



Identity Theft: It's Personal

In the course of a busy day, you may write a check at the grocery store, charge tickets to a ball game, rent a car, change service providers for your cell phone, or apply for a credit card. While you likely don't give these everyday transactions a second thought, identity thieves do.

What is identity theft?

Identity theft occurs when someone uses your personal identifying information, like your name, Social Security number, or credit card number, without your permission, to commit fraud or other crimes.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years and thousands of dollars cleaning up the mess the thieves have made of a good name and credit record. In the meantime, victims of identity theft may lose job opportunities, be refused for loans, and even get arrested for crimes they didn't commit.

How do thieves steal an identity?

According to the Federal Trade Commission, skilled identity thieves may use a variety of methods to obtain your personal 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 through a credit card swipe machine.
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.

What do thieves do with a stolen identity?

Once they have your personal information, identity thieves use it in a variety of ways. 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.
- Change the billing address on your credit card so that you no longer receive bills, and then run up charges on your account.
- Use your name to get utility services like electricity, heating, or cable television.
- Create counterfeit checks using your name or account number.
- Open a bank account in your name and write bad checks.
- Clone your ATM or debit card and make electronic withdrawals in your name, draining your accounts.
- Get a driver's license or official ID card issued in your name but with their picture.
- File a fraudulent tax return using your information.
- 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 at least once per year from each of the three major credit bureaus. You can request a free credit report at www.annualcreditreport.com. If you check your credit report regularly, you may be able to limit the damage caused by identity theft. Unfortunately, many consumers learn that their identity has been stolen after some damage has already been done.

To find out more about how to protect yourself from becoming a victim of identity theft, visit www.ftc.gov/idtheft.

Source: Federal Trade Commission, www.ftc.gov/idtheft

How to Protect Yourself

Nothing can guarantee that you won't become a victim of identity theft. However, you can minimize your risk, and the damage if a problem develops, by making it more difficult for identity thieves to access your personal information. Here are some tips from the Federal Trade Commission to help protect you or someone you know from becoming a victim of this crime.

- **Shred** financial documents and paperwork with personal information, before you discard them.
- **Protect** your Social Security number. Don't carry your Social Security card in your wallet or write your Social Security number on a check. Ask to use another identifier, if possible.
- **Don't give out** personal information on the phone, through the mail, or over the Internet, unless you know who you are dealing with.

- **Never click** on links sent in unsolicited emails. Use firewalls, anti-spyware, and anti-virus software to protect your home computer; keep them up-to-date.
- **Don't use** an obvious password like your birth date, your mother's maiden name, or the last four digits of your Social Security number.
- **Keep** your personal information in a secure place at home, especially if you have roommates, employ outside help, or are having work done in your house.



Identity Theft Victims: Immediate Steps towards Recovery

Victims of identity theft lose more than money, they lose time. The average identity theft victim spends 30 hours working with creditors, credit reporting agencies, financial institutions, and law enforcement in order to re-establish their credit records.

If you are a victim of identity theft, taking the following five steps can help you minimize the damage to your credit report:

- **Review all three credit reports.** Check to see if any unauthorized charges have been made to your accounts or if any new accounts have been opened.
- **Close the accounts that you know, or believe, have been tampered with or opened fraudulently.** When calling your creditors, ask to speak with the security or fraud department where a representative will be able to help you dispute any unauthorized charges that have been made.
- **Place a fraud alert on your credit reports.** Contact the toll-free fraud number on any of the three consumer reporting companies below to place a fraud alert on your credit report. A fraud alert will notify your creditors to contact you and verify your identity before approving a request of credit in your name. You only need to contact one of the three credit reporting agencies to place an alert, because that company is required to contact the other two.

Equifax: 1-800-562-6285; www.equifax.com

Experian: 1-888-397-3742; www.experian.com

TransUnion: 1-800-680-7289; www.transunion.com

Continue to review your credit reports on a regular basis for suspicious activity. If you find any unauthorized accounts, contact those creditors and dispute the accounts with the credit reporting agency.

- **File a report with your local police department or the police department in the community where the identity theft took place.** After filling out a report, ask for a copy of it, as well as the case number of the report, which you can then provide to creditors who ask for proof of the crime.
- **File a complaint with the Federal Trade Commission.** Sharing your identity theft complaint with the FTC provides important information that can help law enforcement officials across the nation track down identity thieves and stop them.

Following these steps as soon as you are aware that your credit records have been compromised and keeping good records of your correspondences with creditors will put you on the road to reclaiming your financial health.

Source: Federal Trade Commission

As a member of United Financial Credit Union, you can take advantage of the *Accel* program, a free financial education and counseling program. To use this service, simply call 1-877-33ACCEL (332-2235) or visit them on the web at www.accelservices.org.

