, mother's maiden name, account numbers, and other identifying information.

Before you share any personal information, confirm that you are dealing with a legitimate organization. Check an organization's website by typing its URL in the address line, rather than cutting and pasting it. Many companies post scam alerts when their name is used improperly. Or call customer service using the number listed on your account statement or in the telephone book.

Safeguard your purse and wallet

Protect your purse and wallet at all times. Don't carry your Social Security number or card; leave it in a secure place. Carry only the identification information and the credit and debit cards that you'll actually need when you go out.

Store information in secure locations

Keep your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house. Share your personal information only with those family members who have a legitimate need for it. Keep your purse or wallet in a safe place at work; do the same with copies of administrative forms that have your sensitive personal information.

Ask about information security procedures in your workplace or at businesses, doctor's offices or other institutions that collect your personally identifying information. Find out who has access to your personal information and verify that it is handled securely. Ask about the disposal procedures for those records as well. Find out if your information will be shared with anyone else. If so, ask how your information can be kept confidential.

What is a credit freeze?

Washington State has laws that let consumers “freeze” their credit – in other words, letting a consumer restrict access to his or her credit report. If you place a credit freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. This means that it’s unlikely that an identity thief would be able to open a new account in your name. Placing a credit freeze does not affect your credit score – nor does it keep you from getting your free [annual credit report](#), or from buying your credit report or score.

Please refer to the Washington State Attorney General’s website for more information regarding Washington’s Credit Freeze by visiting www.atg.wa.gov/freezecharts

What does a credit freeze *not* do?

While a credit freeze can help keep an identity thief from opening most new accounts in your name, it’s not a solution to all types of identity theft. It will not protect you, for example, from an identity thief who uses your existing credit cards or other accounts. There are also new accounts, such as telephone, wireless, and bank accounts, which an ID thief could open without a credit check. In addition, some creditors might open an account without first getting your credit report. And, if there’s identity theft already going on when you place the credit freeze, the freeze itself won’t be able to stop it. While a credit freeze may not protect you in these kinds of cases, it can protect you from the vast majority of identity theft that involves opening a new line of credit.

What’s the difference between a credit freeze and a fraud alert?

A [fraud alert](#) is another tool for people who’ve had their ID stolen – or who suspect it may have been stolen. With a fraud alert in place, businesses may still check your credit report. Depending on whether you place an initial 90-day fraud alert or an extended fraud alert, potential creditors must either contact you or use what the law refers to as “reasonable policies and procedures” to verify your identity before issuing credit in your name. However, the steps potential creditors take to verify your identity may not always alert them that the applicant is not you.

A credit freeze, on the other hand, will prevent potential creditors and other third parties from accessing your credit report at all, unless you lift the freeze or already have a relationship with the company. Some consumers use credit freezes because they feel they give more protection. As with credit freezes, fraud alerts are mainly effective against new credit accounts being opened in your name, but will likely not stop thieves from using your existing accounts, or opening new accounts such as new telephone or wireless accounts, where credit is often not checked. Also, only people who’ve had their ID stolen – or who suspect it may have been stolen, may place fraud alerts. In [some states](#), anyone can place a credit freeze.

About identity theft insurance

Although identity theft insurance won’t deter identity thieves, it can, in certain circumstances, minimize losses if an identity theft occurs. As with any product or service, as you consider whether to buy, be sure you understand what you’d be getting. Things to consider include: (1) the amount of coverage the policy provides; (2) whether it covers any lost wages (and, if so, whether there’s a cap on the wages you can claim, or a separate deductible); (3) the amount of the deductible; (4) what might be excluded (for example, if the thief is a family member or if the thief made electronic withdrawals and transfers); (5) whether the policy provides a personal counselor to help you resolve the problems of identity theft; and (6) whether your existing homeowner’s policy already contains some coverage. Be aware that one of the major “costs” of identity theft is the time you will spend to clear your name. Also be aware that many companies and law enforcement officers will only deal with you (as opposed to an insurance company representative). So, even if your policy provides you with a personal counselor, that counselor can often only guide you, as opposed to doing the work to clear your name. And, as you evaluate insurance products and services, you may also consider checking out the insurer with your local Better Business Bureau, consumer protection agency and state Attorney General.

DETECT

The best way to detect identity theft is to monitor your accounts and bank statements each month, and check your credit report on a regular basis.

What are the signs of identity theft?

Stay alert for the signs of identity theft, like:

- Accounts you didn't open and debts on your accounts that you can't explain.
- Fraudulent or inaccurate information on your credit reports, including accounts and personal information, like your Social Security number, address(es), name or initials, and employers.
- Failing to receive bills or other mail. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.
- Receiving credit cards that you didn't apply for.
- Being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason.
- Getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

How do you find out if your identity was stolen?

Unfortunately, many consumers learn they their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts or debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

What personal information should I monitor regularly?

Early detection of a potential identity theft can make a big difference. Keep an eye out for any suspicious activity by routinely monitoring:

Your financial statements: Monitor your financial accounts and billing statements regularly, looking closely for charges you did not make.

Your credit reports: Credit reports contain information about you, including what accounts you have and how you pay your bills. The law requires each of the major nationwide consumer reporting agencies to provide you with a free copy of your credit report, at your request, once every 12 months. If an identity thief is opening credit accounts in your name, these accounts are likely to show up on your credit report. To find out, order a copy of your credit reports.

Once you get your reports, review them carefully. Look for inquiries from companies you haven't contacted, accounts you didn't open, and debts on your accounts that you can't explain. Check that information, like your Social Security number, address(s), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. Continue to check your credit reports periodically, especially for the first year after you discover the identity theft, to make sure no new fraudulent activity has occurred.

How do I get my free annual credit reports?

An amendment to the federal [Fair Credit Reporting Act](#) requires each of the major nationwide consumer reporting companies to provide you with a free copy of your credit report, at your request, once every 12 months.

To order your free annual report from one or all the national consumer reporting companies, visit www.annualcreditreport.com, call toll-free 877-322-8228, or complete the Annual Credit Report Request Form and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. You can print the form from ftc.gov/credit. Do not contact the three nationwide consumer reporting companies individually; they provide free annual credit reports only through www.annualcreditreport.com, 877-322-8228, and Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Under federal law, you're also entitled to a free report if a company takes adverse action against you, such as denying your application for credit, insurance or employment, and you request your report within 60 days of receiving notice of the action. The notice will give you the name, address, and phone number of the consumer reporting company that supplied the information about you. You're also entitled to one free report a year if you're unemployed and plan to look for a job within 60 days; you're on welfare; or your report is inaccurate because of fraud. Otherwise, a consumer reporting company may charge you up to \$9.50 for any other copies of your report.

To buy a copy of your report, contact:

Equifax Consumer Fraud Division 800-525-6285 PO Box 740256 Atlanta, GA 30374	TransUnion Fraud Victim Assistance Dept. 800-6807289 PO Box 6790 Fullerton, CA 92834	Experian National Consumer Assist. 888-397-3742 PO Box 9530 Allen, TX 75013
--	--	---

Should I use a credit monitoring service?

There are a variety of commercial services that, for a fee, will monitor your credit reports for activity and alert you to changes to your accounts. Prices and services vary widely. Many of the services only monitor one of the three major consumer reporting companies. If you're considering signing up for a service, make sure you understand what you're getting before you buy. Also check out the company with your local Better Business Bureau, consumer protection agency and state Attorney General to see if they have any complaints on file.