STONEHEARTH
CAPITAL MANAGEMENT

IDENTITY THEFT

5/31/17

Reduce your chances of becoming a victim and what to do if you do become a victim.

As investment executives who specialize in helping our clients meet their financial goals, we understand that you may have questions about the areas you need to focus on during this phase in your life. This special report presents ways to reduce your chances of becoming a victim of identity theft, as well as what to do if you do become a victim.

WWW.STONEHEARTHCAPITAL.COM
199 ROSEWOOD DRIVE, SUITE 200 • DANVERS, MA 01923 • {978} 624-3000

Identity Theft

Identity theft is when someone wrongfully obtains your personal information and uses that information without your permission, usually for personal economic gain. The 2017 Identity Fraud Study released by Javelin Strategy & Research, found that $16 billion was stolen from 15.4 million U.S. consumers in 2016, compared with $15.3 billion and 13.1 million victims one year earlier.[1] This is a 16% increase in the number of victims. One in 20 U.S. citizens will become a victim of identity theft in 2017 costing them an average of $100 and an average of two months to clear their name.[2] We are all exposed to becoming victims. There is no way to entirely insulate yourself from this risk, however, there are some "best practices" that will certainly make it tougher for an identity thief to steal your identity. Below we will explore some of the more common examples of identity theft as well as tips to avoid them.

HIGHLIGHTS INCLUDE:

- Phone Calls
- Emails
- Password Management
- Mailboxes
- Protecting the Identity of your Children
- ATM Machines
- What to Do if you Become a Victim

1. PHONE CALLS

One tried and true way into your home is through the phone, whether it be your landline or your cell phone. As soon as you pick up the phone, the threat of identity theft increases. There are two particular threats that are currently trending in this space:

> **Threat #1:** Identity thieves are calling individuals pretending to be a representative from their credit card company. They claim there is a problem with your credit card, requiring reactivation to resolve. Reactivation requires that you punch your credit card numbers into your phone, and voila, you have just become a victim.
>
> **Threat #2:** Who doesn't want to win a free trip to the Caribbean? If it sounds too good to be true, then it is! In order to collect your winnings, you are required to pay a small "processing fee" that the thief can conveniently collect over the phone using your credit card. Not only will they collect your processing fee, but they will also make additional purchases using your stolen credit card.

[1] Identity Fraud Hits Record High with 15.4 Million U.S. Victims in 2016, Up 16 Percent According to New Javelin Strategy & Research Study. (n.d.). Retrieved May 31, 2017, from https://www.javelinstrategy.com/press-release/identity-fraud-hits-record-high-154-million-us-victims-2016-16-percent-according-new

[2] Briscoe, B. (2017, May 26). New Trends In Identity Theft | WFMYNEWS2.com. Retrieved May 31, 2017, from http://www.wfmynews2.com/news/local/2-wants-to-know/new-trends-in-identity-theft/443370704

TIPS:

- Don't presume that your caller ID will protect you. Identity thieves have figured out ways to hack the caller ID system so that it will show whatever they want it to.
- Never give personal information to someone that calls *YOU*. Instead, tell them that you do not have time to deal with it right now, but you will give them a call back shortly. This will give you enough time to verify their number and validate their claim.

2. EMAILS

I recently received an email informing me that my Apple ID had been used to log into a computer in Bangladesh. That didn't sound good. The email suggested that I click on the link below if I didn't recognize this computer. In doing my research on identity theft, I have become much more careful about clicking links within emails. So instead of clicking on the link, I logged into my Apple ID and changed my password. Shortly after, I received a confirmation email from Apple regarding my change of password. I compared the original email to this email and noticed that there were some discrepancies between the two pertaining to how they were formatted. I believe someone was trying to get me to click on the link below, which may download keystroke logging malware that will record my keystrokes.

Keystroke logging: Keystroke logging, often referred to as **keylogging** or **keyboard capturing**, is the action of recording (logging) the keys struck on a keyboard, typically covertly, so that the person using the keyboard is unaware that their actions are being monitored.[3]

TIPS:

- Do not click on any links within emails unless you are sure it is a legitimate email. Call the sender to verify that they indeed sent you the email.
- Watch out for short emails from friends and family asking you to "check out this site." Their email address has most likely been compromised.
- Make sure you run an updated antivirus/malware software on *ALL* of your electronic devices, including your smartphone.
- Make sure that your electronic device is running the most current operating system available. Ransomware called "Wannacry," recently spread throughout the world, gaining access to computer files that it encrypted with a request for payment in exchange for the key to get your data back. The targeted computers were running older operating systems.
- Back up your computer files on a regular basis either locally or to the cloud using secure tools such as "carbonite" or "dropbox" services. This way if you ever become a victim to ransomware you have a duplicate copy of your files that you can turn to.
- Do not send an email with personal information embedded in the body of the email or as an attachment. If necessary, then password protect the attached document or use a tool that will encrypt the email.[4]

[3] Wikipedia. (n.d.). Keystroke logging - Wikipedia. Retrieved May 31, 2017, from https://en.wikipedia.org/wiki/Keystroke_logging

[4] Kaufman, L. (2013, February 2). The Best Free Ways to Send Encrypted Email and Secure Messages. Retrieved May 31, 2017, from https://www.howtogeek.com/135638/the-best-free-ways-to-send-encrypted-email-and-secure-messages/

Remember the Target data breach in 2013 that resulted in stolen debit and credit card numbers? It all started with an email sent to an employee at Target's HVAC vendor. The email contained malware that enabled the hackers to gain access to the HVAC vendor's login credentials to Target's network (which was used to monitor the HVAC system). Unfortunately, Target did not segregate information on their network which means the HVAC vendor's access was all that was needed to view sales transactions stored on Target's network. [5]

3. PASSWORD MANAGEMENT

Passwords are a common gatekeeper to private, personal information. In the hands of unauthorized individuals, a substantial amount of damage can be done in a short period of time. Unfortunately, most people don't take their passwords seriously. Password management vendor, SplashData, found that the number one password used today is *password*.[6] Another popular one is a pet's name. Convenience comes at a price. We may not get burned today, but if we play with fire long enough we know we will eventually get burned.

TIPS:

- Passwords should NOT be something you can remember. Your pets' name is NOT a good password.
- Each site should have a different password; do not repeat them.
- Passwords should include: capital and lowercase characters, symbols and numbers.
- Passwords should be stored in a secure place.
- Consider a password management tool (such as Dashlane). These tools will encrypt and securely store your passwords in the cloud. They can generate "very secure" passwords upon request and they can also give you an analysis of how secure your existing passwords are and how many times you are using the same password for two different access points. This solution still requires that you remember one master password to get into the password management system. One additional benefit is that you can share this with someone your trust, like your spouse.
- When available turn on two-factor authentication.

4. MAILBOXES

53% of identity theft occurs by physically stealing your information.[7] One of the more popular scams is to simply steal the credit card offers that you receive right out of your mailbox. Thieves submit the application for credit and return for the physical credit card when it finally arrives in the mail.

[5] Kassner, M. (2016, February 2). Anatomy of the Target data breach: Missed opportunities and lessons learned | ZDNet. Retrieved May 31, 2017 from http://www.zdnet.com/article/anatomy-of-the-target-data-breach-missed-opportunities-and-lessons-learned/

[6] Gray, R. (2013, September 12). Most common and hackable passwords on the internet. Retrieved May 31, 2017, from www.telegraph.co.uk/technology/internet-security/10303159/Most-common-and-hackable-passwords-on-the-internet.html

[7] Briscoe, B. (2017, May 26). New Trends In Identity Theft | WFMYNEWS2.com. Retrieved May 31, 2017, from http://www.wfmynews2.com/news/local/2-wants-to-know/new-trends-in-identity-theft/443370704

TIPS:

- Consider using a P.O. Box instead of a mailbox. If you prefer a mailbox, then consider one with a locking mechanism on it.
- Actively monitor your credit report.
    - Sign up for a credit monitoring service such as IDSheild ($$) or CreditKarma (free).
    - Check your credit report at least annually. You are entitled to a free report each year from EACH of the three credit bureaus, so it is possible to get a copy every 4 months if you stagger the requests.
    - Consider freezing your credit. Safest solution, but a bit inconvenient. Massachusetts charges $5 per credit bureau each time you freeze or unfreeze your credit.
- Sign up to stop those credit offers at www.optoutprescreen.com or national mailings lists, at www.dmachoice.org.
- Be sure to shred your credit card offers. Do not just throw them in the trash.

5. PROTECT THE IDENTITY OF YOUR CHILDREN

A study done by Carnegie Mellon CyLab found that identity theft was 51 times greater for children than for adults.[8] Children under the age of 18 cannot apply for their own credit card. So in theory, you would expect most, if not all, children NOT to have a credit profile. However, there is a glitch in the system. The credit bureaus create your profile when you apply for credit. They verify your social security number, but not your name and date of birth. Thieves are applying for credit with a valid social security number (which they stole from a child) but with a fake name and date of birth (over age 18). Since the child or their parents presume there is no credit report, they never think to request a copy of their credit report. By the time your child applies for credit, the damage is done and will take a long time to recover from.

TIPS:

- Check your children's credit report from each of the three credit bureaus. Hopefully, nothing will turn up.
- Limit who you share your child's social security number with. Many companies have just grown used to asking for this information when in reality there may be no real purpose for them having it.

6. ATM MACHINES

ATM fraud here in the U.S. is up over 500% in just one year. [9] Thieves are inserting small cameras, skimmers (devices used to read your card as you insert it) and fake keypads that record your PIN entry all in the pursuit of capturing your personal information.

[8] Weisman, S. (2015). *Identity theft alert: 10 rules you must follow to protect yourself from America's #1 crime* (2nd ed.). Upper Saddle River, NJ: Pearson Education, Inc.
[9] Boyce, L. (2016, April 18). Five signs an ATM has been tampered with. Retrieved May 21, 2017 from http://www.thisismoney.co.uk/money/saving/article-3545646/Criminals-taking-quick-hit-approach-cash-machine-fraud-expert-warns-five-signs-ATM-tampered-with.html

TIPS:

- Cover the keypad with your other hand before entering your PIN.
- Never use an ATM that looks like it has been tampered with.
- Be wary of private ATM machines found in restaurants, convenience stores and shopping outlets. When possible use the ATM machines found at the banks. Private machines are more prone to being tampered with.

6. WHAT TO DO IF YOU BECOME A VICTIM

Despite your best efforts, you may still become a victim of identity theft, sometimes through no fault of your own (aka Target). If you become a victim here are some suggestions to follow:

- Visit IdentityTheft.gov and click "Get Started." This site is provided by the Federal Trade Commission (FTC), the nation's consumer protection agency. The site will provide tips, worksheets, blank forms and sample letters to guide you through the recovery process.
- In the event of credit card fraud, contact the provider immediately to cancel your card and to have a new one issued. Your bank will have a process that you need to follow to request any fraudulent charges be credited back to your account.
- Contact one of the credit bureaus to request an initial fraud alert. You only need to call one. That bureau is required to contact the other two.
    - Equifax: 800.525.6285
    - Experian: 888.397.3742
    - TransUnion: 800.680.7289

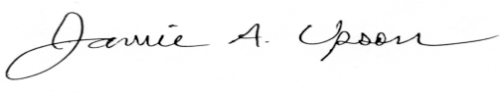
- Placing an initial fraud alert entitles you to a free credit report from each of the credit bureaus. Take advantage of this and review the reports for fraudulent activity.
- Consider putting a credit freeze on your account with all three bureaus (freezes require that you notify all three bureaus). This should prevent new credit accounts from being created.
- Consider subscribing to a credit monitoring service, like IDShield. They typically have identify theft specialists who can help guide you.
- Update passwords immediately for all impacted accounts.
- Notify the credit bureaus, in writing, to dispute the fraudulent activity on your credit report and request that it be removed from your files. A report from the police and/or an identity theft affidavit from the FTC may be required.

Be sure to share your identity theft stories with others to increase awareness. Last summer, my wife and I took our kids on a trip to Washington D.C. We decided to drive. During our trip, we stopped to eat, to fill up the gas tank and for bathroom breaks. A couple weeks later, I received a call from my credit card company. Their identity theft division flagged a purchase done within the past hour at a Sears in Connecticut for $1,000 even. I was at my office in Danvers, Massachusetts when I received the call. I verified that my credit card was in fact in my possession.

My best guess is that, when we stopped for dinner in Connecticut, the waitress took my credit card to process the payment and my credit card was out of sight for a couple of minutes. Those couple of minutes provided ample time for someone to copy the information on my card. I also recall the waitress taking an interest in where we lived, which at the time I thought she was just being friendly. My credit card provider quickly reversed the charge and didn't even hit me up with the $50 fee that they could have charged me. I have told this story ever since, and I find that most others have an identity theft story of their own. The paths thieves take to steal personal information will inevitably change, but the outcome remains the same. Stay alert my friends!

As always, if you have any questions, please lean on us here at Stonehearth Capital Management. We are here to help.

Sincerely,



Jamie A. Upson, CFP®, CMFC, AAMS
President & CEO
Jamie@stonehearthcapital.com

David Juliano CLU, ChFC, RICP
Senior Financial Advisor
David@stonehearthcapital.com

Footnotes, disclosures and sources:

Stonehearth Capital Management, LLC is a Registered Investment Advisor. Registration does not imply a certain level of skill or training.

Opinions, estimates, forecasts and statements of financial market trends that are based on current market conditions constitute our judgment and are subject to change without notice.

This material is for information purposes only and is not intended as an offer or solicitation with respect to the purchase or sale of any security.

Investing involves risk including the potential loss of principal. No investment strategy can guarantee a profit or protect against loss in periods of declining values.

Diversification cannot guarantee a profit or protect against loss in a declining market.

Opinions expressed are not intended as investment advice or to predict future performance.

Past performance does not guarantee future results.

Consult your financial professional before making any investment decision.

Opinions expressed are subject to change without notice and are not intended as investment advice or to predict future performance.

All information is believed to be from reliable sources; however, we make no representation as to its completeness or accuracy. Please consult your financial advisor for further information.

These should not be construed as investment advice. Neither the named representative nor the named Broker dealer or Investment Advisor gives tax or legal advice. All information is believed to be from reliable sources; however, we make no representation as to its completeness or accuracy. Please consult your financial advisor for further information.

By clicking on these links, you will leave our server, as they are located on another server. We have not independently verified the information available through this link. The link is provided to you as a matter of interest. Please click on the links below to leave and proceed to the selected site.