

Identity Protection 101

IDENTITY THEFT OCCURS WHEN

a criminal obtains your personal information and uses it for his/her own gain.



- > Name
- > Birth date
- > Social Security number
- > Driver's license number
- > Bank account information

You use this information every day to identify yourself at school, when you make purchases online or when you apply for a job. However, before doing so, it's important to think about the reasons why people and businesses want to know something about you – and what they could do with this information.

As a young adult, you may be at a greater risk of ID theft. Criminals may target you because you have little or no credit history. If they steal your identity, they have a blank slate to run up debt or commit other crimes, and in many cases, you may not realize that you've been a victim until it's too late.

LOOK INSIDE FOR:

- > What Can Criminals Do with Your Identity?
- > How to Review Your Credit Report
- > What Should I Do if I'm a Victim?

The good news is that you can take steps today to help protect your identity.

Identity PROTECTION

What can criminals do with your identity?

- > Open new checking or credit accounts.
- > Make fraudulent purchases or drain your bank account.
- > Use your name when arrested.
- > Use your name and Social Security number to get a job, rent an apartment or file a fraudulent tax return.



The effects of ID theft can be pretty serious. Negative credit information can make it difficult to qualify for new credit, both now (when you apply for credit cards and even student loans) and in the future (when you're ready for a car loan or a mortgage). You may also have trouble getting a new cell phone, renting an apartment or even getting a job.



MORE EVERYDAY *tips*

- > Report lost/stolen ID cards, licenses, credit cards or personal documents as soon as you realize that they are missing.
- > Don't share your credit or debit card with anyone else...not even to a friend for a cup of coffee. It's not that your friends and classmates aren't trustworthy, but this is your personal information and your responsibility — so only you should be using it.



- > Be mindful of how much you share on social networking sites, especially information like your birthday or hometown, which could be useful to criminals. Consider limiting access to your profiles to friends only.
- > Be sure to log out of websites every time, especially when using computers at the library or a computer lab. If you

- don't actively log out, the web browser may store this information, allowing the next person who uses the computer to potentially access your account.
- > Monitor your bank account activity. Check your statements to make sure every purchase is yours, and sign up for alerts that will notify you if your account balance gets low.



CHECK YOUR CREDIT REPORT

One important way to fight ID theft is to check your credit report regularly.

Your credit report includes information about your how many credit cards you have, your outstanding balances and your payment habits.

Your credit reports are used by lenders when evaluating credit applications. Your credit reports can also be used by potential landlords and cell phone companies, and even employers, to determine if you pay bills responsibly. So, it's important to check the information in your report to make sure

it's giving an accurate picture of your reputation.

By law, you are permitted to request one free copy each year from each of the three major credit bureaus. How-

ever, the only way to get your free credit reports is to visit

annualcreditreport.com or call **1-877-FACT-ACT**. You can request all three reports at once, or you can stagger your requests throughout the year.

Major Credit Bureaus

Equifax

equifax.com
1-800-685-1111

Experian

experian.com
1-888-397-3742

Transunion

transunion.com
1-800-888-4213

To order your free annual copy of your credit report:
annualcreditreport.com
1-877-FACT-ACT
(1-877-322-8228)





HOW TO REVIEW YOUR CREDIT REPORT

1 Identifying information (your name, address, Social Security number) — Be sure to check the little things, like whether your name is spelled correctly. If it's not, your report may contain someone else's information.

2 Credit account information — Each account will be listed, along with your credit limit, the amount you currently owe, how many payments have been late and other information. If you see an account you don't recognize or a balance that is larger than it should be, you may have been the victim of identity theft.

3 Public records — This section may include any bankruptcies, foreclosures, judgments and liens filed against you. These records can have a long-term, negative effect on your credit, so make sure they belong to you, not a criminal.

4 Inquiries — An inquiry occurs every time a business requests your credit report, such as when you apply for credit. A number of inquiries can indicate that you are seeking a lot of new credit, which can be a warning sign to lenders that you could get into financial trouble.

Other signs of ID THEFT

- > Missing or late bills for credit cards or utilities.
- > New mail or late-payment notices for unfamiliar loans or accounts.
- > Calls or letters from debt collectors about merchandise or services you didn't buy.
- > Denial of credit when you apply for a loan or credit card or when you attempt to use an existing credit card in good standing.

While some of these things may happen for legitimate reasons or because of simple errors, they may be signs of a problem. Be sure to investigate them carefully.



Common ID Theft TACTICS.

HOW DOES IT HAPPEN?

OLD-FASHIONED STEALING:

Criminals steal your wallet or purse.

DUMPSTER DIVING:

Criminals go through your trash to look for mail or other items with personal information, like bank statements and credit card pre-approval offers.

SHOULDER SURFING:

Criminals simply watch you while you use an ATM or complete another transaction.

HACKING:

Criminals access your information on computers.

PHISHING:

Criminals send a fake e-mail asking you to provide or verify personal information.

PRETEXTING:

Criminals pretend to be someone else and trick you into providing personal information.

SKIMMING:

Criminals use a special storage device that steals card numbers while processing your transaction at an ATM or store register.

PROTECT YOURSELF:

- > Never leave your wallet or purse sitting out, especially when you're not in your room.
- > Find a safe place to keep credit cards, passport and other documents when you're not using them.

- > Shred sensitive documents. Or, just cut them up before throwing them away.

- > Be mindful of your surroundings when at an ATM or store register.
- > Don't provide information over the phone in a public place.

- > Don't share more information than necessary with businesses.
- > Look for secured websites (https) when you shop, bank or pay bills using the Internet.

- > Don't reply to unsolicited e-mails.
- > Check out companies before you do business with them.

- > Watch for familiar-sounding names and familiar-looking logos.
- > Don't verify or provide information over the phone unless you've made the call.

- > Look closely at ATMs and store registers before using them. If something looks funny, walk away.

What should I do if I'm a

VICTIM?

1 If you think you've been a victim of ID theft, call your creditors. They can work with you to close any accounts that have been opened by criminals and dispute any fraudulent transactions.

2 Contact the credit bureaus and ask them to place a "fraud alert" on your credit report. This can stop criminals from opening new accounts in your name and alert potential lenders that your report may contain fraud. Follow any instructions provided to correct any false information.

3 Next, file a report with your local police. While they may not be able to find the criminal, a written police report can help you clear your name. Obtain a copy to submit to creditors and the credit bureaus as proof of the crime.

4 Finally, file a complaint with the Federal Trade Commission (FTC). The FTC maintains a database of fraud cases that helps law enforcement track and apprehend criminals.



Call the FTC's Identity Theft Hotline at **1-877-IDTHEFT** or visit ftc.gov/idtheft.

pnc.com/pncmoney101