



### **How do thieves steal an identity?**

Identity theft starts with the misuse of your personally identifying information such as your name and Social Security number, credit card numbers, or other financial account information. For identity thieves, this information is as good as gold.

Skilled identity thieves may use a variety of methods to get hold of your information, including:

1. **Dumpster Diving.** They rummage through trash looking for bills or other paper with your personal information on it.
2. **Skimming.** They steal credit/debit card numbers by using a special storage device when processing your card.
3. **Phishing.** They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. **Changing Your Address.** They divert your billing statements to another location by completing a change of address form.
5. **Old-Fashioned Stealing.** They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records, or bribe employees who have access.
6. **Pretexting.** They use false pretenses to obtain your personal information from financial institutions, telephone companies, and other sources. For more information about pretexting, click [here](#).

### **What do thieves do with a stolen identity?**

Once they have your personal information, identity thieves use it in a variety of ways.

Credit card fraud:

- They may open new credit card accounts in your name. When they use the cards and don't pay the bills, the delinquent accounts appear on your credit report.
- They may change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account. Because your bills are now sent to a different address, it may be some time before you realize there's a problem.

#### Phone or utilities fraud:

- They may open a new phone or wireless account in your name, or run up charges on your existing account.
- They may use your name to get utility services like electricity, heating, or cable TV.

#### Bank/finance fraud:

- They may create counterfeit checks using your name or account number.
- They may open a bank account in your name and write bad checks.
- They may clone your ATM or debit card and make electronic withdrawals your name, draining your accounts.
- They may take out a loan in your name.

#### Government documents fraud:

- They may get a driver's license or official ID card issued in your name but with their picture.
- They may use your name and Social Security number to get government benefits.
- They may file a fraudulent tax return using your information.

#### Other fraud:

- They may get a job using your Social Security number.
- They may rent a house or get medical services using your name.
- They may give your personal information to police during an arrest. If they don't show up for their court date, a warrant for arrest is issued in your name.

### **How can you find out if your identity was stolen?**

The best way to find out is to monitor your accounts and bank statements each month, and check your credit report on a regular basis. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. For more information, visit the [Detect Identity Theft](#) section.

Unfortunately, many consumers learn that their identity has been stolen after some damage has been done.

- You may find out when bill collection agencies contact you for overdue debts you never incurred.
- You may find out when you apply for a mortgage or car loan and learn that problems with your credit history are holding up the loan.
- You may find out when you get something in the mail about an apartment you never rented, a house you never bought, or a job you never held.

## **What should you do if your identity is stolen?**

Filing a police report, checking your credit reports, notifying creditors, and disputing any unauthorized transactions are some of the steps you must take immediately to restore your good name. To learn more about these steps and more, visit the [DEFEND: Recover from Identity Theft](#) section. To file a complaint, [click here](#).

## **Should you file a police report if your identity is stolen?**

A police report that provides specific details of the identity theft is considered an Identity Theft Report, which entitles you to certain legal rights when it is provided to the three major credit reporting agencies or to companies where the thief misused your information. An Identity Theft Report can be used to permanently [block fraudulent information](#) that results from identity theft, such as accounts or addresses, from appearing on your credit report. It will also make sure these [debts do not reappear](#) on your credit reports. Identity Theft Reports can prevent a company from continuing to [collect debts](#) that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to place an [extended fraud alert](#) on your credit report.

You may not need an Identity Theft Report if the thief made charges on an existing account and you have been able to work with the company to resolve the dispute. Where an identity thief has opened new accounts in your name, or where fraudulent charges have been reported to the consumer reporting agencies, you should obtain an Identity Theft Report so that you can take advantage of the protections you are entitled to.

In order for a police report to entitle you to the legal rights mentioned above, it must contain specific details about the identity theft. You should file an [ID Theft Complaint](#) with the FTC and bring your printed ID Theft Complaint with you to the police station when you file your police report. The printed ID Theft Complaint can be used to support your local police report to ensure that it includes the detail required.

A police report is also needed to get copies of the thief's application, as well as transaction information from companies that dealt with the thief. To get this information, you must submit a request in writing, accompanied by the police report, to the address specified by the company for this purpose. You can find more information and a model letter [here](#).

## **How long can the effects of identity theft last?**

It's difficult to predict how long the effects of identity theft may linger. That's because it depends on many factors including the type of theft, whether the thief sold or passed your information on to other thieves, whether the thief is caught, and problems related to correcting your credit report.

Victims of identity theft should monitor financial records for several months after they discover the crime. Victims should review their credit reports once every three months in the first year of the theft, and once a year thereafter. Stay alert for other signs of identity theft.

Don't delay in correcting your records and contacting all companies that opened fraudulent accounts. Make the initial contact by phone, even though you will normally need to follow up in writing. The longer the inaccurate information goes uncorrected, the longer it will take to resolve the problem.

### **What can you do to help fight identity theft?**

A great deal.

Awareness is an effective weapon against many forms identity theft. Be aware of how information is stolen and what you can do to protect yours, monitor your personal information to uncover any problems quickly, and know what to do when you suspect your identity has been stolen.

Armed with the knowledge of how to protect yourself and take action, you can make identity thieves' jobs much more difficult. You can also help fight identity theft by educating your friends, family, and members of your community. The FTC has prepared a collection of easy-to-use materials to enable anyone regardless of existing knowledge about identity theft to inform others about this serious crime. To learn more, [click here](#).