

Tips on How to Prevent Various Types of 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. Other types of identity theft include 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 it should be stored in a safe and protected place. In addition, only carry the credit cards you need. This practice limits access to your accounts in the event that your purse or wallet is lost or stolen. It’s 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.
- **Make sure you always have your driver’s license with you.** If someone steals your purse or wallet, your driver’s license can easily be sold to someone who looks like you. Once a person has your driver’s license it is easy to obtain other forms of identification in your name.
- **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 or 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 “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. 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 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. Be sure to always use a secured network, and frequently update firewall protections on your computer. Also limit the amount of personal information you post on 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.

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

About DISB

The mission of the District of Columbia Department of Insurance, Securities and Banking, also known as DISB, is two-fold: (1) protect consumers by providing equitable, thorough, efficient, and prompt regulatory supervision of the financial services companies, firms, and individuals operating in the District of Columbia; and (2) develop and improve market conditions to attract and retain financial services firms to the District of Columbia. Visit us online at disb.dc.gov. This information is courtesy of the National Association of Insurance Commissioners.

Published Sept. 16, 2016