

Defensive Steps to Take if Your Identity or Personal Information is Stolen

What are the steps I should take if I'm a victim of identity theft?

If you are a victim of identity theft, take the following four steps as soon as possible, and keep a record with the details of your conversations and copies of all correspondence.

1. Place a fraud alert on your credit reports, and review your credit reports.

Fraud alerts can help prevent an identity thief from opening any more accounts in your name. Contact the toll-free fraud number of any of the three consumer reporting companies below to place a fraud alert on your credit report. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, too. If you do not receive a confirmation from a company, you should contact that company directly to place a fraud alert.

Equifax: 1-800-525-6285; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241

Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9532, Allen, TX 75013

TransUnion: 1-800-680-7289; www.transunion.com; Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

Once you place the fraud alert in your file, you're entitled to order one free copy of your credit report from each of the three consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Once you get your credit 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(es), name or initials, and employers are correct. If you find fraudulent or inaccurate information, get it removed. See [Correcting Fraudulent Information in Credit Reports](#) to learn how. When you correct your credit report, use an Identity Theft Report with a cover letter explaining your request, to get the fastest and most complete results.

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.

2. Close the accounts that you know, or believe, have been tampered with or opened fraudulently.

Call and speak with someone in the security or fraud department of each company. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures.

When you open new accounts, use new Personal Identification Numbers (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, or a series of consecutive numbers.

If the identity thief has made charges or debits on your accounts, or has fraudulently opened accounts, ask the company for the forms to dispute those transactions:

- For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. If the company doesn't have special forms, use the sample letter to dispute the fraudulent charges or debits. In either case, write to the company at the address given for "billing inquiries," NOT the address for sending your payments.

- For new unauthorized accounts, you can either file a dispute directly with the company or file a report with the police and provide a copy, called an “Identity Theft Report,” to the company.
- If you want to file a dispute directly with the company, and do not want to file a report with the police, ask if the company accepts the FTC’s ID Theft Affidavit (PDF, 56 KB). If it does not, ask the representative to send you the company's fraud dispute forms.
- However, filing a report with the police and then providing the company with an Identity Theft Report will give you greater protection. For example, if the company has already reported these unauthorized accounts or debts on your credit report, an Identity Theft Report will require them to stop reporting that fraudulent information. Use the cover letter to explain to the company the rights you have by using the Identity Theft Report. More information about getting and using an Identity Theft Report can be found [here](#).

Once you have resolved your identity theft dispute with the company, ask for a letter stating that the company has closed the disputed accounts and has discharged the fraudulent debts. This letter is your best proof if errors relating to this account reappear on your credit report or you are contacted again about the fraudulent debt.

3. File a complaint with the Federal Trade Commission.

You can file a complaint with the FTC using the online complaint form; or call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261; or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. Be sure to call the Hotline to update your complaint if you have any additional information or problems.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials across the nation track down identity thieves and stop them. The FTC can refer victims' complaints to other government agencies and companies for further action, as well as investigate companies for violations of laws the agency enforces.

Additionally, you can provide a printed copy of your online Complaint form to the police to incorporate into their police report. The printed FTC ID Theft Complaint, in conjunction with the police report, can constitute an Identity Theft Report and entitle you to certain protections. This Identity Theft Report can be used to (1) permanently block fraudulent information from appearing on your credit report; (2) ensure that debts do not reappear on your credit report; (3) prevent a company from continuing to collect debts that result from identity theft; and (4) place an extended fraud alert on your credit report.

4. File a report with your local police or the police in the community where the identity theft took place.

Call your local police department and tell them that you want to file a report about your identity theft. Ask them if you can file the report in person. If you cannot, ask if you can file a report over the Internet or telephone. See below for information about Automated Reports.

If the police are reluctant to take your report, ask to file a "Miscellaneous Incident" report, or try another jurisdiction, like your state police. You also can check with your state Attorney General's office to find out if state law requires the police to take reports for identity theft. Check the Blue Pages of your telephone directory for the phone number or check www.naag.org for a list of state Attorneys General.

When you go to your local police department to file your report, bring a printed copy of your FTC ID Theft Complaint form, your cover letter, and your supporting documentation. The cover letter explains why a police report and an ID Theft Complaint are so important to victims.

Ask the officer to attach or incorporate the ID Theft Complaint into their police report. Tell them that you need a copy of the Identity Theft Report (the police report with your ID Theft Complaint attached or incorporated) to dispute the fraudulent accounts and debts created by the identity thief. (In some jurisdictions the officer will not be able to give you a copy of the official police report, but should be able to sign your

Complaint and write the police report number in the “Law Enforcement Report” section.)

What is a fraud alert?

There are two types of fraud alerts: an initial alert, and an extended alert.

- An initial fraud alert stays on your credit report for at least 90 days. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial alert is appropriate if your wallet has been stolen or if you've been taken in by a "phishing" scam. With an initial fraud alert, potential creditors must 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. When you place an initial fraud alert on your credit report, you're entitled to order one free credit report from each of the three nationwide consumer reporting companies, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports.
- An extended fraud alert stays on your credit report for seven years. You can have an extended alert placed on your credit report if you've been a victim of identity theft and you provide the consumer reporting company with an Identity Theft Report. An automated Identity Theft Report, such as the printed ID Theft Complaint available from this Web site, should be sufficient to obtain an extended fraud alert. With an extended fraud alert, potential creditors must actually contact you, or meet with you in person, before they issue you credit. When you place an extended alert on your credit report, you're entitled to two free credit reports within twelve months from each of the three nationwide consumer reporting companies. In addition, the consumer reporting companies will remove your name from marketing lists for pre-screened credit offers for five years unless you ask them to put your name back on the list before then.

To place either of these alerts on your credit report, or to have them removed, you will be required to provide appropriate proof of your identity: that may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

As mentioned, depending on the type of fraud alert you place, potential creditors must either contact you or take reasonable steps to verify your identity. This may cause some delays if you're trying to obtain credit. To compensate for possible delays, you may wish to include a cell phone number, where you can be reached easily, in your alert. Remember to keep all contact information in your alert current.

What does a fraud alert not do?

While a fraud alert can help keep an identity thief from opening new accounts in your name, it's not a solution to all types of identity theft. It will not protect you from an identity thief using your existing credit cards or other accounts. It also will not protect you from an identity thief opening new accounts in your name that do not require a credit check – such as a telephone, wireless, or bank account. And, if there's identity theft already going on when you place the fraud alert, the fraud alert alone won't stop it. A fraud alert, however, can be extremely useful in stopping identity theft that involves opening a new line of credit.

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.

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.

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.

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.

What is an Identity Theft Report?

An Identity Theft Report can be used to permanently block fraudulent information from appearing on your credit report. An Identity Theft Report will also make sure these debts do not reappear on your credit

report. An Identity Theft Report can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. It's also needed to place an extended fraud alert on your credit report.

Creating an Identity Theft Report may require two steps:

Step One is obtaining a copy of a report filed with a local, state, or federal law enforcement agency, like your local police department, your State Attorney General, the FBI, the U.S. Secret Service, the FTC, or the U.S. Postal Inspection Service. There is no federal law requiring a federal agency to take a report about identity theft; however, some state laws require local police departments to take reports. The law requires the report to provide as much information as you can about the crime, including anything you know about the dates of the identity theft, the fraudulent accounts opened and the alleged identity thief. If you do not provide detailed information, it may be impossible for consumer reporting companies and creditors to comply with your requests. We suggest that you file an online Complaint form with the FTC, and then ask your local police department to incorporate a copy of the printed ID Theft Complaint into the police report. By following this procedure, the consumer reporting company and the information provider may require less additional information and/or documentation under Step Two, below.

Step Two of an Identity Theft Report depends on the policies of the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company). That is, they may ask you to provide information or documentation in addition to that included in the law enforcement report which is reasonably intended to verify your identity theft. They must make their request within 15 days of receiving your law enforcement report, or, if you already obtained an extended fraud alert on your credit report, the date you submit your request to the credit reporting company for information blocking. The consumer reporting company and information provider then have 15 more days to work with you to make sure your Identity Theft Report contains everything they need. They are entitled to take five days to review any information you give them. For example, if you

give them information 11 days after they request it, they do not have to make a final decision until 16 days after they asked you for that information. If you give them any information after the 15-day deadline, they can reject your Identity Theft Report as incomplete; you will have to resubmit your Identity Theft Report with the correct information.

You may find that most federal and state agencies, and some local police departments, offer only "automated" reports, reports that do not require a face-to-face meeting with a law enforcement officer. Automated reports may be submitted online, or by telephone or mail. If you have a choice, do not use an automated report. The reason? It's more difficult for the consumer reporting company or information provider to verify the information. Unless you are asking a consumer reporting company to place an extended fraud alert on your credit report, if you use an automated report the consumer reporting company or information provider will probably ask you to provide additional information or documentation.

What do I do if the police only take reports about identity theft over the Internet or telephone?

The FTC ID Theft Complaint has a special section for police reports that are not filed face-to-face, to help you use it to supplement an automated police report. If you file a police report online or over the phone, complete the "Automated Report Information" block of the ID Theft Complaint. Attach a copy of any filing confirmation received from the police.

If you have a choice, however, you should file your police report in person and not use an automated report. It is more difficult for the consumer reporting company and information provider to verify the information in an automated report, and they will likely require additional information and/or documentation.

What do I do if the local police won't take a report?

There are efforts at the federal, state and local level to ensure that local law enforcement agencies understand identity theft, its impact on victims, and the importance of taking a police report. However, we still

hear that some departments are not taking reports. The following tips may help you to get a report if you're having difficulties:

- Provide the officer with a copy of the Law Enforcement Cover Letter that explains why the police report and the Identity Theft Report are so important to both victims and industry.
- Furnish as much documentation as you can to prove your case. Debt collection letters, credit reports, a copy of your printed ID Theft Complaint, and other evidence of fraudulent activity can help demonstrate the legitimacy of your case. Provide the police a copy of "Remedying the Effects of Identity Theft," which shows that police reports are necessary to secure your rights.
- Be persistent if local authorities tell you that they can't take a report. Stress the importance of a police report; many creditors require one to resolve your dispute. Remind them that consumer reporting companies will automatically block the fraudulent accounts and bad debts from appearing on your credit report, but only if you can give them a copy of the police report. In addition, a police report may be needed to obtain the fraudulent application and other records the company has.
- If you're told that identity theft is not a crime under your state law, ask to file a Miscellaneous Incident Report instead.
- If you can't get the local police to take a report, try your county police. If that doesn't work, try your state police.

Some states require the police to take reports for identity theft. Check with the office of your State Attorney General, which can be found at www.naag.org, to find out if your state has this law.

How do I prove that I'm an identity theft victim?

Applications or other transaction records related to the theft of your identity may help you prove that you are a victim. For example, you may be able to show that the signature on an application is not yours. These documents also may contain information about the identity thief that is valuable to law enforcement. By law, companies must give you a copy of the application or other business transaction records relating to your identity theft if you submit your request in writing, accompanied by a

police report. Read more about getting information from businesses, and use this model letter to request this information.

Should I apply for a new Social Security number?

Under certain circumstances, the Social Security Administration may issue you a new Social Security number - at your request - if, after trying to resolve the problems brought on by identity theft, you continue to experience problems. Consider this option carefully. A new Social Security number may not resolve your identity theft problems, and may actually create new problems. For example, a new Social Security number does not necessarily ensure a new credit record because credit bureaus may combine the credit records from your old Social Security number with those from your new Social Security number. Even when the old credit information is not associated with your new Social Security number, the absence of any credit history under your new Social Security number may make it more difficult for you to get credit. And finally, there's no guarantee a new Social Security number wouldn't also be misused by an identity thief.

[This data sheet has been provided as a public service by](#)

Code Electric

[Providing central Iowa with quality electrical installations since 1993.](#)

[\(515\) 208-2415](#)

code_electric@msn.com

www.code-elec.com