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 state uses your Social Security number as your driver's license number, ask to substitute another number. Do the same if your health insurance company uses your Social Security number as your policy 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.

back to top

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.

back to top

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.

back to top

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.

back to top

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.

back to top

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.

back to top

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.

back to top

What is a credit freeze?

Many states have 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.

Credit freeze laws vary from state to state. In some states, anyone can freeze their credit file, while in other states, only identity theft victims can. The cost of placing, temporarily lifting, and removing a credit freeze also varies. Many states make credit freezes free for identity theft victims, while other consumers pay a fee – typically $10. It's also important to know that these costs are for each of the credit reporting agencies. If you want to freeze your credit, it would mean placing the freeze with each of three credit reporting agencies, and paying the fee to each one.

You can find more information about credit freeze laws specific to your state by clicking here, including information on how to place one.

back to top

Who can access my credit report if I place a credit freeze?

If you place a credit freeze, you will continue to have access to your free annual credit report. You'll also be able to buy your credit report and credit score even after placing a credit freeze. Companies that you do business with will still have access to your credit report – for example, your mortgage, credit card, or cell phone company – as would collection agencies that are working for one of those companies. Companies will also still be able to offer you prescreened credit. Those are the credit offers you receive in the mail that you have not applied for. Additionally, in some states, potential employers, insurance companies, landlords, and other non-creditors can still get access to your credit report with a credit freeze in place.

back to top

Can I temporarily lift my credit freeze if I need to let someone check my credit report?

If you want to apply for a loan or credit card, or otherwise need to give someone access to your credit report and that person is not covered by an exception to the credit freeze law, you would need to temporarily lift the credit freeze. You would do that by using a PIN that each credit reporting agency would send once you placed the credit freeze. In most states, you'd have to pay a fee to lift the credit freeze. Most states currently give the credit reporting agencies three days to lift the credit freeze. This might keep you from getting "instant" credit, which may be something to weigh when considering a credit freeze.

back to top

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.

back to top

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.

back to top

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.