Protect your identity

Identity theft basics

What is identity theft?

Identity theft is when someone uses your personal information without your permission. They may open a credit card account, get a loan, or rent apartments in your name using your personal information. They also might access your bank or retirement accounts. You may not know that identity theft has happened until you see your credit report, are notified when trying to apply for credit, or get called by a debt collector.

For more information about identity theft, visit the Federal Trade Commission's website or the Consumer Financial Protection Bureau's website.

How does identity theft happen?

Identity theft is a serious crime. Identity thieves steal information in several ways, such as:

- Digging through trash cans and other places to find documents that contain credit card numbers, account numbers, Social Security Numbers and other personal information
- Retrieving information from lost or discarded computer equipment, mobile phones and PDAs, or wallets
- Using rogue Radio-Frequency Identification readers; stealing checks, credit cards, debit cards, passports, driver's licenses, Social Security cards; or skimming the information from card readers to create new cards
- Stealing information from personal computers using malware or spyware
- Hacking into computer networks and databases to steal large amounts of personal information or infiltrating organizations that store large amounts of valuable information
- Acting as a trusted organization to obtain personal information and/or financial information through the mail, telephone, text messaging and email

What are some common warning signs of identity theft or fraud?

- Bills that do not arrive as expected
- Unexpected credit cards or account statements
- Denials of credit that you did not apply for
- Calls or letters about purchases you did not make
- Charges on your financial statements that you don't recognize
- Incorrect information on your credit reports - accounts or addresses you don't recognize or information that is inaccurate

The Federal Trade Commission's website has additional information regarding the warning signs of identity theft, the Consumer Financial Protection Bureau's website also provides information on common identity theft warning signs.

How can I protect myself from identity theft?

- Destroy or shred documents that include personal information before disposing of them
- Password-protect your computer and other devices, and use anti-virus software
- Use caution when sharing account numbers and personal information online or over the phone
- Beware of phishing phone calls or emails where criminals ask you to provide your information to them - they can pose as banks, retail businesses or even people you know like family members, friends or coworkers
- Monitor your credit card accounts and bank statements
- Always clear your personal information before donating or selling computers and other devices
- Obtain your free annual credit report and review it for accuracy

How does monitoring my credit help protect my identity?

Monitoring your credit report is a good way to spot signs of identity theft, such as errors and suspicious activity and accounts or addresses you don't recognize.

The Consumer Financial Protection Bureau's website provides additional information on monitoring your credit report.

What should I do if I think I may be a victim of identity theft?

You should place an initial fraud alert on your file as soon as you suspect you might be a victim of identity theft. You may request a fraud alert from each of the credit reporting companies over the internet or by mail.

Online:

- Equifax - www.equifax.com/CreditReportAssistance
- Experian - www.experian.com/fraud
- TransUnion - www.transunion.com/fraud

Mail:

- Equifax
- P.O. Box 105139
- Atlanta, GA 30348-5139

- Experian
- P.O. Box 2002
- Allen, TX 75013

- TransUnion
- P.O. Box 2000
- Chester, PA 19016

Here are some other steps you can take:

- Contact the security or fraud departments of each business where an account was opened or charged without your knowledge.
- Follow up in writing, with copies of supporting documents.
- Keep copies of documents and records of your conversations about the theft.
- Complete an ID Theft Affidavit and include it with your written statement.
- File a report with law enforcement officials and provide copies to any creditors needing proof of the crime.
- Report to the creditor the accounts that you know, or believe, have been tampered with or opened fraudulently.
- Report identity theft to the Consumer Financial Protection Bureau by submitting a complaint. Your complaint helps law enforcement officials across the country in their investigations. Visit the CFPB's website to find out more information on submitting an identity theft complaint.

Visit IdentityTheft.gov to report identity theft to the Federal Trade Commission and get a free personal recovery plan that:

- Walks you through each recovery step
- Pre-fills letters and forms for you to send to businesses, debt collectors, and others
- Tracks your progress and adapts to your changing situation.

IdentityTheft.gov has information - and recovery plans - for more than 30 types of identity theft, including tax refund fraud and child identity theft.

What is fraud alert?

A fraud alert is used to inform creditors that you may be a victim of fraud. A fraud alert can make it harder for an identity thief to open accounts in your name. The fraud alert requires creditors to verify that you are the person adding new credit accounts or changing limits on existing credit accounts by contacting you at a phone number you have provided.

There are three types of alerts you can place on your file:

- Initial fraud alert - if suspect that you have become or are about to become a victim of fraud or identity theft (duration 90 days)
- Extended fraud alert - if you are a victim of fraud or identity theft; requires a copy of the identity theft report (duration 7 years)
- Active duty military alert - if you are in the military and want to minimize your risk of fraud or identity theft while you are deployed (duration 1 year).

Contact any one of the credit reporting companies to place a fraud alert. They will share your request with the other credit reporting companies.

As a victim of fraud or identity theft, you have the right to:

- Request the credit reporting company to block information from your credit report that was the result of identity theft. You must provide an identity theft report from a law enforcement agency to request a block
- Dispute information you believe is incorrect
- Request a fraud alert be placed on your credit report

The Federal Trade Commission's website provides additional information about your rights when recovering from identity theft.

Does placing a fraud alert hurt my credit score?

Placing a fraud alert does not affect your credit score. It alerts creditors that you have been a victim of fraud and that they should take extra steps before extending new credit in your name. These extra steps may slow down the approval process for new credit.