

MARCH 2007



Summit

160 Bovet Road
Suite 405
San Mateo CA, 94402
info@summit-advisors.com
650-357-9410

Mark Pietrofesa

mark@summit-advisors.com
650-357-9410

Rafael Velez

rafael@summit-advisors.com
650-357-9410

William Fisher

william@summit-advisors.com
650-357-8812

Michael Radakovich

michael@summit-advisors.com
503-445-6661

Cristina Petersen

cristina@summit-advisors.com
650-357-8812

Slamming the Door on Identity Thieves

MAKE SURE YOUR FINANCIAL ACCOUNTS AND ELECTRONIC INFORMATION ARE PROTECTED AGAINST IDENTITY THEFT BY FOLLOWING THESE STEPS.

Imagine receiving an e-mail, purportedly from the Social Security Administration, that simply asks you to confirm your Social Security number to make sure you receive your annual benefit increase. It looks perfectly legitimate, down to the government agency's logo, but in fact, it's a scam.

"When you think about it, the Social Security Administration is not going to ask you for your Social Security number and they're not going to contact you via e-mail," says Steve Weisman, author of *50 Ways to Protect Your Identity and Your Credit* (Prentice Hall, 2005). Identity theft scammers count on the fact that a handful of unsuspecting victims will respond impulsively to an unsolicited e-mail and send their Social Security number—or, in other cases, their bank account or credit card numbers or other personal information. Identity thieves use the information to either open up an account in your name or to hijack an existing account. In either case, your credit can be severely damaged and you can spend countless hours undoing the mess.

WEALTHY AT HIGH RISK

Wealthy families in particular are at risk for identity theft; indeed, both Bill Gates and Oprah Winfrey have been victims. "Criminals go where the money is," says Weisman. What makes many wealthy people vulnerable is that they often have people working for them in their home who may have access to documents containing personal data. That's why it's wise to always conduct a background check on prospective employees.

High-net-worth families also often have money managers and accountants who can readily

obtain financial account information and Social Security numbers. Even if you trust them implicitly, says Weisman, it's wise to probe them about what security measures they're taking to protect your information. "They might be completely reliable, but sometimes they'll have people who work for them who aren't," he says. "It's best to find out what they're doing to protect you."

EDUCATE YOURSELF ABOUT SCAMS

Protecting your personal information is the key to thwarting identity thieves, and being aware of common scams is a big help, says Weisman. E-mails that claim to be from the government or a financial institution and that request personal information constitute one of the largest categories of scams known as "phishing." (You should never provide sensitive personal information in an e-mail.) But identity thieves don't just limit themselves to e-mail; they also call potential victims and pretend to be from a bank or government agency. "If you're contacted by someone who asks for personal information, don't give it," says Weisman, who was motivated to write a book on identity theft after someone stole his credit card at the gym and he became a victim. "If you think it might possibly be legitimate, then call a number you know is accurate at your bank or credit card company and talk to someone."

Other scams are more insidious. Identity thieves, for example, now share information about their victims with other criminals. "Other scammers call and say, 'We're from the government,'" says Weisman. "'And we know you have been scammed, and we are here to help you.' And they get them again." Also frightening is how identity thieves are now stealing people's

Slamming the Door on Identity Thieves

Continued from page 1

*“Protecting yourself
online also
requires vigilance.”*

medical insurance information to pay for their own health care. Not only can it be a financial burden for victims, it can also be extremely dangerous because it means that someone else’s medical information is in your files—a real problem when it comes to receiving the right blood type in an operation.

TAKING PROTECTIVE MEASURES

Protecting yourself completely against identity theft is almost impossible because so many governmental and private institutions maintain databases filled with your personal information. However, there are important steps you can take to lessen the chance that you’ll become a victim. Since identity thieves often steal bills and tax returns out of unlocked mailboxes, one simple step is to keep your mailbox locked. You should also keep any papers that have account or Social Security information in a secure place in your house.

Junk mail, particularly credit card offers, are also tempting items for identity thieves. They can fill out applications meant for you

and establish accounts in your name which they control. Reducing the volume of unwanted offers is a smart security measure that can be done by either logging onto www.optoutprescreen.com or calling 888-567-8688. Weisman also says that people can respond quickly to identity theft by scrutinizing their credit card statements and, at least once a year, reviewing a credit report for unauthorized activity. The three major credit reporting bureaus offer ongoing monitoring services that will alert you to possible fraudulent activity. They are: Equifax (www.equifax.com), Experian (formerly TRW; www.experian.com) and TransUnion (www.transunion.com).

Protecting yourself online also requires vigilance. Besides ignoring scam e-mails, be sure that your home computer’s spyware and firewall are up-to-date and operational. Also, if you make purchases online, be sure you use sites that display the padlock icon or use https in the URL address, both of which indicate a secure site.

For more information about strategies to avoid identity theft and protect your financial assets, contact your Financial Advisor. ■

This newsletter is provided by the firm listed on the header. This firm is either a registered investment adviser (“RIA”), qualifies for an exemption or exclusion from registration as an investment adviser or does not fall within the definition of an RIA under the Investment Advisers Act of 1940 (the “Act”) or applicable state laws. Any subsequent, direct communication by the firm with a prospective client shall be conducted by a representative that is registered, qualifies for an exemption or exclusion from registration in the state where the prospective client resides or is not defined as an investment adviser representative under the Act or any applicable state laws.

This newsletter contains general information that is not suitable for everyone. The information contained herein should not be construed as personalized investment advice. There is no guarantee that the views and opinions expressed in this newsletter will come to pass. Investing in financial markets involves gains and losses and may not be suitable for all investors. Information presented herein is subject to change without notice and should not be considered as a solicitation to buy or sell any security.