



ID Theft & Account Fraud

About Identity Theft

What is identity (ID) theft?

ID theft refers to crimes in which someone uses another individual's personal information, such as name, Social Security number, birth date, mother's maiden name or other identifying information, to commit fraud. In many cases, the thief steals an identity to commit financial fraud, such as borrowing money or making purchases on accounts opened in the victim's name. Thieves often default on the payments and leave the victim to clean up the mess. Another form of fraud is account fraud—this is the use of someone else's existing accounts, such as credit cards or bank accounts, to make unauthorized purchases or withdrawals.

In 1998, the Identity Theft and Assumption Deterrence Act made identity theft a federal crime. For information about laws specific to your state, visit your [state Attorney General's website](#).

How can someone steal my identity?

Identity thieves use many methods to get your personal information. Crooks continually come up with new ways to steal the information they need, which means that you have to be on constant alert to outsmart them. Some of the ways they can get the information they need include:

- stealing your mail or completing change of address forms to divert your mail to another location.
- "dumpster diving" in trash bins for documents that contain your data.
- "shoulder surfing"—watching or listening as you punch in your password or PIN or say your credit card number.
- stealing your unattended wallet, purse, backpack, mobile device or laptop computer.
- finding the information in your home.
- hacking into your computer or redirecting you to bogus websites, where you unsuspectingly enter your information.
- enticing you to respond to "phishing" emails, which attempt to trick you into revealing your confidential information. Phishers often send emails that appear to be from a real bank, credit card company or online merchant—just to trick you into going online and typing in your private information such as account numbers, usernames, PINs and passwords. Then the crooks take the information and go online and pretend to be you so that they can withdraw money from your bank account or make fraudulent charges on your credit cards.
- using the telephone to capture your account numbers and PIN codes. This is called "voice phishing," or "vishing" for short. You are sent an email, but instead of being asked to click on a link to go online, you are asked to call a phone number. Typically the email

will say there is trouble with your account and you have to call to straighten it out. But the number is not legitimate and your personal information is captured as you enter it into the fraudulent phone system.

- stealing records from businesses, schools and other organizations that have information about you in their database.

Can children have their identity stolen?

Yes. Though children under 18 make up only a small percentage of victims, anyone with a Social Security number (SSN) is vulnerable. Children are attractive targets because they can be easy marks and are much less likely to detect the crime.

For this reason, it's important for parents to keep their eyes open for signs of identity theft, not only for themselves but for their children as well. They should request a free credit report for their children whenever they check their own report. Generally speaking, young children won't have a credit report. If you find a credit report on file for your child, contact the credit bureau to discover how it was created and check it carefully and regularly.

How can I spot an identity thief?

Identity thieves can be difficult or impossible to recognize. They don't need to carry weapons, use force, or even have direct contact with victims.

Many identity thieves do not know the individuals they steal from. However, in many cases, the thief is closely connected to the victim—a co-worker, neighbor, roommate or household employee. Particularly in cases of children's stolen Social Security numbers, perpetrators are likely to be family members. Your best strategy for avoiding ID theft is to recognize the crime exists and be alert for its signs.

What can crooks do with my personal information?

Once a crook has stolen your personal data, he or she can use it to get a driver's license, open a credit card or other type of account, take out a loan, rent an apartment, obtain employment, write bad checks, run up your credit card, buy a cell phone, drain your bank account or even commit other more serious crimes—all under your name.

After the damage is done, victims may be denied credit, charged a higher interest rate, refused a job, rejected for a home rental, turned down for a loan and worse. It can take victims many hours over many months—even years—to clear their names and clean up their credit report.

Am I responsible if a thief commits a crime while using my identity?

If a thief makes charges on your credit card and you follow the proper procedures to alert the creditor, you most likely will be responsible for no more than \$50—and perhaps nothing at all.

In cases where a thief commits a more serious crime, such as driving under the influence while using your identity, you may be detained by police and spend time and effort trying to clear up the situation. While, ultimately, you probably will not be held responsible for the crime, the cost in time and money to clear your name can be considerable. For instance, you could be turned down for a job or anything else that requires a background check while false information remains on your record.

For more information about criminal identity theft and how to clear your name, visit the Privacy Rights Clearinghouse (www.privacyrights.org) or call the organization at 619-298-3396.

How can I tell if I'm a victim of identity theft?

Identity theft can go undetected for many months—but there are signs of the fraud. Some of these include:

- missing credit card and loan statements, which may indicate that a thief has stolen them from your mailbox or changed your mailing address with your creditors.
- unauthorized purchases on your credit cards.
- cards and bills for accounts you didn't open, or rejection letters for credit you didn't apply for.
- calls or letters from collectors about bills you don't recognize.
- being denied such things as credit, a job, insurance or a home rental for no obvious reason.

Read your account statements promptly and carefully and check your credit report every year—some experts recommend twice a year—even if you haven't seen anything to indicate you are a victim of identity theft. Look for any suspicious activity, such as accounts, loans and inquiries you don't recognize.

What is a credit report?

A credit report is a detailed record of your credit history compiled by credit reporting companies. These companies also are known as credit bureaus or consumer credit reporting agencies. Equifax, Experian and TransUnion are the three major U.S. credit reporting companies.

Information in your credit report may include:

- your credit limits and current balances with credit cards, mortgage lenders and other creditors.
- your payment record (including on-time, late or missed payments).
- accounts in default or in collection.
- property repossessions.
- bankruptcy filings.
- lawsuits, judgments and liens against you and your property.
- personal information, such as SSN, birth date, recent addresses and employers.

- a listing of recent inquiries from third parties (for example, prospective creditors, insurers and employers).

Your credit report is used by creditors to decide whether to grant you credit and at what rates and terms. Insurers, employers and prospective landlords also make decisions based on the information in your file. Unpaid charges as a result of identity theft can damage your credit—so it is important to follow directions for disputing inaccurate information in your credit report.

How do I get copies of my credit report?

Consumers are entitled to a free copy of their credit report from each credit bureau every 12 months. Order yours through the [Annual Credit Report Request Service online](#), by phone (877-322-8228/TTY 800-821-7232) or by mail (print out the Annual Credit Report Request Form from the website and mail it to: Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281).

By law, you're also entitled to additional free reports if:

- a company denies your application for credit, insurance or employment based at least in part on information obtained from a credit report. The company that denied your application will send you an “adverse action” notice containing the name of the credit bureau you must contact to get your free report. You must ask for your report from the agency that supplied the information within 60 days of receiving notice of the decision.
- you're unemployed and plan to look for a job within 60 days (one report per agency per year).
- you're on welfare (one report per year).
- you dispute information in your credit file and it results in a change in the report.
- you place an initial fraud alert in your credit file.
- you place an extended fraud alert (seven years) in your credit file (an additional two free credit reports within 12 months).

Under state law, consumers in Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey and Vermont can get an additional free copy of each credit report upon request. If you do not live in one of these states, and you are not entitled to another free report, you can buy a copy of your report from any of the three credit bureaus for between \$1 and about \$11 by contacting the credit bureaus directly:

- Equifax: 800-685-1111; www.equifax.com
- Experian: 888-397-3742; www.experian.com
- TransUnion: 800-916-8800; www.transunion.com

Preventing Identity Theft

What can I do to protect myself from identity theft?

While experts agree that you can't entirely prevent the possibility of identity theft, you can greatly reduce your risk by taking steps to protect your information. First, adopt a "need to know" attitude about providing your Social Security number. Don't give it out unless necessary.

Second, check your credit report from each of the three major credit reporting companies at least once every year for free at the [Annual Credit Report website](#); by phone (877-322-8228/TTY 800-821-7232) or by mail. To ask for your report by mail, print out the Annual Credit Report Request Form from the website and mail it to: Annual Credit Report, P.O. Box 105281, Atlanta, GA 30348-5281. Checking your credit report may not protect you from identity theft, but it can help limit any damage if you discover the crime early.

Here are some of the other ways to protect yourself:

- Don't leave your purse, wallet, backpack, mobile device or computer unattended.
- Don't carry your Social Security card or birth certificate with you.
- Don't include your Social Security number on your checks or driver's license.
- Send and receive mail in a locked mailbox inaccessible to others.
- Request that the U.S. Postal Service hold your mail while you are on vacation. (For information about vacation holds, call 800-275-8777.)
- Shred unwanted credit card offers and documents that contain information a crook could use to hurt you.
- At home, keep all confidential information well hidden or under lock and key.
- Don't give out personal information on the phone, through the mail or over the Internet unless you've initiated the contact or have a reasonable basis to know that the request is legitimate and coming from a trusted source.
- Confirm that your employer keeps all personnel and payroll documents under lock and key.
- Regularly update your virus protection software.
- Before you get rid of an old computer or cell phone, delete all your personal information by erasing the hard drive or memory.

By taking these precautions, you can reduce your risk—but unfortunately you can't always stop ID theft. If you're a typical consumer, your personal information is in many different databases. Despite your best efforts to protect your information, you may always be vulnerable to determined hackers who steal customer records from businesses and other organizations.

In which situations am I required to provide my Social Security number?

Generally speaking, your Social Security number (SSN) is required only for Social Security, income taxes, obtaining credit (loans, credit cards, etc.), opening bank accounts and as a way to verify information about you on file with credit reporting agencies. Credit reporting agencies keep track of consumer credit information by SSN.

Businesses often ask for it when you open financial services accounts or obtain insurance, since many insurers include a credit check in the application process. It's okay to ask anyone who

requests your Social Security number why they need it and what will happen if you don't provide it. If you are not satisfied with the answer, don't give out your number.

What sorts of precautions should I take while using the Internet and email?

The Internet is safe to use if you take precautions that make it difficult for cyber-crooks to steal your information. Anyone who uses the Internet should follow these tips:

- Create hard-to-guess passwords that use a combination of characters, and don't ever write them down.
- Make sure your wireless connection at home has a "security key" to keep out hackers.
- Be extra careful with your Internet activity in public wireless "hotspots," which often lack adequate security.
- Log out completely whenever you leave a computer, even for a few minutes.
- Don't take advantage of the "remember information" feature to store your username, password or other identifying information for the websites you visit.
- Do not open or download files or links sent to you by strangers.
- Don't respond to email messages asking for personal information or inviting you to call unfamiliar telephone numbers to discuss your account. Instead, you should call a trusted phone number or log on to a trusted website for the company that purportedly sent the email before you do anything.
- Check the URL for the sites you visit to avoid being redirected to a bogus website that tries to steal your information.
- Make purchases and other transactions only on secure sites that display the closed padlock icon in the browser status bar or a web address (URL) starting with "https://" instead of one with no "s" after http.
- Read the privacy policy for any website that asks you to reveal your personal information, and be sure you are satisfied with the site's policies and practices.
- Don't ever post information such as your address, cell phone number, previous employers or Social Security number in an online resume or personal profile.

How can I make sure no one discovers my PINs and passwords?

To make sure your PINs and passwords stay secret, create ones that are difficult to guess and then take precautions to keep them confidential:

- Create passwords that contain a combination of letters and numbers.
- Do not use easy-to-guess, personalized passwords such as your dog's name, mother's maiden name, address or phone number.
- Never write down your password or PIN. Memorize it instead.
- Beware of "shoulder surfers," who watch as you punch in your code.
- Never reveal your password or PIN to someone who initiates contact with you.
- Create a new PIN or password if the security of an existing one is ever in question.
- Don't take advantage of the "remember information" feature to store your username or password for the websites you visit.

- If you bank, invest or shop online, make sure your wireless connection has a "security key" to keep out hackers. Be extra careful in public wireless "hotspots," which often lack adequate security.

What is "pretexting"?

Pretexting is a term for when crooks get you to reveal your confidential information under false pretenses. For example, a pretexter may call and claim that he is conducting a survey on behalf of a government agency or that he works for a company that you do business with. He then will ask you questions that cause you to reveal such things as your Social Security number, mother's maiden name, employer, bank account number, PINs or passwords.

Pretexters can pose as surveyors, service providers, computer technicians—they will use any and all tricks to get your guard down. Be suspicious of anyone who contacts you asking for personal information. Give information only when you are the one who initiates the contact and you are sure of the person or company you are dealing with -- and that you actually are dealing with *that* person or company.

Are credit monitoring services worth the money?

Credit monitoring services can alert you to changes or suspicious activity in your credit file. But credit monitoring doesn't prevent identity theft; it just provides an early warning that allows you to take action to limit the damage. The three major credit bureaus all offer monitoring services, as do financial institutions and private companies. Prices and services vary widely, so if you are considering a monitoring service, shop around.

Look for a service that monitors reports from all three credit bureaus (some monitor only one) and alerts you to changes within 24 hours (some do this only weekly or monthly). Some services include additional features, such as fraud resolution assistance and fraud insurance. Depending on the service you choose, you could pay anywhere from about \$40 per year to \$200 per year.

Deciding whether such a service is worth the money really depends on your particular circumstances. If you are an identity theft victim or believe you're at high risk to become one, then you may find a credit monitoring service worth every penny. On the other hand, average (not high risk) consumers can do their own monitoring free by ordering their credit report from one of the three bureaus every four months.

Should I purchase identity theft insurance?

Identity theft insurance reimburses victims for the time and money they spend to stop the thief and clear their names. Covered expenses might include phone and mailing costs, notary fees, attorney fees and lost wages. Identity theft insurance does not reimburse stolen money.

Many consumer advocates are skeptical about the value of identity theft insurance. Since the coverage does not replace stolen money and an attorney is usually not needed to resolve an identity theft case, reimbursable losses may be lower than you would expect. Check with your

current insurance agent because you may already be covered against ID theft expenses under your homeowners insurance or renters policy. Stand-alone ID theft policies are available for between \$25 and \$50 per year. They have deductibles and a cap on the losses you can claim, so closely compare various policies before you choose.

What is an active duty military alert?

Members of the military who are away from their regular duty station can place an "active duty alert" on their credit reports to help minimize the risk of identity theft. The alert stays in effect for one year. You can renew the alert if your deployment lasts longer than a year. An active duty alert will also remove you from credit reporting companies' marketing lists for pre-screened credit card offers for two years, unless you ask to be returned to the lists before that time.

How can I stop or limit the use of my personal information for marketing?

It's virtually impossible to ensure you will never get another telemarketing call, piece of junk mail or promotional email message. However, you can reduce the number of marketing communications you receive by taking your name off lists ("opting out"):

- Visit the Direct Marketing Association's website (www.dmchoice.org) for information about how to have your name removed from national mailing, telemarketing and email lists.
- When given the option on a form or website, choose not to receive marketing communications. (You may have to check/un-check a box.)
- Contact businesses that have you on their marketing lists and ask them to remove your name. Reputable companies will honor your wishes.
- Follow instructions in your bank's privacy notice for removing your name from marketing lists.
- The national credit bureaus offer a toll-free number that enables consumers to opt out of all pre-approved credit offers with just one phone call (888-5-OPTOUT, or 888-567-8688; www.optoutprescreen.com). If you opt out, you won't get unsolicited credit or insurance offers, so you must seek out these services when you need them. The opt out can take six to eight weeks to take effect.
- Avoid promotions or contests, which may just be ways to entice you to provide your contact information for marketing purposes.

Advice for Victims

What should I do if my purse or wallet is lost or stolen?

If your wallet disappears, always consider the possibility of identity theft. Even if the contents are returned, you can't be sure that account numbers and other information were not copied.

- Contact your creditors, banks and other card issuers to cancel cards that were in your wallet and request replacements with new account numbers. (Take time now to make a copy of the fronts and backs of your cards or prepare a list of account numbers and

creditor contact information to save you trouble if you have to report a loss.) Cancel credit cards, ATM cards, auto club cards, library cards, your driver's license and anything else a crook could take advantage of. If your checkbook is lost or stolen, contact your bank. And don't forget to cancel your cellular service immediately if your phone's missing (you are responsible for all calls until you report the phone missing). Set up new PINs and passwords for all accounts.

- Contact any one of the three major credit bureaus and place an initial fraud alert in your file. Whichever bureau you contact will notify the other two. The alert entitles you to a free copy of your credit report. Experian: 888-397-3742, www.experian.com; Equifax: 800-525-6285, www.equifax.com; TransUnion: 800-680-7289, www.transunion.com.
- File a police report. Request a copy of the report and make a note of the incident number. You may need a police report to clear up fraudulent accounts.
- Look for signs of fraud. When you receive copies of your credit reports, examine them carefully. Call the help number given on the report and ask if any new accounts have been opened since the report was prepared. Continue to request your credit reports every two or three months for at least a year after the loss or theft of your wallet. As explained in another section of this guide, you are entitled to one free report each year from each of the three credit bureaus.

What should I do if my identity has been stolen?

Start by following the same steps you would take if your wallet were lost or stolen:

- Contact one of the three credit bureaus to place a fraud alert in your credit report.
- File a police report and request a copy of it.
- Report your cards and accounts (and cellular service if you lost your phone) as lost or stolen so that new accounts can be created. Open new accounts. Set up new PINs and passwords.
- Get copies of your credit reports and examine them closely for fraudulent activity. Watch for signs of fraud. Continue to monitor your credit reports frequently until all affected accounts have been cleared up and there are no new signs of identity theft.

File a complaint with the FTC online (www.ftc.gov), by phone (877-438-4338; TTY: 866-653-4261) or by mail (Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580). The FTC can refer your complaint to other government agencies that may be able to help. The agency also enters complaints into the Consumer Sentinel, a database available to civil and criminal law enforcement units in the U.S. and abroad.

What should I do if I find fraudulent accounts or unauthorized charges?

Immediately contact the creditors who granted credit or extended services to the imposter. Notify the company's fraud department that you are a victim of identity theft. Ask the companies to close the accounts and follow all instructions for disputing the charges. Usually, you will be asked to complete a fraud affidavit. If the company doesn't have its own fraud affidavit, use the Federal Trade Commission's ID Theft Affidavit available online at www.ftc.gov/idtheft. Follow

up by sending your request in writing, asking the creditor to confirm in writing that it has closed the accounts and discharged the fraudulent debts.

What should I do if the police will not take my complaint?

If you are having trouble getting your local police to take your identity theft report, try these tips:

- Check with your state Attorney General's office (www.naag.org) to find out if state law requires the police to take reports for identity theft.
- If you're told that identity theft is not a crime under your state's laws, ask to file a miscellaneous incident report instead.
- Furnish as much documentation as you can (such as your notarized identity theft affidavit) to support your claim.
- Be persistent. Explain the necessity of a police report to help you resolve your identity theft case; many companies require one before they will release you from responsibility for fraudulent debts.
- If you can't get the local police to take a report, try a county or state law enforcement agency.
- In addition to local police, contact law enforcement units such as the sheriff, state Attorney General, FBI, FTC, U.S. Secret Service and U.S. Postal Inspection Service to find out how they can help.

How can I place a fraud alert on my credit report?

A fraud alert is a notation on your credit report that requires the three major credit reporting agencies (Experian, TransUnion and Equifax) to alert you when someone applies for credit in your name. These alerts also are intended to prompt creditors to verify your identity before issuing credit in your name, although they are not compelled by law to do so.

Any consumer can request an "initial" fraud alert, which stays on your report for at least 90 days. This might be appropriate if you have a reason to believe you might become a victim of identity theft. For example, you might want to place a fraud alert if you lost your wallet or inadvertently gave information to someone you believe may be a scam artist. You can renew the alert after 90 days.

Can I put a fraud alert on my credit report for longer than 90 days?

Yes, as a victim of identity theft you are allowed to place an extended (seven-year) fraud alert in your credit bureau file rather than the 90-day initial fraud alert. You will be required to send a copy of your police report along with your request. For more information, visit the identity theft websites of the Federal Trade Commission (www.ftc.gov) and the Privacy Rights Clearinghouse (www.privacyrights.org).

What is the charge to place a fraud alert?

There is no charge to place a fraud alert on your file. By contacting any one of the three credit reporting companies, your alert will automatically be sent to the other two. Call Experian (888-397-3742), Equifax (800-525-6285) or TransUnion (800-680-7289).

Can I get a free credit report if I place a fraud alert?

Yes. A request for an initial fraud alert entitles you to one free credit report from each of the three reporting companies (in addition to the free ones each year). An extended alert entitles you to an additional two free credit reports within 12 months.

What is the difference between a "fraud alert" and a "credit security freeze"?

A credit security freeze is a much more stringent measure of protection. Rather than simply alerting you when someone applies for credit in your name, a freeze actually prevents anyone from accessing your credit file until you take steps to give permission by "lifting" the freeze. Companies that can't check your credit report usually won't approve an application for credit, phone service, insurance, housing or employment until you authorize the credit bureau to release your information.

You can use a password (PIN) given to you by the credit bureau to temporarily lift the freeze and allow creditors, employers and other legitimate businesses to view your credit report. A freeze may slow down the process of getting new credit, but it doesn't prevent you from getting the credit or other services you want.

How can I place a security freeze on my account?

To place freezes, you must contact each credit bureau individually. The fees and procedures vary by state, but in most cases it is free for victims of identity theft to place a freeze. There are fees for lifting or removing a freeze, and to place a freeze if you are freezing your credit report for preventative reasons.

- [Experian](http://www.experian.com); 888-397-3742
- [Transunion](http://www.transunion.com); 888-909-8872
- [Equifax](http://www.equifax.com); 800-685-1111

How can I decide whether or not to "freeze" my credit report?

Only you can decide whether the added security is worth the trouble. If you are a victim of identity theft or if you have reason to believe you are likely to become a victim, you have good reason to consider freezing your credit report. A credit freeze may not be an inconvenience if you do not plan to apply for loans and other credit, a job that requires a background check, a rental home or insurance.

What is the process for disputing fraudulent transactions?

For existing accounts, contact the creditor. Tell the representative that you are an identity theft victim and ask about the process for disputing fraudulent transactions. The representative may send you the company's own fraud dispute forms or suggest that you use the FTC's ID Theft Affidavit, which you can download at the [FTC website](#).

Send the forms along with a letter, a copy of your police report and any other supporting materials such as bills, statements or fraudulent applications to the creditor's "billing inquiries" or fraud unit address (Do not mail the materials to the address for sending payments!) Ask for written confirmation that the company has closed the disputed account and discharged the fraudulent debt.

If a creditor has reported fraudulent debts on your credit report, dispute the debts by contacting the credit reporting agencies. Enclose a copy of your report with the erroneous information circled. The consumer reporting company will send you the results of the investigation, and, if the dispute results in a change of information, a free copy of your report.

Send all letters by certified mail, return receipt requested. Keep copies of correspondence and notes about phone calls. If you are not satisfied with the outcome of your dispute, you may add a short statement to your credit report.

What is an identity theft affidavit?

The FTC provides an identity theft affidavit that can be used by victims to dispute debts resulting from the crime. However, some companies and collectors might require that you use their own affidavits. The FTC form is accepted by the three major credit bureaus and many credit issuers and other financial institutions. You can download the form online (www.ftc.gov/idtheft) or request it by phone (877-ID-THEFT).

The FTC's easy-to-complete five-page form gathers information about you, how the fraud took place, law enforcement actions, supporting documentation and fraudulent accounts opened in your name. Submit an affidavit to every company that provided goods or services to the person who stole your identity. Ask for and keep written confirmation that your affidavit was received.

How do I prove to bill collectors that I am not responsible for fraudulent debts?

Many consumers first learn their identity has been stolen when they start receiving collection calls for fraudulent accounts. Tell bill collectors that you are a victim of identity theft and ask for:

- his or her name, the name, address, email address, phone and fax numbers of the collection company and the case number.
- the name, address and phone number of the original credit grantor and the account number for the debt.
- the amount of the debt.
- the date the account was first opened and any transaction or application information available.

- a description of the collector's relationship with the original creditor (in-house collection agency, independent collector, law firm, etc.).
- the procedure for proving that you are an identity theft victim.

Follow the collector's identity theft procedure, providing all necessary forms and supporting material as soon as possible. All important phone conversations should be followed up and confirmed in writing. Ask the collector to confirm in writing that you do not owe the debt. Keep a call log and copies of all correspondence.

Be aware that third-party bill collectors must:

- send you written notice of the debt.
- provide a copy of the credit application or other records related to the fraud if you submit your request in writing. (A forged signature or incorrect address, for example, could help you prove the debt is fraudulent.)
- forward your records to law enforcement officers upon your request.
- tell the owner of the debt that you are a victim of identity theft.

You can stop harassing collection calls by third party collectors if you write a letter stating that you do not want to be contacted by phone. The collector must stop calling you, but it doesn't have to stop the collection process. You must still prove that the debt is not yours.

For additional information about dealing with debt collectors when you are an identity theft victim, visit the Identity Theft Resource Center online (www.idtheftcenter.org).

How long will my life be impacted by identity theft?

It's impossible to predict how long you'll be dealing with identity theft. The outcome depends on many factors—how the thief used your information, whether or not it was passed on to other crooks, how quickly you put a stop to it and how much success you're having disputing fraudulent accounts with credit bureaus, creditors and debt collectors. This is one reason prevention is so important.

Some victims report that they have been affected for up to five years, while others were able to clear their name and credit report in less than a year.

Should I apply for a new Social Security number?

Probably not. A new Social Security number can create new problems. For example, you may find it difficult to get new credit because you have no credit history under the new number. You also may find that the credit reporting agencies combine the credit history under your old number with the information under your new number, leaving you in exactly the same position you were in before getting a new Social Security number. Because of the potential problems, applying for a new Social Security number should be reserved for cases that cannot be resolved despite continued efforts.

Identity Theft Resources

Federal Trade Commission

www.ftc.gov/idtheft; 877-382-4357 or 877-ID-THEFT

As the nation's consumer protection agency, the FTC offers extensive information, tools and tips to help consumers understand, prevent and recover from identity theft.

Privacy Rights Clearinghouse

www.privacyrights.org

Non-profit consumer organization provides a wealth of information.

Identity Theft Resource Center

[www.idtheftcenter.org](http://wwwidtheftcenter.org); 888-400-5530

National non-profit program dedicated exclusively to the issue of identity theft.

Credit Reporting Companies

Equifax

P.O. Box 105069, Atlanta, GA 30348

Report fraud: 800-525-6285, and write to the address above

Order credit report: 800-685-1111 and www.equifax.com

Experian

P.O. Box 9532, Allen, TX 75013

Report fraud: 888-397-3742, and write to the address above

Order credit report: 888-397-3742 and www.experian.com

TransUnion

P.O. Box 6790, Fullerton, CA 92834

Report fraud: 800-680-7289, and write to the address above

Order credit report: 800-888-4213 and www.transunion.com

Checking Account Fraud

To report fraudulent use of your checking account, contact your bank. You may also want to contact one or more of the following (your bank can provide guidance):

- TeleCheck: 800-710-9898
- Certegy (formerly SCAN): 800-437-5120
- ChexSystems: 800-428-9623
- CrossCheck: 800-843-0760

Social Security Administration

www.ssa.gov; 800-269-0271

If a thief is using your Social Security number, contact the Office of the Inspector General of the Social Security Administration.

U.S. Postal Inspection Service

<https://postalinspectors.uspis.gov>; 877-876-2455

[File a complaint online](#) with the U.S. Postal Inspection Service if your mail has been tampered with or stolen or if you believe someone has filed a false change of address. You can also send your mail fraud complaint by mail, using the address provided on the [form](#), or contact the agency by phone.