SARD
WEALTH MANAGEMENT GROUP, LLC

CLIENT NEWSLETTER **BY: JONATHAN SARD, CFP®**
4th QUARTER - 2017

IMPORTANT INFORMATION

President Trump has proposed his blueprint for tax reform. Because the proposed changes are just proposals and will probably not all come to fruition, we will just list a few of the highlights. They will consider reducing the number of income tax brackets, while also reducing the actual tax rates. They will also consider eliminating some tax deductions, while doubling the standard deduction, but eliminating the personal exemption deduction. The estate tax is also on the chopping block. We will keep you updated if something ends up passing!

We hope to have the 2018 retirement plan contribution limits by the end of October and we will publish those numbers in our next newsletter.

Lastly, at the end of our newsletter is this year's Privacy Policy statement. Please let us know if you have any questions.

Avoiding the Cyber crooks

How can you protect yourself against ransomware, phishing, and other tactics?

Imagine finding out that your computer has been hacked. The hackers leave you a message: if you want your data back, you must pay $300 in bitcoin. This was what happened to hundreds of thousands of PC users in May 2017 when they were attacked by the WannaCry malware, which exploited security flaws in Windows.

How can you plan to avoid cyberattacks and other attempts to take your money over the Internet? Be wary, and if attacked, respond quickly.

Phishing. This is when a cybercriminal throws you a hook, line, and sinker in the form of a fake, but convincing, email from a bank, law enforcement agency, or corporation, complete with accurate logos and graphics. The goal is to get you to disclose your personal information – the crooks will either use it or sell it. The best way to avoid phishing emails: stick to a virtual private network (VPN) or extremely reliable Wi-Fi networks when you are online.[1]

Ransomware. In this scam, online thieves create a mock virus, with an announcement that freezes your monitor. Their message: your files have been kidnapped, and you will need a decryption key to get them back, which you will pay handsomely to receive. In 2016, the FBI fielded 2,673 ransomware attack complaints, by companies and individuals who lost a total of $2.4 million. How can you avoid joining their ranks? Keep your security software and operating system up to date. Your anti-virus programs should have the latest set of virus definitions. Your Internet browser and its plug-ins should also be up to date.[2]

Advance fee scams. A crook contacts you via text message or email, posing as a charity, a handyman, an adult education provider, or even a tax preparer ready to serve you. Oh, wait – before any service can be provided, you need to pay an "authorization fee" or an "application fee." The crook takes the money and disappears. Common sense is your friend here; avoid succumbing to something that seems too good to be true.

I.R.S. impersonations. Cyber gangs send out emails to households and small businesses with a warning: you owe money. That money must be paid now to the Internal Revenue Service through a pre-paid debit card or a money transfer. These scams often prey on immigrants, some of whom may not have a great understanding of U.S. tax law or the way the I.R.S. does business. The I.R.S. never emails a taxpayer out of the blue demanding payment; if unpaid taxes are a problem, the agency first sends a bill and an explanation of why the taxes need to be collected. It does not bully businesses or taxpayers with extortionist emails.[1]

Three statistics might convince you to obtain cyber insurance for your business. One, roughly two-thirds of all cyberattacks target small and medium-sized companies. About 4,000 of these attacks occur per day, according to IBM. Two, the average cost of a cyberattack for a small business is around $690,000. This factoid comes from the Ponemon Institute, a research firm that conducted IBM's 2017 Cost of Data Breach Study. That $690,000 encompasses not only lost business, but litigation, ransoms, and the money and time spent restoring data. Three, about 60% of small companies hit by an effective cyberattack are forced out of business within six months, notes the U.S. National Cyber Security Alliance.[3]

Most online money threats can be avoided with good security software, the latest operating system, and some healthy skepticism. Here is where a little suspicion may save you a lot of financial pain. If you do end up suffering that pain, the right insurance coverage may help to lessen it.

Given all of the uncertainty in the world today, we always preach how important it is to plan. Be sure you are sitting down with us on a regular basis to discuss your entire financial situation. Each quarter we want to remind you to alert us to changes in your financial situation or investment objectives to ensure that we are aware of any situation that might require changes in the management of your accounts. Please remember to contact us to discuss how these changes impact your investment accounts!

Citations.
1 - gobankingrates.com/personal-finance/avoid-12-scary-money-scams/ [8/28/17]
2 - eweek.com/security/the-true-cost-of-ransomware-is-much-more-than-just-the-ransom [8/18/17]
3 - sfchronicle.com/business/article/Interest-in-cyberinsurance-grows-as-cybercrime-12043082.php [8/28/17]

Financial Tip of the Month

Combat identity theft with a credit freeze

A credit freeze (also known as a security freeze) can be a great weapon against identity theft. It lets you restrict access to your credit report, tripping up con artists who try to open accounts in your name. Lenders won't extend credit if they can't check someone's payment history.

If you suspect a crook is attempting to gain unauthorized access to your credit report, a credit freeze is a good first step.

How does a credit freeze work?

Contact each of the nationwide credit reporting agencies. You'll need to provide information in writing, including your:

- Name
- Address
- Date of birth
- Social Security number
- And other identifying information

Expect to pay a fee to each reporting agency typically ranging from $5 to $10, unless you're over age 65 or can prove via a police report that you're a victim of identity theft. Also, be aware that freezing your credit report will not automatically freeze your spouse's report. You'll have to do this for each of the three credit reporting agencies: Equifax, Experian and TransUnion. One credit agency is not obligated to inform the other two about the request.

Placing a freeze on your credit report doesn't affect your credit score or prevent you from ordering copies of your report. A credit freeze will typically last until you remove it, either permanently or temporarily with a designated PIN or password.

Credit freezes are not foolproof

Government agencies, such as taxing authorities, still have access to your credit report. It also may be released in response to court orders, subpoenas or search warrants. And collection services and current creditors will still be able to get the information they need to contact people. In other words, a credit freeze won't shut out legitimate debt collectors.

If you're planning to apply for a job, take out a mortgage, switch utility providers or shop for insurance, find out which credit reporting agency each business typically uses. That way you can remove the specific credit freeze needed while still road blocking other credit reporting avenues from identity thieves.

Please keep in mind that this tip is designed to be of help for you, but is not to be relied upon as advice. It is merely a reminder that there are many choices you have available to you, and that planning may be the only way to find the right answers for your situation. As with any financial issues, make sure you get the right information before making a decision. If you have any questions, we'll be glad to help you!

Client Quiz

Question: You must be at least how old to take advantage of retirement plan catch-up contributions?

A. 40
B. 50
C. 55
D. 59 1/2

We wanted to thank those of you who have participated in our Client Introduction program. As you know, marketing for new clients takes a great deal of money, time, and energy and we would much rather spend our resources improving your financial health. We, like most businesses are looking to grow; however, for the benefit of our existing clients we are only able to take on a limited number of new clients each year. Over the years, we have learned that encouraging you to introduce us to people you know works well for all of us…we help you, and you help us. If you aren't familiar with our friends helping friends program, please call our office

or be sure to ask us at your next meeting. The few minutes it takes to learn about how it works will be well worth your time and energy!

Answer: B. You must be at least 50 years old in the year in which you take advantage of the catch-up contribution. If you turn 50 on December 31st, you can still take advantage of the catch-up contribution that year.

If you would like some of your friends, coworkers, relatives, business acquaintances, etc. to receive a FREE subscription to this newsletter, please call our office and we'll add them to the mailing list. We'll also send them a note with their first issue telling them that you had suggested they receive the newsletter, and to contact us if they would like to stop at any time. If you enjoy this newsletter, why not share it for FREE with people you know, with no hassle for you?

Sard Wealth Management Group, LLC
Privacy Policy

Your privacy is important to Sard Wealth Management Group, LLC. We understand that the information you provide to us is private. This policy outlines what information we collect, how we use it and how we protect it. We will affirm our Privacy Policy annually in writing with all current Clients.

We collect information about you to provide services and products to help you meet your financial goals and objectives and to allow us to provide high levels of customer service to you. We also gather information in order to help us fulfill our legal and regulatory requirements. Information collected may vary depending on the products and services requested and the scope of your relationship with us.

Information Collected about You: We collect nonpublic personal information about you through account and insurance applications, our financial planning questionnaire, and through our day-to-day meetings, interactions, and the services we provide. The following types of information are maintained:

- Personal Information: name, address, phone number, tax identification number, date of birth, employment, children, wedding anniversary, and hobbies/interests
- Financial Information: income, investment and bank accounts, insurance policies, investment experience, and net worth
- Health Information: personal and family medical history, diagnoses and prescriptions
- Service-oriented information: account balances, payment history, account numbers, and account activity

Disclosure of Personal Information: We train our staff to take caution in handling personal information and keeping it secure. It is our policy not to share any private information with any businesses for marketing purposes. We do not disclose any private information with any outside firm with the exception of those that require specific information in order for a specific account to be established or to execute a specific transaction. The following information is shared by us:

- Personal and financial information: shared with a brokerage firm or investment company to setup and manage investment accounts for you and with insurance companies to initiate an insurance policy on your behalf.
- Health-related information: shared with insurance companies to initiate life, health, disability, or long-term care insurance on your behalf
- All types of information: shared with your accountant or lawyer to allow us to collaborate for your benefit. We may be required by law or regulation to disclose information to third parties such as in response to a subpoena, to prevent fraud, to comply with rules and regulations to which we are subject, in response to inquiries from industry regulators, and in order to comply with our broker/dealer's policies with whom our associated persons may be registered.

From time to time, we may provide via mail, email, or in person, investment reports of all household accounts to members of the same household. Household accounts include those held by spouses (or domestic partners) of the same family, and minor children for which one parent is the custodian and/or owner of the child's account. We may answer general account questions relating to accounts of a member of the household for either spouse.

If you close your account or discontinue your relationship with us, we will continue to treat your information with the same attention to privacy as for active Clients. Former Clients may request a current copy of our privacy policy at any time by calling our office at (404) 843-4483.

If you do NOT wish to have household account reports shared or object to our disclosing your private information as outlined in this policy, please provide us with a written statement clarifying your wishes.