

Identity Theft

While there are no guarantees with avoiding identity theft, there are steps you can take to minimize your risk and minimize the damage if a problem occurs.

Identity theft is a serious crime. How does it happen? Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes. While you can't entirely control whether you will become a victim, there are steps you can take to minimize your risk.

1. Protect your Social Security Number, bank account and credit card numbers, PINs (personal identification numbers), passwords and other personal information. Never provide this information in response to a phone call, a fax, a letter or an e-mail you've received — no matter how friendly or official the circumstances may appear.
2. Don't throw away old ATM or credit card receipts, bank statements, tax returns or other documents containing personal information without shredding them first. ID thieves pick through trash bins looking for trash they can turn into cash.
3. Beware of offers that seem too good to be true. Con artists often pose as charities or business people offering jobs, rewards or other "opportunities." They hope that trusting souls will send cash or checks, provide SSNs or credit card numbers, or wire money from a bank account.
4. Before selling, donating or disposing of an old personal computer, use special software to completely erase files that contain financial records, tax returns and other personal information. If you use a computer at a school or library, do not put your personal information on that computer. Even if you delete the information it will stay on the hard drive.
5. Try to use a locked mailbox or other secure location for your incoming mail. Pick up your mail as soon as possible. And for outgoing mail containing a check or personal information, put it in a blue Postal Service mailbox, hand it to a mail carrier or take it to the post office instead of leaving it in your doorway or home mailbox.

If you think your identity has been stolen, here's what to do:

1. Contact the fraud departments of any one of the three consumer reporting companies to place a fraud alert on your credit report. The fraud alert tells creditors to contact you before opening any new accounts or making any changes to your existing accounts. You only need to contact one of the three companies to place an alert. The company you call is required to contact the other two, which will place an alert on their versions of your report, and, if you ask, only the last four digits of your Social Security number will appear on your credit reports. Here are the numbers to each of the three consumer reporting companies: Equifax: 1-800-525-6285, Experian: 1-888-397-3742, Trans Union: 1-800-680-7289 and alert the Social Security Administration (fraud line): 1-800-269-0271
2. Close the accounts that you know or believe have been tampered with or opened fraudulently. Use an ID Theft Affidavit when disputing new, unauthorized accounts.
3. File a report with your local police or the police in the community where the identity theft took place. Get a copy of the report or, at the very least, the number of the report to submit to your creditors and others that may require proof of the crime.
4. File your complaint with the Federal Trade Commission @ www.ftc.gov. The FTC maintains a database of identity theft cases used by law enforcement agencies for investigations. Filing a complaint also helps the FTC learn more about identity theft and the problems victims are having, so that they can better assist you.