

# *Potential of Identity Theft and the Dangers that Can Result from It*

By Owen E. McCafferty, CPA, CVPM, DABFA

---

At a study group meeting last year, one of the participants disclosed a rather sad series of events that occurred in his practice, as well as individually, by the terror of identity theft.

Identity theft is not a myth; it is a reality. Unfortunately, identity theft can result in devastating loss of credit-based credibility with vendors.

Today, our society is run on credit. Damaged credit can have a long-lasting impact on a person, their business, and their family. One of the most common forms of identity theft today is the activity of going through a person's garbage. Purchasing a home shredder is a good idea. Shred sensitive information. Unsolicited offers from credit card companies can be one of the primary sources of information that a third party can gain by merely going through your garbage.

Once you put your garbage out for pickup, that garbage becomes public property. Try to do everything you can to thwart the efforts of the dishonest. Shred as much of your personal items before throwing them out for garbage. If someone will go to all the trouble to obtain your personal information, at least make it as difficult as possible for them. Shredding does not necessarily assure that the identity problem will be resolved but the effort makes the activity much more difficult for a would-be thief.

Scam E-mail is another way for individuals to obtain information through the technique of "phishing". Usually, an individual receives unsolicited e-mail from a third party asking them to verify their credit card number, debit card number, or other personal information about them.

Be wary of any individuals who ask for information online from credit card companies, governmental entities, your internet service provider, etc. Be aware that when you do provide this information, you are risking that that person will piece together other information to obtain adequate credibility to secure debt instruments attaching your name to them.

Regularly evaluate your account information online if you believe you may have been "phished" by an individual other than the bank. Do not wait for the statement to arrive – it may be too late by then.

More than 27,000,000 Americans have become victims of identity theft. Diligence is required on your part. Even the most intelligent individuals can have their identity stolen.

## **Spies Unbeknownst to You**

Whenever you enter the Internet, cookies can be placed on your computer system. These cookies can have innocuous information that helps speed up the re-access of website pages. Cookies can also be placed within your computer that can send information back to a third party.

For this reason, we strongly suggest that you purchase not only virus protection software but spyware software as well. Some individuals have multiple spyware programs running concurrently so they can have protections in a variety of areas. Update your virus protection and spyware programs at least monthly by purchasing an online service that automatically updates for new viruses and schemes to obtain access to your computer. Sweep your computer on a consistent basis.

While we're on the subject of computerization, always remember to backup and test the backup. Many people will religiously backup their systems only to discover that the back-up system is faulty. You may not know until the time of need and then unfortunately find out that the backup is worthless.

Here are some ideas that can help you mitigate the potential for identity theft. I use the word "mitigate" essentially as a point to start this discussion because the risk of identity theft can never be eliminated 100%.

1. Your Social Security number is essential. Many organizations use Social Security numbers for identity purposes. Try to give an ID number other than your Social Security number. Inquire from the entity that asks you for your Social Security number if another number can be used instead. An idea might be to use your business telephone number as an identifying number. Try not to keep your Social Security card on your person, but rather keep it in a secure place inside your home. The same holds true for other information that may have your Social Security number imprinted on it. Unfortunately, many states require Social Security numbers on drivers' licenses. Some states now allow you to have the choice of eliminating your Social Security number on your driver's license. If you do have that option, take advantage of it.
2. Avoid response to "phishers". These phishers forward e-mails to you requesting personal information. Sometimes, they hide their name in a series of buried screen names that may, on the face, look legitimate. Be wary of giving information to phishers.
3. Be sensitive to credit card numbers. When you order a specific item on the phone, make sure no one is listening around the corner. Others can hear your voice and record the information. When giving out your credit card, use a corded phone rather than a cordless phone since a cordless phone can be tapped by outside parties.
4. Refuse pre-approved offers. If you have the availability to elect to not receive unsolicited credit card offers, please do so.

A whole variety of steps must be taken once you suspect that someone has stolen your identity. First of all, alert financial institutions such as your bank and any credit card company. There are major credit bureaus that might be my first approach. Contact Experian at [www.experian.com](http://www.experian.com), Equifax at [www.equifax.com](http://www.equifax.com), and TransUnion at [www.transunion.com](http://www.transunion.com). In essence, you will ask for a fraud alert to be placed on all your accounts which will then require creditors to contact you before authorizing any charges to your account.

Getting a police report may be essential. Many credit card companies demand that the person you say you are is the person you are. Get the police report to show credibility. Sometimes, creditors suspect that an allegation of identity theft is really an attempt to avoid paying bills.

The Federal Trade Commission offers a form that creditors will accept as proof of innocence in an identity theft case. You must gain a notarized ID theft affidavit. You can download this form at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

As you have heard from us many times, keep logs of what occurs if you suspect you have identity theft. Chart your communications in date, time, and person discussed whenever you alert a financial institution or credit card company. Keep copies of your correspondence. If you use the Internet to alert the major credit bureaus, copy as much of the information from the screen as possible.

You probably know that the Federal Trade Commission recently mandated that credit bureaus provide consumers with free reports every year. To order your report, go to the Federal Trade Commission's web page at [www.annualcreditreport.com](http://www.annualcreditreport.com). The availability is stepped. By September 1, 2005, theoretically, all regions should have access to the credit report. Review your credit report regularly. Inaccuracies naturally occur and identity theft may also be one of the items that you can spot.

OEM/alb

*articles\miscellaneous\identity theft*