PROTECTING YOUR FINANCES IN THE AGE OF CYBERCRIME

Poole Locke Associates

Retirement Income Source®

Protecting Your Finances in the Age of Cybercrime

By David J. Scranton, CFA®, CFP®, ChFC, CLU

Few inventions in recorded history have revolutionized the way we live like the Internet. It has changed the way we communicate and has made thousands of previously slow, complex processes faster and more efficient. Yet, while solving old problems, the Internet — like any invention — has also created new ones. Among the biggest of those problems is the vulnerability of sensitive and/or personal information to a relatively new breed of criminal: cyberthieves.

Most of the country was personally impacted by this problem in September 2017 when Equifax reported a security breach that allowed hackers to access the personal information of 143 million Americans. Equifax is one of three major credit reporting agencies (Experian and TransUnion are the others), and all keep extensive databases of credit-user information that include everything from dates of birth to addresses to Social Security numbers. Once a cyber thief gains access to such information, they can use it to steal your identity and potentially gain access to your credit accounts and personal finances.

Electronic identity theft can ruin a family financially, and unfortunately, it is an issue with no easy solution. According to a 2017 study by Javelin Strategy & Research, between 2011 and 2017, identity thieves stole over $107 billion. In 2016 alone, some $16 billion was stolen from 15.4 million U.S. consumers, up from $15.3 billion stolen from 13.1 million victims a year earlier.[1] The increase illustrates that even as cybersecurity measures improve, criminals become increasingly savvy.

Greater Risk for Older Americans

The bottom line is that keeping our identities and finances safe from criminals in the digital age will be an ongoing challenge for both businesses and individuals. That's especially true for individuals at or near retirement age whose accumulated assets can potentially make them more attractive targets for thieves than younger people who are still in the early process of building their wealth. A top priority for most Americans over age 50 should be "financial defense," which means they should focus on the use of strategies designed to generate income and protect assets from major losses due to extreme fluctuations in the financial markets. In the digital age, however, another essential component of financial defense is cybersecurity: knowing how to protect your identity as you do everything from online shopping and banking to buying gas.

Along with personal accountability, it's important to know that the businesses and institutions in charge of safeguarding your money are also doing their job and employing the most advanced cybersecurity measures available.

In this report, we'll discuss both reactive measures and proactive measures you can use to protect yourself and your finances, depending on the circumstances:

- Reactive: When you're worried about the potential repercussions of a known security breach in which your information may have been compromised (such as Equifax).
- Proactive: When you want to better ensure your information is safe from future hacks.

Reactive Defense

There is some overlap in the two categories, but let's start with reactive measures you can take in response to an incident such as the Equifax breach:

Freeze Your Credit: Equifax offered a free credit freeze following the breach to help block thieves from opening accounts under their victims' names. Equifax made the offer because there is usually a cost of around $10 to freeze a credit account and an additional cost for unfreezing it — the latter of which can also be a time-consuming process. Nevertheless, freezing your credit is a good initial defensive measure in such an incident, not unlike calling to cancel a specific credit card when you've lost it and fear it might be found and used fraudulently.

Monitor Your Accounts: The sheer volume of the Equifax breach allowed perpetrators the ability to make purchases with stolen credit information — but only if victimized cardholders failed to keep a close eye on their accounts. Although an identity theft victim isn't ostensibly responsible for bogus credit card charges, thieves are becoming better at hiding their activity, and if you don't spot and report a bogus charge, you may end up being liable for it. With that in mind, you might want to consider setting up mobile transaction alerts for your cards if you don't already have them. You should also get in the habit of reviewing your checking and savings accounts every day and monitoring your FICO credit score every month. Lastly, get your latest credit reports from all three reporting bureaus and look through them carefully in search of mistakes.

Increase Your Security: You can boost the security of your accounts by signing up for two-factor authentication. This would require using not only a password but also a one-time code sent to your cell phone to access your accounts, thus making it doubly hard for anyone else to gain access. You should also consider setting up a PIN code with your wireless provider to better ensure that a customer service representative can't be tricked into allowing a stranger to access your phone.

Keep an Eye on Your Mail: Cyberthieves sometimes also use stolen information to send phishing emails, which appear legitimate but contain links to malware. Once you click on them, you may fall victim to encrypted ransomware, which kidnaps your personal files by blocking you out of them until you've paid a ransom. Thus, one essential security measure is to back up your important data on a hard drive. You should also read all emails carefully before responding, even if you believe you recognize the sender. Savvy scammers these days can commandeer familiar names and logos, so pay close attention to anything that might seem off or strange about an email and report it without clicking on any embedded links. Be aware, for example, that the IRS never initiates contact with taxpayers via email or text message to request personal information.

If you ever receive a suspicious email or text from the IRS, immediately report it by sending an email to phishing@irs.gov or by calling 1-800-366-4484. Also, be just as attentive to your mail delivered the old-fashioned way. For example, look closely at those "explanation of benefits letters" you get from your healthcare provider and make sure you recognize all the services and charges listed.

Pay Attention to Your Taxes: Credit card theft represents just one element of your finances that can be put at risk by identity thieves. They can also get their hands on your tax refund if you don't take action to stop them. File your return early, and if you believe you've been victimized, file the IRS's identity-theft affidavit, Form 14039, available at www.irs.gov.

Proactive Defense

Some of the reactive defensive measures described above are also proactive steps you can take to better protect yourself from having your personal information compromised in the future—in addition to preventing cyber thieves from using the information fraudulently once they've already obtained it. There are also some additional proactive measures that experts recommend, including the following:

Maximize Password Protection: Passwords can be a pain (especially when we all have so many to remember nowadays), but you should never underestimate their importance or settle for weak passwords just for the sake of convenience. On the contrary, you should create strong passwords and update them frequently. Avoid common bases such as birthdates, pet names, children's names, or your mother's maiden name. Use combinations of lowercase letters, capital letters, numbers, and punctuation symbols. And, again, change your passwords periodically to keep them even stronger.

Don't Overshare on Social Media: Baby Boomers are among the biggest users of Facebook, LinkedIn, Twitter, and several other social media networks these days. And while they are generally less prone to "oversharing" personal information than younger users, they are not immune from making mistakes. Keep any information that a criminal might use from social media and monitor your settings and filters to limit the potential for strangers to have access to everything you post. It can sometimes seem like a futile effort in the age of "viral" online media, but it's well worth it.

Store Digital Records and Paper Records Safely: After a while, it may be easy to lose track of how much personal and financial information may be stored on your computer. But, if you're like most people, odds are it's a lot. Thus, it's important to make sure you have a firewall installed, are using and updating anti-virus and anti-spyware software, are keeping your browser updated, and are keeping your wireless network secure. When getting rid of any documents with financial information, such as tax records, be sure to shred them—and store any such documents you are keeping under lock and key. Under lock and key is also a good place to store your Social Security card; your purse or wallet is NOT!

Secure Your Phone: If you're using an app to do your banking or track your finances on your mobile device, make sure it's one with a good rating and is from a reputable company. Again, it's also smart to secure your phone/mobile device with a strong, frequently updated password and use its auto-lock feature to prevent access if it should fall into the wrong hands.

Discuss Security with Your Financial Advisor: Make a call or set up a meeting to have a frank discussion with your broker or financial advisor to ensure that they and the partner organizations handling your accounts are committed to protecting your information with the most advanced and thorough security measures available. Ask about internal policies in areas such as employee training, background checks, hard copy security measures, and electronic password protection. Ask what kind of cybersecurity insurance they carry and about vetting policies for vendors and administrative organizations they work with. Ideally, those organizations will have additional strict security measures of their own in place, as well as (in the case of a brokerage firm, for instance) an asset protection guarantee from cyber loss.

Helpful Links

In addition to the measures discussed above, if you ever suspect your identity has been stolen, it's important to file a report with the Federal Trade Commission, which you can do online at www.identitytheft.gov.

Although the FTC cannot recover any actual financial loss you may have already incurred, it can help protect you against further criminal activity and launch an investigation on your behalf.

If you believe a bogus tax return may have been filed under your Social Security number or you believe you may be at risk of that happening due to someone gaining access to your SSN (for example, based on losing your wallet or suspicious credit card activity), you should contact the IRS Protection Specialized Unit at 1-800-908-4490.

Again, playing good "financial defense" is essential, particularly for investors within 10 to 15 years of retirement. In the online age, that means taking steps to make sure your assets are protected from unnecessary market risk and loss due to cyber theft!

Sources:

1. https://javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin

Poole Locke
Associates
Retirement Income Source®

1521 Concord Pike, Suite 103 West, Wilmington, DE 19803
(302) 439-0733 | poolelocke@poolelocke.com | www.poolelocke.com

Investment Advisory Services offered through Sound Income Strategies, LLC, an SEC Registered Investment Advisory Firm. Poole Locke Associates and Sound Income Strategies, LLC are not associated entities. Poole Locke Associates is a franchisee of Retirement Income Source®, LLC. Sound Income Strategies, LLC and Retirement Income Source®, LLC are associated entities.