



Consumer Tips October 2011: Protect Yourself From Identity Theft



Americans become victims of identity theft each year, as crooks steal names, Social Security or credit card numbers and use them to commit fraud or other crimes. That personal information is as good as gold to criminals and they will go to any means to get it.

It is amazing to many Americans to learn how easy it is to obtain the needed information without even breaking into a house. Thieves may use something as simple as “Dumpster Diving”, rummaging through trash looking for bills or other paper with personal information on it. Or, they may try “Phishing”, pretending to be financial institutions or companies while sending spam or pop-up messages to get the unsuspecting victim to reveal personal information.

The U.S. Department of Justice reports that many ID theft cases originate with “shoulder surfing”, watching from a nearby location while the victim punches in a telephone calling card or credit card number or eavesdropping on a conversation as you give your credit card number over the telephone to a hotel or car rental agency.

The Internet is an appealing place for criminals to obtain identifying data, such as passwords or even banking information. Many people respond to spam, unsolicited E-mail promising some benefit but asking for identifying data.

“With enough identifying information about an individual, a criminal can take over that person’s identity to conduct a wide range of crimes,” The Justice Department warned. This information can be used for false applications for loans and credit cards, fraudulent withdrawals from bank accounts, or obtaining other goods or privileges which the criminal might be denied if he were to use his real name.

To avoid becoming a victim, the Justice Department asks consumers to be stingy with personal information.

“Start by adopting a ‘need to know’ approach to your personal data. A person who calls you and says he’s from your bank, doesn’t need to know information that’s already on file at the bank. Also, the more information you have printed on your personal bank checks—such as Social Security number or home telephone number, the more personal data you are handing out routinely to people who may not need that information.

“If someone you don’t know calls you on the telephone offering a “major” credit card or “prize” but asks for personal data, ask them to send a written application form. If they won’t do it, hang up. If they do, review it carefully.

“If travelling, have your mail held at your local post office, or ask someone you know and trust to collect and hold it until you return. Ask a neighbor to remove and hold circulars, newspapers or other tell-tale items that would indicate no one is home.

“Check your financial information regularly and look for what should be there and what shouldn’t. If someone has gotten your financial data and made unauthorized debits or charges, checking your monthly statements carefully may be the quickest way to find out.

“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 report these transactions and to request further action.”

By taking these precautions, you can save yourself hours of sleepless nights trying to remedy the harm not only to your credit report, but to your good name and reputation.

This information is provided with the understanding that the association is not engaged in rendering specific legal, accounting, or other professional services. If specific expert assistance is required, the services of a competent, professional person should be sought.

Provided as a public service by the Pennsylvania Association of Community Bankers.



Consumer Tips October 2011: Protect Yourself From Identity Theft