GuidanceResources®

Identity Theft

What to Do If You Are a Victim of Identity Theft

The recent data breach at Equifax, the credit bureau, could affect millions of people across the United States and the globe. It has also highlighted the dangers of identity theft in our increasingly digitized world.

Identity theft is the fastest-growing type of fraud in the United States. Even though we have been much more diligent about protecting our personal information, there are still more than 12 million cases of identity theft in the United States a year, costing in excess of $21 billion. If you have been the victim of identity theft, there are a few steps you should take immediately to limit any damage to your finances, credit history and reputation, according to Federal Trade Commission, the nation's consumer protect agency.

Immediate Steps

1. Place an initial fraud alert
2. Order your credit reports
3. Create an identity theft report

It is important when you begin the process to also keep a record of all the steps you have taken in case any of your claims are disputed. Some things to keep in mind when creating and keeping your log:

Telephone Calls: Log all telephone calls. Record the date of each call and the names and telephone numbers of everyone you contact. Prepare your questions before you call and write down the answers.

Postal Mail: Send letters by certified mail. Ask for a return receipt.

Documents: Create a filing system. Keep all originals. Only send copies of your documents and reports.

Make a timeline: List important dates, including when you must file requests, a company must respond to you, or you must send follow-up.

Placing an Initial Fraud Alert

When you detect fraud, call one of the three credit reporting companies that keep records of your credit history and ask them to put an initial fraud alert on your credit report. You must provide proof of your identity. The company you call must tell the other companies about your alert. The three companies that keep records of your credit history are:

- **Equifax:** 800.525.6285
- **Experian:** 888.397.3742
- **TransUnion:** 800.680.7289

An initial fraud alert makes it harder for an identity thief to do more harm. An alert on your report means that a business must verify your identity before it issues credit in your name. The initial alert stays on your report for 90 days. It allows you to order one free copy of your credit report from each of the three credit reporting companies.

Ordering Your Credit Reports

After you place an initial fraud alert, the credit reporting company will explain your rights and how you can get a copy of your credit report. Here are the steps:

- Contact each credit reporting company.
- Explain that you placed an initial fraud alert.
- Order your free copy of your credit report.

Creating an Identity Theft Report

An Identity Theft Report helps you deal with credit reporting companies, debt collectors and businesses at which accounts were opened in your name. You can use the report to:

- Get fraudulent information removed from your credit report
- Stop a company from collecting debts that result from identity theft
- Place an extended fraud alert on your credit report
- Get information from companies about accounts the identity thief opened or misused

The 3 Steps to Creating an Identify Theft Report

- Submit a complaint about the theft to the FTC, at www.ftc.gov. When you finish writing all the details, print a copy of the report, which is called an Identity Theft Affidavit.
- File a police report about the identity theft, and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit when you file the police report.
- Attach your FTC Identity Theft Affidavit to your police report to make an Identity Theft Report.

Keep in mind when disputing claims that some companies want more information than the Identity Theft Report includes, or want different information. The information you need to provide depends on the policies of the credit reporting company and the business that sent the information about you to the credit reporting company.

Next Steps

Review Your Credit Reports

After you get your credit reports, check for any fraudulent transactions or accounts you aren't already aware of.

Also check all key information, including your name, address, Social Security number and employers. If you see errors on the report, like accounts you didn't open or debts you didn't incur, contact the credit reporting companies and the fraud department of each business that reported an error.

Dispute Errors with Credit Reporting Companies

If you find mistakes when you review your credit reports, send letters explaining the mistakes to:

- The three credit reporting companies
- The fraud department of each business that reported a fraudulent transaction on your existing accounts
- The fraud department of each business that reported an account fraudulently opened in your name

If the errors resulted from identity theft and you have an Identity Theft Report, ask the credit reporting companies and businesses to block the disputed information from appearing on your credit reports. The credit reporting companies must block transactions and accounts if you are an identity theft victim.

Other Considerations: Requesting a Credit Freeze

You may want to contact the credit reporting companies to place a freeze on your credit file. A freeze means potential creditors cannot get your credit report. That makes it less likely an identity thief can open new accounts in your name. The cost to place and lift a freeze depends on state law. In many states, identity theft victims can place a freeze for free, but in others, victims must pay a fee, which is usually about $10. If you have a police report, you may be able to place or lift a freeze for free.

Putting a credit freeze on your credit file does not affect your credit score. But it does mean that your credit history can't be checked. So if you want a business, lender, or employer to be able to review your credit report, you must ask the credit reporting company to lift the freeze. You can ask to lift the freeze temporarily or permanently. You may be charged a fee to lift the freeze.

Resource

- U.S. Federal Trade Commission

Monitoring Your Identity for Fraud

As many as 143 million Americans may be in danger of identity theft as a result of the recent data breach at Equifax, one of the three U.S. credit bureaus. Identity theft can be very time consuming and expensive to correct. There are businesses that will monitor your credit history for a fee, but you can also self-monitor to lower your risk for identity theft. Use these tips to monitor your identity at no cost.

Credit Monitoring Services

Check with your bank or credit card issuer in order to determine whether or not they offer credit monitoring services.

Most banks can notify you via free online or mobile alerts as soon as any suspicious account activity is detected. This could include telephone or Internet transactions, international purchases, or transactions over a specific dollar amount.

Report and Dispute

Review credit card and bank statements and report and dispute any unauthorized transactions.

Check your monthly billing and account statements promptly when they arrive. Quickly report and dispute any erroneous or suspicious information with card issuers, financial institutions and vendors as necessary. You might also want to monitor utility bills for any unauthorized purchases or services.

You have the right to withhold payment for a disputed amount without penalty until the card issuer can investigate the claim and make a final determination.

Consider signing up for online access to your accounts in order to monitor activity and transactions on a daily basis.

Credit Report

Review credit reports and report any incorrect information. You are entitled to a free credit report from each of the three major credit bureaus (Equifax, TransUnion and Experian) each year. Unless you are already a victim of identity theft, it is advisable to request a report from one of the credit bureaus every four months.

You are also entitled to a free report from each of the major credit bureaus when you place an initial fraud alert on your credit report file.

Check your report for any information that you do not recognize, such as liens, judgments, bankruptcies, accounts and any other possible indications of identity theft. Report and dispute any fraudulent or incorrect information.

Fraud Alerts

Place a free fraud alert on your credit report file. You can request this through any of the three major credit bureaus. You only need to request this through one of the bureaus, which will communicate the request to the other two. This alert will need to be renewed every 90 days and gives lenders additional steps to take in order to confirm your identification before issuing a new line of credit.

Credit Security Freeze

With millions of identity theft cases reported each year, a security freeze can be a useful measure in preventing identity theft. While not for every consumer, the security freeze is considered the strongest measure one can take in protecting a credit file.

What is a credit freeze?

Also known as a security freeze, this tool lets you restrict access to your credit report, which in turn makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your file, they may not extend the credit.

Does a credit freeze affect my credit score?

No. A credit freeze does not affect your credit score.

A credit freeze also does not:

- Prevent you from getting your free annual credit report
- Keep you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you're doing any of these, you'll need to lift the freeze temporarily, either for a specific time or for a specific party, say, a potential landlord or employer. The cost and lead times to lift a freeze vary, so it's best to check with the credit reporting company in advance.
- Prevent a thief from making charges to your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Can anyone see my credit report if it is frozen?

Certain entities still will have access to it:

- Your report can be released to your existing creditors or to debt collectors acting on their behalf.
- Government agencies may have access in response to a court or administrative order, a subpoena, or a search warrant.

How do I place a freeze on my credit reports?

Contact each of the nationwide credit reporting companies:

- **Equifax:** 1.800.349.9960 or https://www.freeze.equifax.com/Freeze/jsp/SFF_PersonalIDInfo.jsp
- **Experian:** 1.888.397.3742 or https://www.experian.com/freeze/center.html
- **TransUnion:** 1.888.909.8872 or https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

You'll need to supply your name, address, date of birth, Social Security number and other personal information. After receiving your freeze request, each credit reporting company will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze?

In a few states, credit freezes expire after seven years. In the vast majority of states, a freeze remains in place until you ask the credit reporting company to temporarily lift it or remove it altogether. A credit reporting company must lift a freeze no later than three business days after getting your request. The cost to lift a freeze varies by state.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit reporting company the business will contact for your file, you can save some money by lifting the freeze only at that particular company.

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

A credit freeze locks down your credit. A fraud alert allows creditors to get a copy of your credit report as long as they take steps to verify your identity. For example, if you provide a telephone number, the business must call you to verify whether you are the person making the credit request. Fraud alerts may be effective at stopping someone from opening new credit accounts in your name, but they may not prevent the misuse of your existing accounts. You still need to monitor all bank, credit card and insurance statements for fraudulent transactions.

Three types of fraud alerts are available:

1. **Initial Fraud Alert.** If you're concerned about identity theft, but haven't yet become a victim, this fraud alert will protect your credit from unverified access for at least 90 days. You may want to place a fraud alert on your file if your wallet, Social Security card, or other personal, financial or account information are lost or stolen.
2. **Extended Fraud Alert.** For victims of identity theft, an extended fraud alert will protect your credit for seven years.
3. **Active Duty Military Alert.** For those in the military who want to protect their credit while deployed, this fraud alert lasts for one year.

To place a fraud alert on your credit reports, contact one of the nationwide credit reporting companies. A fraud alert is free. The company you call must tell the other credit reporting companies; they, in turn, will place an alert on their versions of your report.

Resource

- Federal Trade Commission: www.ftc.gov

Removing Incorrect Information from Your Credit Report

The Fair Credit Reporting Act (FCRA) establishes procedures for correcting fraudulent information on your credit report and requires that your report be made available only for certain legitimate business needs.

Under the FCRA, both the consumer reporting company and the information provider (the business that sent the information to the consumer reporting company, such as a bank or credit card company) are responsible for correcting fraudulent information in your report. To protect your rights under the law, contact both the consumer reporting company and the information provider.

Consumer Reporting Company Obligations

Consumer reporting companies will block fraudulent information from appearing on your credit report if you take the following steps:

Send them a copy of an identity theft report and a letter telling them what information is fraudulent. The letter also should state that the information does not relate to any transaction that you made or authorized. In addition, provide proof of your identity that may include your Social Security number, name, address and other personal information requested by the consumer reporting company.

The consumer reporting company has four business days to block the fraudulent information after accepting your identity theft report. It also must tell the information provider that it has blocked the information. The consumer reporting company may refuse to block the information or remove the block if, for example, you have not told the truth about your identity theft. If the consumer reporting company removes the block or refuses to place the block, it must let you know.

Information Provider Obligations

Information providers stop reporting fraudulent information to the consumer reporting companies once you send them an identity theft report and a letter explaining that the information they are reporting resulted from identity theft. However, you must send your identity theft report and letter to the address specified by the information provider. Note that the information provider may continue to report the information if it later learns that the information does not result from identity theft.

If a consumer reporting company tells an information provider that it has blocked fraudulent information in your credit report, the information provider may not continue to report that information to the consumer reporting company. The information provider also may not hire someone to collect the debt that relates to the fraudulent account or sell that debt to anyone else who would try to collect it.

Resources

- AnnualCreditReport.com: www.annualcreditreport.com
- Federal Trade Commission: www.ftc.gov

Here when you need us.

Call: 844.824.3273 (844.UCI.EAP3)
TTY: 800.697.0353
Online: guidanceresources.com
App: GuidanceNow℠
Web ID: UCIEAP3