Ginsburg Financial Advisors, Inc.
Personal Financial Planning & Investment Management
Larry P. Ginsburg, CFP® **Adele Ostomel, CFP®**

phone: **(510) 339-3933**
fax: (510) 339-1611
LGinsburg@GinsburgAdvisors.com
AOstomel@GinsburgAdvisors.com

We are all Probably at Risk for Cybercrime

What can we do to minimize the potential of becoming a victim?

▲ Why is cybercrime important to me?

The increasing use of the internet and internet-enabled devices (i.e. any device connected to the internet such as computers/laptops, mobile phones, and tablets) in all aspects of our daily lives has made us more and more exposed to cybercriminals. As a society, we have come to rely on the internet to complete our everyday tasks, in both personal and business matters. This increasing reliance on the internet, especially for banking and commerce, made us all more vulnerable to cybercrime. We learned about the extent of the threat of cybercrime at a recent conference. Our goal is to share helpful information to reduce the possibility of you becoming a victim of cybercrime.

▲ How pervasive is the threat of cybercrime?

Widespread use of the internet has manifested into what has been coined the “Internet of Things” (“IoT”). The IoT is much broader than conventional internet-enabled devices and includes “smart” thermostats and home security systems, heart monitor implants, biochip transponders for animals, automobile sensors, or any other device that can transmit data over the internet. Forbes predicts that by the year 2025, there will be over 80 billion devices connected to the internet. As the number of devices increases, so too will the opportunity for cybercriminals to hack into unsecured devices (or inadequately secured devices) to obtain personal and financial information.

▲ What do the experts say about the threat of cybercrime?

We recently attended a conference where the speaker presented on the topic of “Cyber Crimes and the Increased Threat of Fraud”. The speaker’s background includes over 17 years spent with the FBI. He is currently Chief of Financial Crimes Investigations at a large national financial services company where he is responsible for the enterprise-wide Anti-Money Laundering, OFAC/Sanctions, Fraud Prevention and Internal Investigative programs of the firm. In his prior role with the FBI, he worked as a senior executive at FBI Headquarters in Washington D.C. where he oversaw the Cyber Division's efforts to combat the highest priority cyber threats emanating from Asia, Eurasia, Middle East, and Africa.

In the conference, we learned that a significant amount of attention is being directed to a myriad of massive-scale cyber-intrusions and the subsequent fallout, resulting in the loss of personal identifying or non-public information. Some recent examples you may have heard of include the data breaches at Target and Equifax. What you may not know is how this stolen information is being used. Cybercriminals are becoming more strategic in how they choose their targets. Compromised emails from financial institutions, where criminals recognize the opportunity to target individuals with a financial account(s), are used for phishing attacks (phishing is the attempt to obtain sensitive information such as usernames, passwords, credit card details and money, often disguising as a trustworthy entity in an electronic communication). An example of a phishing attempt is when you receive an email from your bank account, letting you know that they require updated information, and providing a link for you to enter personal information such as account number, birthdate, or social security number. No financial institution will ask you for such information via an email. (NEVER respond to such messages or click on the attachment or website!)

These types of cybercrimes are rarely a “one and done” event. Equal attention should be focused on the aftermath of the data breach, not just by companies who were breached, but by victims who have had their identity and information compromised. We learned that

if you have been a victim of fraud or identity theft once, you are usually put on a list sold to scammers and are more likely to be targeted for potential cybercrime in the future.

▲ How your accounts are protected at Ginsburg Financial Advisors ("GFA")

We want to reassure you that your investment portfolio accounts held at Pershing and managed by GFA are safe. The process we use to transfer money, invest and trade in client accounts includes several safeguards to prevent fraudulent activity. We require a significant amount of identification and documentation in order to link new Automatic Clearing House ("ACH") or electronic funds transfer ("EFT") transactions to bank accounts, including a "wet" signature on the establishing documents. We have secure servers in our office maintained by a very experienced service company of more than fifteen Information Technology ("IT") professionals. We have an encrypted backup system to secure client data. We also use an encrypted email system to communicate anything that includes sensitive data. We do this to prevent any potential inadvertent loss of data. By data, we include any private, non-public information about a client that could be used inappropriately. (Our almost twenty-year relationship with Advantage Microsystems, our IT service company we employ on a monthly retainer, has allowed us to avoid any turbulence with our technology system. We have been fortunate never to have experienced a "crash" nor have we ever had any breach of our data systems.)

▲ How are your account assets protected?

Your accounts at Pershing are insured by the Securities Investor Protection Corporation ("SIPC"). The SIPC protects against the loss of cash and securities (such as stocks and bonds) held by a client due to theft or malfeasance at a brokerage firm where assets are missing from customer accounts. The limit of SIPC protection is $500,000, which includes a limit of $250,000 for cash.

In addition to SIPC protection, Pershing provides coverage in excess of SIPC limits. The excess of SIPC coverage is re-evaluated annually, for Pershing LLC accounts. The additional protection for our clients where Pershing LLC is the custodian include:

- An aggregate loss limit of $1 Billion for eligible securities over all client accounts
- A per-client loss limit of $1.9 million for cash awaiting reinvestment-within the aggregate loss limit of $1 billion

An excess of SIPC claim would only arise if Pershing failed financially and client assets for covered accounts, as defined by SIPC, cannot be located due to theft, misplacement, destruction, burglary, robbery, embezzlement, abstraction, failure to obtain or maintain possession or control of client securities, or to maintain the special reserve bank account required by applicable rules.

It is important to recognize that SIPC and the excess of SIPC coverage do not protect against the decline in value of your securities due to market fluctuation.

▲ How you can protect yourself?

While GFA has safeguards in place to protect your privacy and your personal information that we have on our system, you could still be exposed to risk in many other ways. Here are some tips to minimize your exposure:

- Do not click on a link in an email until you validate the source. If you think an email could be suspicious, look very closely at the sender's actual email address. Frequently you will see it is NOT from the sender referred to in the subject line, or the company that is purportedly sending you the message.

- Make sure the information in your social media accounts are only visible to friends and family (and do not accept friend requests from people you do not know). Your social media accounts are a smorgasbord of personal information ready to be deciphered by the right cybercriminal. One reason Larry does not post on social media is because he does not want to become a more vulnerable target. He recommends that you not post on social media that you will be going on vacation for a specific time or posting photos while you are on vacation. This creates a golden opportunity for thieves who might learn you will not be home, so they perceive an easier target should they come to "visit" while you are away.

- Consider the use of a password manager tool to help you organize and maintain your passwords. Password managers generate, store, and recall complicated passwords for the websites you use. They help you use unique, secure passwords to protect your information and do all of the leg work for you.

- Use different passwords for different accounts. A data breach from one account could lead to a greater loss if that same username and password worked for multiple logins (usernames are typically an email address and by default are the same). If it is too difficult to manage a different username and password for every account, a suggestion would be to separate your accounts into groups (for example one for emails, one for bank accounts, etc.). This way, if there is a data breach you can change all the passwords related to that group.

- Use a "strong" password for your accounts. This involves upper and lower-case letters, numbers and symbols. The number one ranked password most used by consumers is "password". If there are numerical requirements, the top password used is "password123". Do not become a victim by making it easy for the criminals.

- Do not save passwords or other sensitive information on your phones. Hackers can gain access to your phone notes, even if you have a locked device. Information in address books are also stored in plain text, meaning that they do not have any protections from capable hackers.

These are just a few tips on how you can better protect yourself from becoming a victim of cybercrime. If you have any questions regarding cyber security or would like additional tips on how to protect yourselves, please let us know. We are here to assist you. We hope this information is helpful to you. As we often like to communicate, we are in the "anxiety reduction business." Keeping your data and your financial assets safe will certainly reduce your potential anxiety.

This information was compiled by Ginsburg Financial Advisors, Inc.