What Are Identity Theft and Identity Fraud?

The short answer is that identity theft is a crime. 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. In the United States and Canada, for example, 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 victim's 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.

In one notorious case of identity theft, the criminal, a convicted felon, not only incurred more than $100,000 of credit card debt, obtained a federal home loan, and bought homes, motorcycles, and handguns in the victim's name, but called his victim to taunt him -- saying that he could continue to pose as the victim for as long as he wanted because identity theft was not a federal crime at that time -- before filing for bankruptcy, also in the victim's name. While the victim and his wife spent more than four years and more than $15,000 of their own money to restore their credit and reputation, the criminal served a brief sentence for making a false statement to procure a firearm, but made no restitution to his victim for any of the harm he had caused. This case, and others like it, prompted Congress in 1998 to create a new federal offense of identity theft.

What Are The Most Common Ways To Commit Identity Theft Or Fraud?

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 happing until the criminal has already inflicted substantial damage on the victim's assets, credit, and reputation.