

# Protecting the Real You

By Shawn Stevenson, Source Water Specialist

You know who you are, figuratively speaking, and self proclamation is one of the cornerstones of American society. Unfortunately a question that seems to be gaining momentum over the past several years is “who is being you?” In other words who is pretending to be you by using your identity? Anyone who has ever had anything stolen understands the feeling of loss and astonishment when they realize what has happened. One of the main components for successful identity theft is the victim being unaware of the theft for an extended period of time. This gap in time paves the way for the thieves to continue with their scam and typically accrue substantial debt in your name.

Once the damage has been done the burden of proof lies with the victim. Our credit system seems to work as an inverse to our justice system. We are guilty until proven innocent and it will take several months typically to clear your name through countless hours on the phone with the reporting credit bureaus. As we all know the quality of our lives is affected by our reputation. Many privileges and services are now credit score driven and your score reflects your financial reputation. Once your reputation has been tarnished the steps in returning it to a previous status are extensive.

It seems like every week we hear of a new scam on the news about credit or identity theft. The number one fraud complaint filed with the Federal Trade Commission (FTC) in fraud related cases was identity theft, with over 250,000 in 2004. That is not including the unreported cases making it a major source of personal financial turmoil (*Real Simple, Oct 2005*). Many of the new scams are quite ingenious and will continue to change as authorities become wise to the standard processes. In truth you can take every possible personal precaution and still get burned based on the volatile nature of this crime.

As we move through life we acquire more things and along with these come increased debt. Our spending habits are tracked and filed to create profiles about us and the public in general. How is this data being compiled you might ask? Cookies on your computer keep track of what websites you visit, credit cards are monitored for revolving debt, and grocery store member cards record what you buy, and when, while enticing you with a supposed discount member price! Data brokers legally compile personal information

about you. Usually they supply marketers, creditors and any party that has a legitimate interest. Many of the businesses and state agencies that we deal with sell personal data to interested parties. Just recently one of Oregon’s state agencies sold information to a source that was determined to be illegitimate - after the fact. Several of the sources of your personal data are out of your control, but this should not deter you from taking ownership of the things you can change. It has not gotten to the extent of **Big Brother** is watching your every move but, we should all be aware that a lot of what we do is being tracked. The intent of this article is not to create paranoia, however, a little caution can go a long way.

Personal information also circulates in multiple forms including bank statements, credit card statements, and the Internet. Obtaining your personal information can be achieved in several ways, including theft of a wallet, Phishing, phone scams, Skimming credit and ATM cards, Internet fraud, stealing mail, and sifting through trash. One of the common gateways to accessing this data is by hacking stored passwords and keystrokes from your home or work computer. As the quantity of personal information distribution sources increase, so do the chances of some of it getting into the wrong hands. Telemarketers obtain information everyday from us unknowingly providing it. Using caller ID and not letting children answer the phone are good initial preventive measures. The Federal Government has also created the National Do Not Call Registry which can be contacted to reduce telemarketing (*Real Simple, Oct 2005*).

To help reduce credit card companies and the credit bureaus sharing your personal data, you need only to **Opt-out!** Many agencies associated with your credit provide you with a privacy notice and give you the option not to have your information shared. The credit bureaus also offer a toll-free number that enables you to “opt-out” of having pre-approved credit offers sent to you for two years. It pays to read the fine print of these disclosure notices.

Let’s examine some of the scams in detail and some ways to combat them. The more informed you are, the better chance of preventing a theft. One of the more popular scams over the past year has been Phishing. **Phishing** is where an email is sent stating that your information has been either lost or leaked and the false bank or agency needs to update your account information. One of the most popular Phishing scams is the **free credit report offer**. It is recommended to check your report but, do not use a

provided link enclosed in an email. Please note that banks and credit agencies will not request personal information via email. Do not provide personal information to any request, unless you instigated the offer or promotion.

**Skimming** scams involve swiping the card through a reader to obtain magnetic stripe information to utilize later. This can occur at any location from questionable individuals at a legitimate retailer or especially at a restaurant where cards are taken out of view.

A **change of address** scam has been quite popular as well. This scam involves an individual going into the post office and changing your mail delivery location to obtain your information. If you don't receive any mail for several days in a row, contact the local post office and then the police if indeed your address was falsely changed.

**Taking pictures** of your credit card is another quick scam, cell phones with cameras have been used to photo the card numbers at grocery stores while in line. Be aware of your surroundings and who is in close proximity to you while in a line or being provided a service.

There are some simple procedures that you can undertake to help protect yourself from putting your identity in jeopardy. Keep credit and debit cards in your view during purchases as much as possible. Request a copy of your credit report by directly contacting one of the major agencies: Beacon, Equifax, Experian, or Trans Union either by phone or by written letter. The best way to keep track of what is going on with "the real you" is to check your credit report periodically throughout the year.

Many of the scam scenarios mentioned can be referenced on the Federal Trade Commission (FTC) website. There is a wealth of knowledge available on tactics and procedures. Another solution contributing to the prevention of ID theft could stem from taking a few minutes to instill these extra precautions into your daily life.

- *Avoid surveys and emails asking personal information.*
- *Carry more cash for small transactions.*
- *Install spy-ware software on your main use computer.*

- *Keep debit cards within close proximity or be present for swipe.*
- *Keep tabs on mail delivery.*
- *Periodically clear your cookie folder on your computer.*
- *Shred all mail with personal information enclosed.*
- *Update Windows Service Pack to newest version to increase security encryption.*
- *Utilize a firewall and antivirus software.*
- *Utilize encryption on wireless routers.*
- *Watch bank and credit card accounts closely.*

In terms of ID theft most people figure that it won't happen to them or that the chances are low. But everyday the odds increase against you if you don't pay attention to your account information, surroundings, and credit history. You have spent a lifetime establishing your identity. Don't let someone else turn your financial life upside down with a few hours of devious thievery.

### **By Shawn Stevenson Source Water Specialist**

This information is provided for you to take appropriate measures to protect your personal identification. OAWU does not assume any responsibility for any information presented or implied by the parties outlined via informative phone numbers, website links or circumstances that may conclude after contacting them.

<http://www.ftc.gov>

[www.donotcall.gov](http://www.donotcall.gov) Or call 1-888-382-1222

Call 1-888-5-OPTOUT (567-8688)

Equifax, Inc.  
Options  
PO Box 740123  
Atlanta, GA 30374-0123

Experian  
Consumer Opt-Out  
701 Experian Parkway  
Allen, TX 75013

TransUnion  
Name Removal Option  
P.O. Box 505  
Woodlyn, PA 19094