

Identity Theft

Identity (ID) theft is a crime where a thief steals your personal information, such as your full name or social security number, to commit fraud. The identity thief can use your information to fraudulently apply for credit, file taxes, or get medical services. These acts can damage your credit status, and cost you time and money to restore your good name. You may not know that you are the victim of ID theft until you experience a financial consequence (mystery bills, credit collections, and denied loans) down the road from actions that the thief has taken with your stolen identity.

There are several common types of identity theft that can affect you:

- Child ID Theft- Children's IDs are vulnerable because the theft may go undetected for many years. By the time they are adults, the damage has already been done to their identities.
- Tax ID Theft- A thief uses your social security number to falsely file tax returns with the Internal Revenue Service or state government.
- Medical ID Theft- This form of ID theft happens when someone steals your personal information, such as your Medicare ID or health insurance member number to get medical services, or to issue fraudulent billing to your health insurance provider.
- Senior ID theft - ID theft schemes that target seniors. Seniors are vulnerable to ID theft because they are in more frequent contact with medical professionals who get their medical insurance information, or caregivers and staff at long-term care facilities that have access to personal information or financial documents.
- Social ID theft - A thief uses your name, photos, and other personal information to create a phony account on a social media platform.

Prevent Identity Theft

Take steps to protect yourself from identity theft:

- Secure your social security number. Don't carry your social security card in your wallet or write your number on your checks. Only give out your social security number (SSN) when absolutely necessary.
- Don't respond to unsolicited requests for personal information (your name, birthdate, social security number, or bank account number) by phone, mail, or online.
- Watch out for "shoulder surfers." Shield the keypad when typing your passwords on computers and at ATMs.

- Collect mail promptly. Ask the post office to put your mail on hold when you are away from home.
- Pay attention to your billing cycles. If bills or financial statements are late, contact the sender.
- Review your receipts. Ask for carbon copies and incorrect charge slips as well. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- Shred receipts, credit offers, account statements, and expired cards, to prevent “dumpster divers” from getting your personal information.
- Store personal information in a safe place at home and at work.
- Install firewalls and virus-detection software on your home computer.
- Create complex passwords that identity thieves cannot guess easily. Change your passwords if a company that you do business with has a breach of its databases
- Order your credit report once a year and review to be certain that it doesn't include accounts that you have not opened. Check it more frequently if you suspect someone has gained access to your account information.