INVESTMENT INSIGHT
2017
THIRD QUARTER
LEGACY WEALTH MANAGEMENT

CYBERSECURITY

Protecting your financial information

In light of media attention to the most recent breach in cybersecurity, this time by Equifax, we are using this issue of* Investment Insight *to highlight the facts behind the incident and discuss both what you can do in response as well as what Legacy's daily practices are to protect your private information. If you have questions after reading this information on cybersecurity, feel free to contact your relationship manager at Legacy.

While our steadfast approach on doing what is best for our clients has not changed over the 35 plus years we've been in business, the investment industry has been dramatically altered as computer technology has become a part of everyday life. As we increasingly rely on computers in every aspect of our financial lives, from making investments and transferring funds, to tracking our portfolios and planning for the future, we enjoy a level of convenience, efficiency and time savings unimaginable when our firm first began in 1982. However, with this incredibly powerful tool comes risks – cybercrime, hacking, phishing, malware, spoofing. These once new words have become increasingly familiar terms in describing threats of criminal activity.

At Legacy Wealth Management, we take these threats seriously and have implemented a series of security steps to protect against attempted cyber intrusions. This issue of *Investment Insight* describes some of the more common threats, how we protect your information, and steps you can take to protect yourself against the risk of falling victim to cyber criminals.

$16 billion was stolen from 15.4 million U.S. consumers in 2016. . . . In the past six years identity thieves have stolen over $107 billion.

Cybercrime is Real

Fraudsters trick their victims into responding to official looking emails asking for identity details or passwords (spoofing, phishing). They convince victims to download seemingly innocent files that contain malicious bits of software (malware) that can steal identity information and take control of computers. They find weaknesses in firewalls, use stolen passwords or break through weak defenses, accessing email and other accounts (hacking) to impersonate their victims.

The Equifax Security Breach

As you likely now have heard, earlier in the year Equifax suffered a security breach which has potentially exposed about 143 million Americans' personal information, including names, addresses, dates of birth and Social Security numbers. In the wake of this breach, we recommend that you do the following:

Determine Your Impact

Visit https://trustedidpremier.com/eligibility/eligibility.html to determine if you may have been impacted by this incident.

Enroll in Identity Theft Protection

Regardless of whether your information was or was not compromised, you can enroll in Equifax's complimentary identify theft protection and credit file monitoring services using the link you used to determine your impact https://trustedidpremier.com/eligibility/eligibility.html. Equifax is offering this service *free* to all Americans for one year. The deadline to enroll ends on Tuesday, November 21, 2017.

As an alternative to Equifax's free service you can sign up, for a monthly/annual fee, for another identity theft protection service with another provider (i.e. Lifelock, etc.).

Check Your Credit Periodically

You are entitled to one free credit report annually from each of the three credit bureaus, Experian, Equifax, and TransUnion. One strategy is to request your free credit report from one of the credit bureaus every 3-4 months; this way you can verify your credit report's accuracy periodically. To check your credit report visit: www.annualcreditreport.com – this is the *only* website where you can access your free, annual credit report; please beware of other websites offering "free" credit reports.

Set a Fraud Alert

Visit https://www.alerts.equifax.com/AutoFraud_Online/jsp/fraudAlert.jsp in order to set a temporary, 90-day fraud alert at each of the three credit bureaus. The fraud alert on your credit report notifies potential creditors to take additional steps to verify your identification before they extend credit in your name; this makes it harder for an identity thief to open illegitimate accounts in your name since you will receive an alert and be prompted to verify your identity before establishing a new account/credit line.

If you would like to take things one step further you can **Freeze your Credit**, preventing potential lenders and creditors from having any access to your credit report and therefore preventing thieves from establishing new credit in your name even if they do have your personal information. You must place a credit freeze on your accounts at all three credit bureaus individually and there can be a nominal fee ($3 to $10) associated with this action.

Freezing your credit files has no impact on your existing credit or your access to your exiting lines of credit. Once a freeze is in place, you have to go into each credit reporting agency and temporarily lift the freeze in order to establish new credit (i.e. open a new credit card, get a car loan, etc.). To lift the freeze you will need to use the unique personal identification number (PIN) you established for each of the three credit bureaus.

If keeping PIN numbers organized is a difficult task for you, this might not be the best option. If you lose the PIN, you will have to reestablish a new PIN prior to lifting the freeze. Reestablishing your PIN will require additional work which includes providing key documents that prove your identification (birth certificate, driver's license, etc.). Please consider this option carefully before freezing your credit. If you have questions or would like to discuss this option further, please contact your relationship manager.

Because microchip technology has made it difficult for thieves to duplicate your credit cards, criminals now focus on new account fraud. New account fraud occurs when a thief opens an account using stolen personal information.

You Can Protect Yourself

Many consumers, particularly those new to technology, can find the ease and convenience of computers alluring. This can lull the unwary into dropping the common sense caution they would normally use when dealing with their finances. Carelessness when managing personal identity security can lead to identity theft and loss.

One of the most important steps you can take to protect your identity is to protect your passwords. Have strong passwords and use different passwords for each account. Know who you are dealing with on line. Just because an unsolicited communication asking for personal information says it is from a trusted source, don't automatically assume that it is legitimate. Verify the request through a phone call or an email that you have on file from the organization. Make sure your anti-virus and anti-spyware software is up to date on all connected devices, and run periodic scans. Ensure that your computers and network devices are kept up to date and supported by the manufacturer so they have the latest security features to match new threats.

Ways to Protect Your Data

Be strategic with user names and passwords

- create passwords with 8-12 characters, upper and lower case letters, numbers and symbols
- use a unique password for each account
- change passwords often (every 90 days)

Limit what you share on line

- be selective about the information shared on social media and with whom you share it
- keep your personal information private (home address, phone # and birth date)
- use two-factor authentication where available

Safeguard email accounts

- obtain secure storage programs to archive sensitive, private data and documents
- delete all emails that include financial info

Surf safely

- use wireless networks you trust and know are protected
- be sure to log out of web sites completely
- download legitimate apps from trusted publishers

Keep your equipment up to date

- ensure that you've installed the latest versions of software and patches are up to date
- run regular scans to update software

Protecting Your Information at Legacy Wealth Management

At Legacy Wealth Management, we recognize the advantages of computer technology as well as the potential risks it poses. Our over-arching approach to cybersecurity can be summed up in the phrase "know our clients." That is why we have strict rules about how we handle clients' requests for transfers and distributions. We also maintain internal security procedures within our own computer systems to block unauthorized access.

The threats are real; cybercrime is real. But we can continue to benefit from powerful computer technology and thwart cybercriminals by being aware of the risks and taking common sense steps to protect data and personal identity.

We have several compliance policies that address protecting your data. They include our Privacy Policy, Business Continuity Plan, ID Theft Policy and Cybersecurity Policy.

The following lists just a few of the activities that are performed by Legacy to protect your data.

- Hired a cybersecurity vendor who conducted baseline penetration and vulnerability tests; these tests are conducted annually, and servers and computers are monitored daily for intrusion
- Cybersecurity vendor conducts phishing email testing on employees
- Anti-virus provider sends notifications of virus/Trojan files trying to attack computers
- Email security provider prevents/ blocks malicious emails
- Back up all servers and data on a daily basis
- Frequent cybersecurity training of staff; training on common fraud schemes
- Verification of all wire transfers
- Do not allow use of unencrypted flash drives; any outside flash drives are scanned by a computer not connected to our network
- Employees are forced to change their login password every 90 days
- Desktop computers log out after 15 minutes of inactivity
- Server room is locked 24/7
- Third party vendor due diligence
- Do not send client account numbers or social security numbers by email
- a secure client portal is used for passing sensitive information
- PC's are set to check and install updates nightly

This Third Quarter *Investment Insight* was edited by Cathy Simmons, Legacy's Chief Compliance Officer, and Brienne Jackson, a Legacy Director of Financial Planning.

Sources:
Charles Schwab
Javelin Strategy & Research, 2017 Identity Fraud Study

LEGACY WEALTH MANAGEMENT | Right by you.

1715 Aaron Brenner Drive, Suite 301
Memphis, TN 38120
Phone#: (901)758-9006 Toll Free#: (888)326-8554 www.legacywealth.com