

Identity Theft

Identity theft occurs when a criminal uses another person's personal information to take on that person's identity. Identity theft is much more than misuse of a Social Security number—it can also include credit card and mail fraud, but there are many ways to protect yourself.

Tips to Avoid Identity Theft

1. 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.
2. 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.
3. 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.
4. 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.
5. 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.
6. Surf 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 Web sites. 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 Web sites.
7. 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.

Source: National Association of Insurance Commissioners (NAIC): http://www.naic.org/Releases/2007_docs/identity_theft.htm