November 14, 2016

BURKE
FINANCIAL STRATEGIES
An Independent Firm

IDENTITY THEFT

Approximately 15 million United States residents have their identities used fraudulently each year, with financial losses totaling approximately $50 billion. This equates to one identity theft victim for every seven Americans, with an average loss of $3,500, every year.[1] Identity theft is big business, and is by far the fastest growing crime in the U.S. and around the world. Without taking significant steps to address this risk, we are all likely to be victimized someday.

On November 1, 2016, we sponsored a Continuing Education seminar titled Identity Theft Protection, Prevention and Awareness. Mr. Robert Siciliano presented this seminar to a group of Certified Public Accountants and clients. Mr. Siciliano is a nationally recognized authority on identity theft and cyber-crime, appearing on screen and in print throughout the country. In this article, I attempt to summarize Mr. Siciliano's wide-ranging, gripping and sobering presentation.

By now, most of us are generally aware of the various forms of identity theft, and the means by which identity thieves obtain the information needed to perpetrate a fraud. Unfortunately, identity thieves continue to "perfect their craft," so we all need to be very vigilant. In addition to the standard "new credit account fraud" and "account takeover fraud," thieves are now surreptitiously gaining access to individual email accounts. With access, thieves can review all past and current emails, and can assume a victim's identity online to then perpetrate a fraud. We have seen this at Raymond James, receiving emails from "our clients" directing us to wire funds to a third party. In this Newsletter article, I will focus on practical steps we can all take to minimize our risk and to protect ourselves in the event of a security breach.

Awareness:

- First and foremost, be on the look-out for nefarious attempts to gain personal information or access to our computer. Attempts come in many forms. Discuss risks and methods with all family members, especially children and the elderly.

Computers, Passwords and Anti-Virus:

- Never click on a link in an email unless you are absolutely certain of its authenticity.
- Stay out of your junk folder – it is a minefield.
- Install and keep current purchased (not free) anti-virus software. The top names all offer a quality product.
- Set Windows Updates to install automatically.
- Do not use the same password across sites, and do not use easy to hack passwords.

- Consider purchasing password manager software. For $20 to $40/year, password manager software stores and enters unique passwords for all sites, and will also generate unique passwords. All you need to remember is the one password for the software.
- Back up data, preferably on both a separate backup drive and with a cloud based service.
- Be wary of public Wi-Fi. Download a Wi-Fi Hotspot Shield.
- Cover the camera on your monitor when not in use.
- Consider enabling second authentication for accessing email.
- Surf the web carefully…avoid "sketchy" sites.

Credit Cards and other Consumer Credit:

- Set up text alerts, and receive a text summarizing each charge.
- Set up a Credit Freeze at all three credit agencies. Bogus attempts to open a new credit account will be thwarted because required credit information will be withheld. Setting up the freeze is free, at least in NJ. Once set up, the consumer can temporarily or permanently lift the credit freeze for a small fee. This freeze should be set up for kids and the elderly as well. This is your best means of protection should your social security number get in the wrong hands.
    - Equifax: 800-349-9960
    - Experian: 888-397-3742
    - TransUnion: 888-909-8872
- Consider purchasing a Credit Monitoring Service.
- Carefully review statements monthly.
- Every four months, run a free annual credit report from one of the three credit reporting agencies (rotating all three to cover a year). Reports can be accessed at www.annualcreditreport.com. Review report carefully.
- Consider blocking pre-screened offers of credit – www.optoutprescreen.com.

General:

- Shred all documents containing personally identifiable information.
- Receive and pay bills online – more secure than handling by mail.
- Consider a locking mailbox.
- Physically destroy old hard drives and phones. Do not sell used equipment.
- Have insurance agent check your driver's license annually (for tickets/accidents fraudulently assigned).
- Limit circulation of social security number. It is often requested but not always required (New Patient forms, for example).
- Do not pick up and plug in abandoned USBs.
- Be on the lookout for a Key Catcher – a device typically made to look like a USB drive that plugs into the back of a computer and captures and sends, by Wi-Fi, every keystroke.
- Look closely at all ATMs for a possible "skimming" device. Be aware of people "shoulder surfing."

- Discuss with your accountant the possibility of filing IRS Form 14039 – Identity Theft Affidavit. This form puts the IRS on notice that your personal information has been compromised, placing you at risk for the filing a fraudulent tax return. The IRS will provide a PIN to be used for subsequent filings. Note that any data breach, such as those at Home Depot and Target, enable you to file this form/affidavit.
- Check to see if your email account has been compromised in a data breach. Go to www.haveibeenpwned.com and enter your email address. You will see sites listed at which your email account and password have been stolen. You should promptly change your password at these sites.

PT Barnum once said "nobody ever went broke underestimating the intelligence of the American people." We are all gullible…we all have our weak spots. Be aware…and be careful out there.

Steven Criscuolo, CPA
Financial Advisor, RJFS
Chief Financial Officer

1 – www.identifytheft.info