Financially Speaking

Professional Guidance *For the Future You Deserve*

Summer 2006 **Volume 1, Issue 3**

Identity Theft

Recently, I've heard from a family member and a client who have had their financial identities stolen. This national epidemic is on the rise and it's up to you to protect yourself. Reconstructing your financial information after a theft is difficult, time-consuming and from all accounts very frustrating. You see, in every other area of our society you're innocent until proven guilty but become the victim of identity theft and as far as the credit system goes you are guilty until you can prove your innocence. In the world of financial information, a creditor's word supersedes yours and if will be up to you to prove your case absolutely. You will spend your time and money to prove that you did not go on a wild spending spree, and that it was someone else who stole your identity.

Because I can't stress the importance of this enough, this newsletter will focus on what you can do to protect yourself. You've heard most of this before, but it bears repeating. There are things you can easily do and believe me a little time now can keep you from spending hours and hours later.

The very first thing that I want to bring to your attention is that if you even slightly suspect that your information may have been stolen or is at risk, act now. Don't delay. Follow-up with the resources listed below in the hope that you can limit the damage.

Precautions to take now:

When someone steals your identity, what they are really stealing from you is your credit rating. Your credit rating lets you move through the financial world for things we take for granted such as opening a checking account, refinance a mortgage or renting a car.

Start now to protect your credit, the following is a list of some easy steps:

1. Get your credit report at least once a year. Everyone is entitled to a free credit report once a year from each of the three major credit reporting agencies, ***Experian***, ***Equifax*** and ***TransUnion***. Once you receive your credit reports, go through them with a fine tooth comb to make sure that what is in them is accurate. Immediately report any errors. Be prepared to back up your assertions. To get your free credit reports go to *www.annualcreditreport.com* or call 877-322-8228.
2. *Buy a shredder. Purchase a cross cut shredder from your local office supply store and put it where you check your mail or do your paperwork. Constant use of your shredder will prevent dumpster diver's from retrieving your personal information such as account numbers, Social Security number, birth date and driver's license number. Shred anything that you aren't filing away for future use that has any personal information. This includes credit card applications you get in the mail, old tax returns, bank and investment account statements, pay stubs, bills and invoices, credit card receipts, and everything with your Social Security number.*
3. Secure any paperwork that you keep. Commonly the identity thief is someone you know. Sadly, family and friends, the people we trust the most, may be stealing and selling your personal information. Keep your paperwork and documents in a locked file cabinet, safe or safety deposit box.
4. *Be careful when purchasing online. Using credit or debit cards when making online or telephone purchases has become a way of life. You must determine if the company you're dealing with has high security*

©2006 Mary Lacey Gibson, CFP®

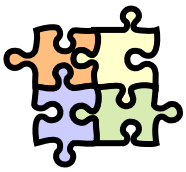
Identity Theft—Continued

standards. Look at their privacy policy and security status before making your purchase. Online, look for a web address that begins with "https" which denotes a secure site and read their security policy. Ask for both privacy and security policies before making phone purchases.

5. Beware of Phishing. Phishing involves using e-mail or the phone to elicit personal information from you. The most common and perhaps the most outrageous (in other words, how could anybody fall for this but they do) Phishing expedition is the Nigerian scam. If you get an e-mail from anyone that claims to be a friend or relative of some high government official in Nigeria or any other country that directs you to contact them so that you can share in several million dollars, please hit your spam or delete button as fast as you can. ***There are many other Phishing expeditions out there. Any time an e-mail or phone call requests your personal information for something that you have never heard of or don't understand, please hit delete or hang up.*** Don't engage in a conversation with these creeps. They are highly trained and convincing at getting information and before you know it you may be saying more than you want to. For further information, visit the Federal Trade Commission web site at *www.consumer.gov/idtheft/*. Anti-Phishing Working Group is an international association focused on eliminating the fraud and identity theft that result form Phishing, Pharming and email spoofing of all types. Their web address is *www.antiPhishing.org/index.html*. You can link to pages for an archive of past and current Phishing emails or to report Phishing.
6. ***Protect your computer. Your computer contains valuable personal information. Beyond knowing who you are dealing with when making online purchases you need to protect your computer from invasion from afar. Use antivirus software and anti-spyware software. Install a firewall if needed by your computer setup. Update them all regularly. It's also extremely important to protect your passwords. Changing your passwords often is an important step to protecting your information. Your e-mail is commonly the entry point for the bad guys. Never open attachments, even from people you know unless it's something you are expecting. The attachment which you think contains newest baby pictures from your cousin could just as easily be someone installing software that monitors your computer. In the event of a problem, have an expert a phone call away to help you out.***
7. Know when to swipe card. I don't mean steal a card, I mean swiping a card in an electronic terminal. In general, it's up to you to keep track of who get your credit and debit card information via terminals. It's best to use only terminals from well-known companies or banks. Avoid no-name ATM machines.
8. *Be careful with your e-mail. I suspect we have all received e-mail that has authentic looking company logos and information and them. The one I receive most often is about my PayPal account. Since I don't have a PayPal account I know this is spam mail on a Phishing expedition. Reputable firms will not contact you via e-mail about problems with your account. If you have any doubt about an e-mail you receive, contact the company by phone, using a number you know to be genuine, to get information. Linking through an email to a web address is also risky. Never link though or copy and paste a web address from an email unless you are certain it is genuine.*

Credit Monitoring Service

To quote the Federal Trade Communication's web site: *"There are a variety of commercial services that, for a fee, will monitor your credit reports for activity and alert you to change your accounts. Prices and services vary widely. Many of the services only monitor one of the three major consumer reporting companies. If you're considering signing up for a service, make sure you understand what you're getting before you buy. Also check out the company with your local Better Business Bureau, consumer protection agency and state Attorney General to see if they have any complaints on file."*



©2006 Mary Lacey Gibson, CFP®

How to Limit the Amount of Junk Mail You Receive

I hear from my clients that they get several pre-approved credit card applications in the mail every week. It's annoying, it fills up the recycle bin and wastes time. The three largest credit bureaus sell your information to credit card companies unless you take steps to prevent it. *You can now opt out by calling the Opt-Out Request Line to remove your name from all marketing lists that credit bureaus sell to direct marketers.* You have a choice of permanently removing your name or for two-year time. Call 888-567-8688.

If you wish to stop other types of junk mail you can do so by sending a letter to: Mail preference service, ***Direct Marketing Association, P.O. Box 9008, Farmingdale, NY 11735***. Include your complete name as well as any other names or nicknames that you may have used, phone number and your mailing address in the letter. Not every company belongs to DMA but it will greatly reduce what you receive.

Financial Trivia

These are just-for-fun miscellaneous financial statistics. Remember, statistics are simple facts and are inherently neutral. Judgments, interpretations and viewpoints are applied to statistics by you. So, as you read the statistics and have reactions to them, ponder how they could impact you, your family or your friends.

- **Over 57 million Americans, according to research firm in Gartner, Inc., in 2004 received e-mail attacks from phishers. The same report stated that Phishing is growing exponentially each year.**
- *Attacks originate from several countries. In 2005 the United States accounted for 32% of attacks with the Republic of Korea coming in second at 15%.*
- In 2004, approximately 2 million U S citizens had their checking accounts raided by cyber thieves with an average loss of $1,200 or $24,000,000,000.
- *The most common companies named in Phishing expedition e-mails, as you might expect, our banks and financial institutions. Citibank Smith Barney and PayPal alone account for over 70% of all Phishing e-mails.*

Books of the Month

The New Retirementality
By Mitch Anthony

Your retirement most likely won't look like your parents'. Mitch Anthony delves into a new way to look at retirement and the many choices now available. After reading this book you will probably rethink and redefine "Retirement".

Affluenza: The All-Consuming Epidemic
By John de Graaf, David Wann and Thomas Naylor.

As the title suggests, we, in our society, are suffering from a disease of over consumption and all of its ill effects. Consuming more than we should hasn't increased our happiness level. As national savings levels have plummeted to an all-time low this book has a very timely message.

©2006 Mary Lacey Gibson, CFP®

Fact or Fiction

As long as we're talking about junk e-mails I thought I'd mention a couple of web sites that track urban myths and legends. Visit *www.snopes.com* or *www.TruthOrFiction.com* to learn if the email forwarded from your best friend is fact or fiction. It is fascinating to learn what is truth or misinformation. For example, some of the "Hottest" urban legends (they are not true) emails include a claim that you must sign up with the National Do Not Call list to prevent telemarketers from calling your cell phone, show a picture of a female tiger raising a group of piglets, warn that prepackaged salads could contain E. coli, warn about the dangers of outdated pancake mix, claim Bill Gates, Microsoft and AOL are giving away cash and merchandise to those who forwarded the e-mail message and claims that Target stores do not support veterans. How many of these have you received? These just scratch the surface. But, some of these could have real financial and lifestyle impacts since they are often written and presented in such a manner that they seem entirely plausible. Now you have a place to check them out to see if they are real or the product of someone's fertile, often vicious, imagination.

Mary Lacey Gibson
CERTIFIED FINANCIAL PLANNER™

Contact Information

383 Olympia Avenue
P.O. Box 1343
San Juan Bautista, CA. 95045
Phone: 831-623-2126
Fax: 831-623-2043
E-Mail:
mary@mlgfinancilplanning.com

We're on the Web
www.mlgFinancialPlanning.com

Publisher—Mary Lacey Gibson
Editing—Deborah Simmons

Thank you for your support. I really appreciate the referrals to family and friends I get from you and the trust in me that it implies. *Mary*

©2006 Mary Lacey Gibson, CFP®