



What Are Identity Theft and Identity Fraud?

"...he that filches from me my good name
robs me of that which not enriches him
and makes me poor indeed." - Shakespeare, *Othello*, act iii. Sc.3.

Identity theft and identity fraud are terms used to refer to all types of crime in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, typically for economic gain. Unlike your fingerprints, which are unique to you and cannot be given to someone else for their use, your personal data, especially your Social Security number, your bank account or credit card number, your telephone calling card number, and other valuable identifying data can be used, if they fall into the wrong hands, to personally profit at your expense.

Many people have reported that unauthorized persons have taken funds out of their bank or financial accounts, or, in the worst cases, taken over their identities altogether, running up vast debts and committing crimes while using the victims' names. In many cases, a victim's losses may include not only out-of-pocket financial losses, but substantial additional financial costs associated with trying to restore his reputation in the community and correcting erroneous information for which the criminal is responsible.

What Are the Most Common Ways to Commit Identity Theft?

Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in "shoulder surfing" watching you from a nearby location as you punch in your telephone calling card number or credit card number or listen in on your conversation if you give your credit-card number over the telephone to a hotel or rental car company.

Even the area near your home or office may not be secure. Some criminals engage in "dumpster diving" going through your garbage cans or a communal dumpster or trash bin -- to obtain copies of your checks, credit card or bank statements, or other records that typically bear your name, address, and even your telephone number. These types of records make it easier for criminals to get control over accounts in your name and assume your identity.

If you receive applications for "pre-approved" credit cards in the mail, but discard them without tearing up the enclosed materials, criminals may retrieve them and try to activate the cards for their use without your knowledge. (Some credit card companies,

when sending credit cards, have adopted security measures that allow a card recipient to activate the card only from his or her home telephone number but this is not yet a universal practice.) Also, if your mail is delivered to a place where others have ready access to it, criminals may simply intercept and redirect your mail to another location.

In recent years, the Internet has become an appealing place for criminals to obtain identifying data, such as passwords or even banking information. In their haste to explore the exciting features of the Internet, many people respond to "spam" unsolicited E-mail that promises them some benefit but requests identifying data, without realizing that in many cases, the requester has no intention of keeping his promise. In some cases, criminals reportedly have used computer technology to obtain large amounts of personal data.

With enough identifying information about an individual, a criminal can take over that individual's identity to conduct a wide range of crimes: for example, false applications for loans and credit cards, fraudulent withdrawals from bank accounts, fraudulent use of telephone calling cards, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name. If the criminal takes steps to ensure that bills for the falsely obtained credit cards, or bank statements showing the unauthorized withdrawals, are sent to an address other than the victim's, the victim may not become aware of what is happening until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.

What Should I Do To Avoid Becoming A Victim Of Identity Theft?

To reduce or minimize the risk of becoming a victim of identity theft or fraud, there are some basic steps you can take. For starters, just remember the word "SCAM":

S **Be stingy about giving out your personal information** to others unless you have a reason to trust them.

At Home

Start by adopting a "need to know" approach to your personal data. Your credit card company may need to know your mother's maiden name, so that it can verify your identity when you call to inquire about your account. A person who calls you and says he's from your bank, however, doesn't need to know that information if it's already on file with your bank; the only purpose of such a call is to acquire that information for that person's personal benefit. Also, the more information that you have printed on your personal bank checks -- such as your Social Security number or home telephone number -- the more personal data you are routinely handing out to people who may not need that information.

If someone you don't know calls you on the telephone and offers you the chance to receive a "major" credit card, a prize, or other valuable item, but asks you for personal data -- such as your Social Security number, credit card number or expiration date, or mother's maiden name -- ask them to send you a written application form.

If they won't do it, tell them you're not interested and hang up. If they will, review the application carefully when you receive it and make sure it's going to a company or financial institution that's well-known and reputable. The [Better Business Bureau](#) can give you information about businesses that have been the subject of complaints.

While Traveling

If you're traveling, have your mail held at your local post office, or ask someone you know well and trust another family member, a friend, or a neighbor to collect and hold your mail while you're away. If you have to telephone someone while you're traveling, and need to pass on personal financial information to the person you're calling, don't do it at an open telephone booth where passersby can listen in on what you're saying; use a telephone booth where you can close the door, or wait until you're at a less public location to call.

C Check your financial information regularly, and look for what should be there and what shouldn't:

What Should Be There

If you have bank or credit card accounts, you should be receiving monthly statements that list transactions for the most recent month or reporting period. If you're not receiving monthly statements for the accounts you know you have, call the financial institution or credit card company immediately and ask about it.

If you're told that your statements are being mailed to another address that you haven't authorized, tell the financial institution or credit card representative immediately that you did not authorize the change of address and that someone may be improperly using your accounts. In that situation, you should also ask for copies of all statements and debit or charge transactions that have occurred since the last statement you received. Obtaining those copies will help you to work with the financial institution or credit card company in determining whether some or all of those debit or charge transactions were fraudulent.

What Shouldn't Be There

If someone has gotten your financial data and made unauthorized debits or charges against your financial accounts, checking your monthly statements carefully may be the quickest way for you to find out. Too many of us give those statements, or the enclosed checks or credit transactions, only a quick glance, and don't review them closely to make sure there are no unauthorized withdrawals or charges.

If someone has managed to get access to your mail or other personal data, and opened any credit cards in your name or taken any funds from your bank account, contact your financial institution or credit card company immediately to those transactions and to request further action.

A Ask periodically for a copy of your credit report.

Your credit report should list all bank and financial accounts under your name, and will provide other indications of whether someone has wrongfully opened or used any accounts in your name.

M Maintain careful records of your banking and financial accounts.

Even though financial institutions are required to maintain copies of your checks, debit transactions, and similar transactions for five years, you should retain your monthly statements and checks for at least one year, if not more. If you need to dispute a particular check or transaction especially if they purport to bear your signatures your original records will be more immediately accessible and useful to the institutions that you have contacted.

Even if you take all of these steps, however, it's still possible that you can become a victim of identity theft. Records containing your personal data -- credit-card receipts or car-rental agreements, for example -- may be found by or shared with someone who decides to use your data for fraudulent purposes.

Accompanying this article are articles about the steps to take if you suspect you have become the target of an identity thief, a review of the latest Washington State legislation to protect us from identity theft scams, and a resource list to help you find out more on the subject.