WEALTHSPIRE ADVISORS

WHITEPAPER | October 2017

Keep Your Identity to Yourself!

Bill Schwartz, CPA, CFP®, Managing Director

Tim Hughes, CFP®, Managing Director

Keep Your Identity to Yourself!

Bill Schwartz, CPA, CFP®, Managing Director

Tim Hughes, CFP®, Managing Director

With all the recent headlines from the hacking of consumer data at Equifax, combined with data breaches over the years at Target, JPMorgan Chase, Yahoo!, Sony, and many more, it is probably safe to assume that your personal financial data is not completely secure in our cyber world. Per a recent study by Javelin Research out of Pleasanton, California, about one out of every sixteen US consumers were a victim of identity fraud in 2016, with damages close to $16 billion[1].

Further, most victims are not even aware that they have been hacked for many months. Fraudsters using your basic financial information can file tax returns in your name to make refund claims, open new credit cards or other credit facilities in your name, steal government benefits, damage your credit status, attempt to wire funds from your accounts, and much more.

Per Federal Trade Commission (FTC) data from 2015, the states (including Washington, DC) with the highest incidents of identity theft (per capita) are[2]:

1. Missouri
2. Washington, DC
3. Connecticut
4. Florida
5. Maryland
6. Illinois
7. Michigan
8. Georgia
9. Texas
10. New Hampshire

And not to leave out our friends from Wisconsin and Virginia, they are ranked 13th and 22nd respectively on this discreditable list.

Recovering from identity theft is a long and arduous process, and although most of the monetary damage can be corrected over time, you could end up being out more money than you think. Legal fees, late charges and penalties, lost wages, credit monitoring expenses, etc. could cost thousands of dollars. In addition, the time and emotional distress of identity theft and fraud should not be discounted.

So, what can be done to minimize the chances of identity theft and fraud? Well, there is no simple answer, and prudence requires awareness of the multiple ways in which we are vulnerable. Below are a few of our suggestions:

Online, Be Alert

Make sure you understand with whom and why you are sharing personal financial information:

- Avoid phishing emails by not opening files, clicking on links, or downloading programs sent by anyone you do not know. Phishing has become very sophisticated and can be among the most successful vehicles for hackers.
- Use strong passwords (include numeric and special characters), and change them somewhat regularly. Avoid simple passwords that can be easily identified in a dictionary search, or with you, such as children's names, favorite sports teams, home address, phone numbers, etc. Also, do not use the same password for your e-mail and online accounts.
- Use dual factor identification whenever possible. For example, at Schwab, using a mobile app, you can obtain one-time password protection, which is a single-use numeric password that you use in addition to your usual password when logging in to Schwab's website. You can call 1.800.435.4000 to enroll.
- Do not give personal information on the phone unless you have initiated the contact.

- Remember to wipe an old computer or cell phone of all data before trading it in for a newer model.
- Use encryption on data and messages whenever possible.
- Sign up for credit monitoring.
- Never post personal financial data on social media or send via email.
- Use security software such as anti-virus software, anti-spyware software, and a firewall.
- Be careful using any public wireless/wi-fi network, and never send any personal financial data on an unprotected network.
- Although convenient, do not use an automatic login feature that saves your username and password, and always use the logoff function when finished with a website or app.
- Consider freezing your credit (more info below).
- Consider establishing an account with Social Security and safeguarding the credentials.

Even Offline, Keep Your Information Secure

Although intuitive, there are a few things on this list that I'm sure many of us do not always do:

- Keep your financial documents and records in a secure place at home (safe) or in a safe deposit box at a bank.
- Lock your wallet or purse in a safe place at work.
- Limit what you keep in your wallet or purse, taking only the identification and debit/credit cards that you will need at the time. Leave Social Security cards at home.
- Shred receipts, credit card offers and applications, insurance forms, checks and bank statements and physician statements when you no longer need them.
- Remove and destroy the labels on prescription bottles before you dispose of them.
- Take outgoing mail to the post office or at least a collection box. Also, remove mail from your mailbox as soon as possible.

Other Actions to Consider

- Consider establishing an online account with the Social Security Administration (before someone else does). This allows you to control your account before a hacker could falsely create one with your social security number. To do so, go here: https://www.ssa.gov/myaccount/
- A credit freeze allows you to restrict access to your credit report, which makes it more difficult for someone (including yourself) to open an account or loan in your name (as an FYI, the freeze does not impact your credit score). To place a freeze on your credit report, you would have to contact each of the nationwide credit bureaus (and there is a fee based upon your state of residence):
  - Equifax - 1.800.349.9960, www.freeze.equifax.com
  - Experian - 1.888.397.3742, www.experian.com/freeze
  - TransUnion - 1.888.909.8872, www.transunion.com/credit-freeze/place-credit-freeze2

You have flexibility to lift the freeze, temporarily or permanently, if you need to open a new account, buy a house or rent an apartment, etc.

- A fraud alert allows new accounts or loans to be opened, but only after a verification process. There are three types of fraud alerts available:
  - Initial Fraud Alert - If you are concerned about identity theft, but have not become a victim, this alert will protect your credit from unverified access for 90 days.
  - Extended Fraud Alert - For victims of identity theft, this will protect your credit from unverified access for seven years.
  - Active Duty Military Alert - For those in the military who want to protect their credit while deployed, this protection lasts for one year.

To place a fraud alert on your credit report, you would have to contact one of the nationwide credit bureaus (there is no fee to place a fraud alert).

- Many insurance companies, including the major insurers such as State Farm and Allstate, offer identity-theft insurance as a rider to your homeowners or renters insurance policies. Although not terribly expensive (as little as $25 to $50 per year), the insurance (generally up to $25,000) is mostly to cover expenses (such as legal fees, etc. mentioned above) accrued while repairing your credit. Some policies will provide a consultant or case manager to help you clean up the mess.

If You Suspect Identity Theft

If you suspect you have become a victim of identity theft, consider acting quickly to minimize any negative consequences:

- Place a fraud alert or credit freeze on your accounts.
- Contact any vendor, bank or institution directly affected.
- Contact the FTC and file an Identity Theft Affidavit and create an Identity Theft Report. You can file your report by calling 1.877.438.4338, or going to www.IdentityTheft.gov.
- Contact your local law enforcement and file a police report. This police report, combined with the Identity Theft Affidavit, are needed to create your Identity Theft Report. This report will be necessary when working with the credit reporting agencies and others in repairing your credit.
- If your social security number was compromised, contact the Social Security Administration (SSA) at 1.800.269.0271 and the Internal Revenue Service (IRS) at 1.800.829.0433.
- Contact the Postal Inspection Service (the law enforcement and security branch of the postal service) if you believe the theft or fraud was committed by mail, or if any fraudulent change-of-address forms were submitted.

Clearly, this list is (exhausting, but) not exhaustive, so to obtain more information, please see the FTC website for details.

With more and more of our lives being realized online, including our financial information, and with criminals in a continuous game of technological one-upmanship with law enforcement, what the future holds for data security is unknown. Will biometric and other technologies make us (and our data) more secure, or will sophisticated fraudsters stay one step ahead? Regardless of the ultimate answer, doing what you can to minimize identity theft and fraud seems to make a lot of sense.

If you would like to discuss any of this in greater detail, please do not hesitate to reach out to your Wealthspire advisor. Stay safe!

Footnotes

1 https://www.javelinstrategy.com/coverage-area/2017-identity-fraud

2 https://www.ftc.gov/news-events/press-releases/2017/03/ftc-releases-annual-summary-consumer-complaints