

What To Do If You're A Victim Of Identity Theft

There are several steps you can and should take to protect yourself if you are a victim of identity theft.

Make Sure to Document Your Actions

Begin documenting the time and money you spend on straightening out identity theft. In some states, any person found guilty of financial identity theft will be ordered to pay restitution to the victim for any financial loss, including lost wages.

- Keep copies of correspondence and documents related to the theft.
- Write records of all telephone calls, including the date and time of your call and the name and title of the person who assisted you.
- Write letters to confirm all phone conversations. Include the date, the name of the person you spoke with, and what actions were taken.
- To be extra careful, send documents and letters Return Receipt Requested and keep the postal receipt with your copy.

Consider using the ID Theft Affidavit to avoid having to complete different forms. This form can assist you in disputing inaccurate information that appears on your credit report as a result of fraud. It's available on www.consumer.gov/idtheft. Keep copies of all affidavits that you send.

Contact the Police

Immediately call the police to file a report with your local law enforcement. If your identity was stolen when you were away from home, you may need to contact the police in that jurisdiction too.

Opening a police case accomplishes two things;

First, the police can start investigating the crime.

Second, you will need information from the police report to help you straighten out your credit and accounts after the crime. When you talk to the police, make sure you get the police report number and information on how to reach the investigator. Give this information to all the companies you contact in getting your credit cleared up after the crime.

After you call the Police, contact the credit bureaus.

Stop the Damage

After you call the police, contact one of the credit bureaus. Next, contact any credit card companies and banks where your accounts may be at risk.

Credit Bureaus

Equifax (800)525-6285
Experian (888) 397-3742
TransUnion: (800) 680-7289

- Ask the credit bureau to notify the other two to flag the accounts with a “fraud alert.” Find out how long the fraud alert will remain on your report, and how to extend that time, if needed. Ask that all creditors contact you at a phone number you provide to verify all future applications.
- Add a “victim’s statement” to the report; include your name, state the problem, and provide a telephone number where you can be reached.
- Have each credit bureau send you a copy of your report. These reports will guide you in tracing where and when any fraud occurred to your accounts.

In a few months, order new copies of your reports to verify your corrections and changes, and to make sure no new fraudulent activity has occurred. Unfortunately, identity thieves often strike the same accounts again and again. Because of this, it is very important to continue to monitor your credit reports very closely for a while after the initial crime. Even with a “fraud alert,” thieves may still find ways to open new accounts. Ask the credit bureaus if they will supply you with free reports every few months.

Credit Card Companies

If a thief has gained access to a credit card, contact the security department of that credit card company.

- Close any affected accounts so that they’re registered as “closed at customer’s request.”
- Get new account numbers, and protect the accounts with passwords.
- Follow up with a letter documenting the date, the name of the person who helped you, and what actions were taken.

Just because one card has been compromised, you may not want to close all of your credit accounts, and you may want to hold on to some cards. You may want to get counseling about this decision from a victim assistance group.

Banks

Inform your bank if your wallet or purse was stolen or lost. Tell them what bank account information, including account numbers, ATM cards, or checks it contained.

- Cancel checking and savings accounts and open new ones.
- Stop payment on outstanding checks.

Get a new ATM card, account number, and PIN or password.

Your Credit Report

Many people don't realize they are victims of identity theft until long after the initial crime occurred. Identity thieves often try to hide the crimes for as long as possible so they can access more money. To stop the crimes as soon as possible, make sure you carefully check your credit reports regularly.

Your credit reports are important tools for limiting the amount of damage a thief can cause.

Contact each of the three major credit reporting agencies to order a copy of your credit report at least once a year.

Make it harder for thieves to use your accounts!

the three major credit reporting agencies to order a copy of your credit report at least once a year.

Your credit report will generally contain information on where you work and live, the credit accounts that have been opened in your name, if you own a home, how well you pay your bills, and whether you've been sued, arrested or have filed for bankruptcy. Consider canceling credit cards you haven't used in a long time. You can also consider adding a "fraud alert" to make it harder for thieves to open new accounts without your knowledge. **With a fraud alert, the credit agency has to call you to confirm any request it receives to open a new account in your name. If you decide you want this service, just reporting agencies. Their numbers are listed on the last page of this booklet**

When choosing a PIN, use one that is hard to guess. Avoid the last 4 digits of your social security number, your mother's maiden name, birth dates, names of pets, or even the name of your hometown baseball team. Try to mix numbers, letters, and symbols.

At Work

The newest trend in identity theft is to hit groups of people, and work places can be vulnerable. Find out if your company has a policy about protecting its employees from identity theft. Make sure your employer stores your personal information in a safe place. Also, find out which other employees have access to your personal information.

Companies and Agencies with Which You Do Business

Identity theft can occur through records maintained by your bank, credit card companies, the Department of Motor Vehicles, utilities, insurance companies, and phone companies. Try to have as little information as possible printed on any cards these groups may issue. If you want, ask these companies about their policies with regard to sharing your information. You can stop many components of information sharing. Make it harder for thieves to use your accounts. Put passwords on credit card, bank, and phone accounts. Get credit cards with your picture on them. Call the companies that issue the accounts to find out what security options they offer.

Don't print your social security number or phone number on your checks. Don't have checks delivered to your home — go and pick them up yourself at your bank.

Your Mail

Reduce the circulation of your information through the mail. Stop receiving prescreened credit offers by calling 1-888-5OPTOUT. You can also reduce direct mail marketing and telemarketing by contacting the Direct Marketing Association. Notify each of the three major credit bureaus that you do not want personal information about you shared for promotional purposes. *(This will also reduce unsolicited mail.) Consider putting a lock on your mailbox.*

Identity Theft Insurance

Home insurance policies can include “identity theft insurance” as an option. But know that if you are a victim, insured or not, you should be able to get out of paying all fraudulent bills.

Try not to use your social security number for an identifier:

- Check your drivers license to make sure you aren't using your social security number as identification — few states require this anymore.
- If a school, employer, health insurer, or other institution needs to give you an identification number, often they simply use your social security number. Find out if they can use another number instead.
- The only place you must use your social security number is on government and financial forms, such as tax forms, and most credit applications.

Credit Agencies

Equifax

P.O. Box 740241
Atlanta, GA 30374
www.equifax.com
Report Fraud:
(800)525-6285
Order a Credit Report:
(800)685-1111

Experian

P.O. Box 2002
Allen, TX 75013
www.experian.com
Report Fraud:
(888)EXPERIAN (397-3742)
Order a Credit Report::
(888)EXPERIAN (397-3742)

TransUnion

P.O. Box 1000
Chester, PA 19022
Www.transunion.com
Report Fraud:

How to Read Your Credit Report

1. Check to make sure you are aware of all accounts listed, and balances are what you expect them to be.
2. Look for anything suspicious in the section that lists who has received a copy of your credit history. Some identity thieves “pretext” by posing as a landlord or employer.
3. Make sure no inquiries have been made about loans or leases you didn’t apply for.
4. Check for addresses where you have never lived.
5. If there is any incorrect information in the records, contact the credit bureau, creditor, employer, or government agency immediately. Follow up with a letter describing what actions were taken. Your protections are usually stronger if you report the problem quickly and in writing.