



Identity theft and credit fraud are crimes that can leave victims emotionally devastated. While some victims can resolve their problems fairly quickly, others spend hundreds of hours and thousands of dollars to repair the damage to their good name and credit record. Some consumers victimized by identity theft may be denied loans for homes, cars or education because of negative information on their credit reports.

What is identity theft, and how does it relate to credit fraud?

Identity theft is the act of using someone else's personal information (such as name, address, account number, driver's license number, Social Security number or health insurance number) without that person's knowledge and using the assumed identity to commit fraud or theft.

Millions of Americans have their identities stolen each year, and the crime can take many forms. Identity thieves may rent an apartment, obtain a credit card or establish a telephone account in your name. You may not find out about the theft until you review your credit report or a credit card statement and notice charges you didn't make or until you've been contacted by a debt collector or a collections agency.

The majority of identity theft cases result in some form of credit fraud, with approximately 25 percent involving credit cards.

How can you protect yourself from identity theft and credit fraud?

While you can't prevent all cases of identity theft and credit fraud from happening, there are 10 steps you can take to help ensure the safety of your personal information:

1. Safeguard your Social Security number. Don't include it in your address book or another location that is easily accessed by others, and be very cautious about providing it unless necessary by law, such as for employment, tax forms or bank records, or you know you are dealing with a reputable company.
2. Don't carry your birth certificate (or your children's) or Social Security card in your wallet.
3. Don't have your driver's license number printed on your checks.
4. Don't make your passwords obvious or easy to guess, and never carry them in your wallet.
5. Sign your new cards as soon as they arrive.
6. Choose online or "paperless" statements from your financial institutions.
7. Don't leave items containing identifying information, such as your purse, wallet or financial statements, in your car or other location where thieves have easy access.
8. Shred anything with your account number or other identifying information before throwing it away.
9. Don't provide credit card numbers, bank account numbers or other identifying information in response to an unsolicited email or telephone call.
10. If your billing statement is incorrect or your credit cards are lost or stolen, notify your card issuers immediately.

In addition to these simple steps, you also should request a copy of your credit report at least once a year. You also can subscribe to a credit monitoring service or an identity protection service that monitors use of your personal information and accounts for you.

What do you do if your identity has been stolen and used fraudulently?

If you are a victim of identity theft or fraud or have reason to believe you are at increased risk, you can take the following four steps to help protect your credit history:

- 1. Contact a credit reporting company to add an initial security alert to your credit report:** An initial security alert notifies potential credit grantors that your identification has been or is likely to be used fraudulently so that they take additional precautions before extending new credit. This alert gives you time to verify whether fraud has occurred and allows you to get a free copy of your credit report.
- 2. Get a police report:** Police reports are vital to placing long-term alerts on your credit report and to recovering from any subsequent account fraud or other crimes using your identity.
- 3. Review your credit report and billing statements for fraudulent activity:** Request a copy of your credit report from a credit reporting company and review it for activity you did not initiate. It is important to note that fraudulent charges on an existing account appear only on your account's billing statement, not your credit report. You should contact each of your creditors to identify and dispute fraudulent charges. Your creditors will likely issue new cards with new account numbers.

- 4. Contact a credit reporting company to add an extended fraud victim alert to your credit report:** If during the initial alert you identified attempts to commit new account fraud, you can provide a copy of the police report to have an extended fraud victim alert added to your credit report. This alert removes you from prescreened credit lists for five years, helps credit grantors to confirm your future credit applications by calling you at a phone number you designate and allows you access to up to two complimentary credit reports within 12 months of placing the alert. It can remain on your report, at your discretion, up to seven years, but it may make it difficult for you to quickly obtain new credit. Though the alert helps protect you from new credit account fraud, you still may be at risk for other types of fraud (payday loans, employment fraud, etc.) that do not involve accessing a credit report. The credit reporting company also will notify the other nationwide consumer credit reporting companies so that they add similar alerts to their files.

To stay on top of the situation, continue to monitor your credit reports and read your financial account statements promptly and carefully. You may want to review your credit reports once every three months in the first year of the theft and once or twice a year thereafter.