
FINANCIAL AND INSURNACE INFORMATION PROVIDED BY THE D.C. DEPARTMENT OF INSURANCE, SECURITIES AND BANKING
1050 First Street, NE, Suite 801 | Washington, DC 20002 | p 202-727-8000 | disb.dc.gov | @DCDISB

# How to Prevent Identity Theft

Identity theft occurs when someone obtains and uses your personal information fraudulently, often for financial gain. Most people think of credit reports, credit cards, and bank accounts when they hear the words "identity theft." This type of identity theft is financial identity theft. However, many more types of identity theft exist, including medical identity theft; insurance identity theft; driver's license identity theft; criminal identity theft; social security identity theft; synthetic identity theft; and child identity theft.

Here are some steps you can take to prevent various types of identity theft.

- **Know what's in your wallet.** Avoid carrying your Social Security number in your wallet or purse. This number provides access to personal information and should be stored in a safe place. In addition, only carry the credit card you need. This practice limits access to your accounts if your purse or wallet is lost or stolen. It is also a good idea to periodically photocopy your cards and keep a record of the customer service phone numbers associated with your financial accounts to speed up the process of cancelling credit cards, if needed.

- **Shred, Shred, Shred. Open all mail and read it carefully—even the items that might appear to be junk mail could contain personal offers.** Any items with personal information, such as pre-approved credit offers, bank statements, or utility bills should be shredded before being discarded.

- **Be suspicious of solicitors.** You should never give personal information, including your Social Security number, to people unless you have verified that they are trustworthy. This advice applies to sharing information over the phone, in-store, or online.

- **Monitor your revolving accounts and credit score.** Check your bank, credit card, and other financial account information, along with your credit score, once a year to reduce the risk of unauthorized charges or credit applications. If you see a suspicious charge, immediately contact your financial institution.

- **Take action against unauthorized actions.** If you notice a new account has been opened in your name without your permission, immediately contact one of the three major credit bureaus—Equifax, Experian or TransUnion—and ask that a one-year or a seven-year "fraud alert" be placed on your record. Once the alert is placed, the other two bureaus will be notified, and creditors will be required to contact you directly before opening new accounts or making changes to existing accounts. Another option is to restrict access to your credit report by asking for a security freeze. Under a freeze, creditors will not have access to your credit report and most likely will not extend credit without report access. The freeze remains in place until you ask the credit bureau to remove it. In addition, file a police report and submit a complaint to the Federal Trade Commission. You also might consider enrolling in paid services that monitor your credit report and alert you when someone applies for credit in your name or your account information is altered.

- **Use the Internet safely.** Millions of people are online at any given time, some of whom are thieves looking to steal your identity. These hackers can be found collecting information from unsuspecting "pop-ups," surfing unsecured networks or hacking into retail websites. Always use a secured network and frequently update antivirus software and firewall protections on your computer. Also, limit the amount of personal information you share on social networking websites.

- **Consider purchasing identity theft insurance.** Several insurance companies offer identity theft insurance. Although it cannot protect you from becoming a victim of identity theft, this insurance provides coverage for the cost of reclaiming your financial identity, such as the expenses of placing phone calls, making copies, mailing documents, taking time off from work without pay and hiring an attorney. As with any insurance policy, make sure you understand what you are purchasing and compare prices, coverages and deductibles among multiple insurers.

**Identity Breach Indicators**

- You are contacted to collect money that you do not owe. The caller will rarely give you a legitimate call back number or email; they do not want to be traced.

- You receive notice from your medical insurance provider that you have reached your limit on medical benefits. It is important to read your medical insurance statements, especially your Medicare Summary Notes and Explanation of Benefit Statements.

- You receive a denial for insurance for a medical condition you do not have; or receive an explanation as to why you were turned down for a credit card for which you did not apply.

- You receive bills for services you did not receive, such as medical bills and extended warranty service. Victims often think these are mistakes, but often it means that their identities have been breached.

If you suspect you are a victim of identity theft or other financial scams, contact the District of Columbia Department of Insurance, Securities and Banking at disb.dc.gov or 202-727-8000.

**About the Department of Insurance, Securities and Banking**
The mission of the District of Columbia Department of Insurance, Securities and Banking is three-fold: (1) cultivate a regulatory environment that protects consumers and attracts and retains financial services firms to the District; (2) empower and educate residents and (3) support the development and expansion of business. Visit us at disb.dc.gov.

This information is provided courtesy of the National Association of Insurance Commissioners.

Updated: August 28, 2019