



Michael Nobile, CFP



**CRESCENT
STERLING LTD**

A REGISTERED INVESTMENT ADVISER



Investor Notes

7/2/2009

Your Identity - Your Most Valuable Asset

According to the Federal Trade Commission, over 9 million Americans are victims of some type of identity theft each year. Either you or someone you know was probably the victim of identity theft within the past year.

Identity theft takes on many forms and is usually the result of your private information ending up in the hands of someone who intentionally sets out to steal or use your identity for monetary gain. Some common methods for obtaining your personal information are: theft of your wallet, purse, or mail; theft of your information from a company that you do business with; rummaging through your trash; or obtaining it from unsecure transactions via the internet. Regardless how your information is obtained, the time and money often required to remedy the situation can be enormous. The FTC estimates that the average time required to fix problems from identity theft is 30-60 hours, while the cost to repair ranges from \$500-\$1200.

What can someone do with information about you and your personal finances? Some common problems include:

- > Stealing your credit card number and running up charges on the card;
- > Opening up a credit card account using your name and social security number;
- > Withdrawing funds from your bank accounts via electronic funds transfer;
- > Establishing an account for cell phone service in your name;
- > Filing for bankruptcy in your name;
- > Filing for social security benefits with your social security number.

All these types of crimes are serious and cost U.S. businesses more than \$50 billion per year according to the FTC. Given the personal time and expense to remedy problems caused

by identity theft, the best solution is prevention. Preventing identity theft does not have to be costly nor does it have to be time consuming; however, there are simple steps that one can take to lessen the chance of being a victim of identity theft.

Treat your social security number and other personal information like a secret. Social security numbers are often requested when conducting business over the phone or internet. If you did not initiate contact, be very suspicious about why someone would need your number. Always ask if a social security number is absolutely necessary or if there is another identifier that could be used. Do not carry your social security card or other sensitive information like user IDs and passwords in your wallet or purse.

Sign up for electronic statements whenever possible. Paper statements tend to be less secure and detection of fraud tends to take longer with paper statements. Take time to review transactions and balances to make sure they are what they should be.

Use a shredder and shred sensitive papers along with old credit cards. Shred statements from phone bills, electric bills, cable bills and any other piece of paper that has information about you or an account with your name on it.

Request a free copy of your credit report from one of the three credit reporting agencies. Under current federal law, the agencies are required to provide to you upon your request, a copy of your credit report once every 12 months. To do so, go to www.annualcreditreport.com (or call 1-877-322-8228) and follow the instructions. Once you receive it, scan each account for unusual

activity and look for accounts that you do not recognize.

To protect your home computer, install a reliable virus protection program and keep it current following the developer's recommendations. If you are connected to the internet via a cable modem, use a router with a built-in firewall to protect unwanted intruders from controlling your computer or stealing information stored on it.

Even if these steps are followed and you take other precautions to minimize risk, identity theft happens. If you find yourself a victim, you should consider these steps to minimize the damage.

Immediately contact one of the credit reporting agencies (Experian, Transunion, or Equifax) and have them place a fraud alert on your account. The other two will then be notified automatically. If you haven't ordered a free credit report, order and review for new accounts or unfamiliar balances. Any account that has been subject to fraud should be closed immediately. It will also be necessary to contact your local police and file a report of your theft. A police report may be needed to validate your claims with creditors or financial institutions. It is also recommended you visit the FTC's website at www.ftc.gov. The FTC has an entire section on identity theft that may include other tips and steps not mentioned in this article.

Protecting your identity is something we all take for granted. By having some understanding of how thieves gain information and use it, you can help minimize the risk of being a victim. For other financial related articles, please visit our website at www.CrescentSterling.com.