WINTER 2018

The FREE STATE Accountant

A Publication of the Maryland Society of Accounting & Tax Professionals

6
How to Protect Your Loved Ones From Elder Financial Abuse

5

7

TABLE OF CONTENTS

CONTRIBUTORS

Glen Frost is managing partner of Frost & Associates, LLC, which is located in the Washington, DC metropolitan area and currently employs 10 attorneys. The firm focuses on Tax Controversy and Litigation, International Tax Matters, Tax Planning, Estate Planning, White-Collar Criminal Defense, and regulatory investigations by various government agencies including the Office of Foreign Asset Control (OFAC). Mr. Frost manages a team of Attorneys, Certified Public Accountants, Enrolled Agents, Former IRS Employees, Certified Fraud Examiners, and other professionals.

Al Giovetti is a CPA in Maryland with over 35 years of public accounting experience, Accreditation in Business Accounting (ABA, 1989), Tax Advisor (ATA, 1984), Retirement Advisor (ARA, 2007), and Principal, Giovetti and Giovetti Certified Public Accountants (1992 – current). Giovetti and Giovetti Certified Public Accountants is a full-service small CPA firm in Catonsville, Maryland. Al is currently serving as Immediate Past President on the Board of Governors for the National Society of Accountants (NSA).

Bob Jennings is a nationally renowned author and speaker, presenting continuing education classes to over 100,000 tax professionals over the last 20 years all over the world. Bob is a licensed CPA (Indiana), a licensed CFP, an IRS Enrolled Agent and a Registered Tax Return Preparer. Bob is also a prolific author and has published over 60 professional articles in such magazines as the Journal of Accountancy as well as many other professional and consumer publications; annually authors several tax, accounting and technology manuals; and is a regular columnist for FoxBusiness.com. As the founder of his own regional CPA firm in 1984, Bob has dealt exclusively with individual and small business financial issues for over 30 years. Bob appears regularly in the media and has been quoted extensively by numerous publications. He has recorded an extensive number of informational videos, DVD's and instructional clips available on his website at TaxSpeaker.com.

Dave Kile is co-founder of Ease Technologies and a former Apple employee with over 25 years' experience in the IT industry. He provides an invaluable expertise working with clients in all aspects of IT support. Mr. Kile has lead teams implementing projects ranging from healthcare patient portals, the creation of public safety IT help desks to the relocation of financial trading firms. Additionally, he is actively involved in providing education seminars, webinars and blogs sharing ways that businesses can improve security and productivity.

Jerry Lotz is a Senior Savings Advisor at CostSeg Energy Solutions. CostSeg Energy Solutions represents companies whose mission is to help commercial property owners and leaseholders save money. He serves as an agent for Cost Segregation Services Inc. (CSSI), based in Baton Rouge, LA. CSSI is an "independent" company that provides "engineering-based" IRS Approved, Cost Segregation Studies and Tangible Property Regulation Consultation. Other CSSI services include: CAP-EX Reversal Analysis, Engineering-Grade Energy Audits, 179D, 45L and LED Lighting Tax Savings Implementations. Jerry is a Baltimore native and holds a business degree from Towson University. He spent 30 years in various managerial positions in the medical sales industry. Jerry enjoys working to provide "exemplary" service to tax professionals and the clients they serve. When he is not working, he enjoys spending time with his wife, children and grandchildren.

Darla McClure - When clients hire Darla McClure, of Stein Sperling, they work with a partner who understands their needs, approaches matters from their point of view and designs practical legal solutions to meet their business objectives. Darla's focus on serving her clients' best interests and getting matters done successfully is underscored by her commitment to providing responsive answers, keeping clients informed and delivering the highest levels of service. Darla regularly counsels business clients on employment matters and resolution of employment disputes. Working closely with management, she helps ensure compliance with state and local laws, and assists in drafting employment policies, benefits and contracts, such as restrictive covenants and confidentiality agreements. Darla's extensive experience also includes organization and entity selection, structuring business ventures, developing shareholder and operating agreements, resolution of business disputes, commercial transactions, mergers and acquisitions, and joint ventures. In addition to her employment and business law practice, Darla is the Managing Principal of Stein Sperling's Frederick, Maryland office. A frequent speaker on topics involving business organization, disputes and employment matters, Darla has addressed various organizations throughout the region, including the Montgomery County Medical Society, where she sits on its Advisory Board. She also serves as the Legislative Affairs Director of the Montgomery County Chapter of the Society for Human Resource Management (MC SHRM), where she contributes to the organization's monthly newsletter and gives presentations on employment law topics. Darla has also spoken to groups of financial professionals, including the Maryland Society of Accounting and Tax Professionals and various chapters of the Maryland Association of Certified Public Accountants.

Marin Perez is the Content Marketing Manager at MileIQ. He has been writing about how technology improves lives for about a decade. He's excited to see how entrepreneurs are using tools like MileIQ to be more successful. When not working, he's thinking about his next trip.

Jim Seminara is an investment advisor and financial planner with Mass Mutual Financial Group of the Mid Atlantic, a MassMutual Agency; courtesy of Massachusetts Mutual Life Insurance Company.

Ellen Silverstein, **CPA** lives in Montgomery County MD, starting in Rockville, moving to Olney/ Brookeville, and settling in Clarksburg. She graduated from the University of Maryland in 1981 and worked for a local Bethesda, Maryland CPA firm for two years, after which followed a two year stint in the private sector. She went back into public accounting and established her own firm in 1991. Concentrating on small businesses and their owners, her business has successfully grown and provides services to a varied client base, covering a wide area of central Maryland with many out of state as well. She has been a member of MSATP since 1993, serving on various committees during this time. Ellen is currently serving as First Vice President on the MSATP Board of Directors and is the Chairperson of the Finance Committee.

Joe Tabeling is a Sales Manager at CQI Associates with over thirty years experience in sales, sales training, motivational speaking, trade show management & design, advertising & marketing, product sourcing, business consulting, basic web page design and licensing negotiations.

MSATP
Est. 1959 Maryland Society of Accounting & Tax Professionals

Maryland Society of Accounting & Tax Professionals, Inc.

10630 Little Patuxent Pkwy, Ste 146
Columbia, MD 21044
(410) 876-5998 | (800) 922-9672
Fax: (443) 881-4146
www.msatp.org | info@msatp.org

MSATP News

CPR Committee Report

HSA Update

As a brief history, the Contraceptive Equity Act was enacted in 2016. Effective January 1, 2018, the Act mandates that male contraceptive services (vasectomies) must be covered as a preventive service, i.e., without any deductible or cost-sharing required. The problem is in its application to a high deductible health plan, a creature of federal law coupled with a health savings account. By requiring that this service be provided without a deductible, is a health savings account associated with a health plan still valid? This question has been raised with the IRS by the Maryland Insurance Commissioner. To date, there has been no response from the IRS.

This is a high stakes issue. The health insurance market, both individual and employer sponsored, has been moving rapidly in the direction of HDHPs in recent years. The obvious reason is that more cost-sharing with a covered individual allows the insurer to charge a lower premium. Enter the Health Savings Account – an essential tool that allows individuals to accumulate, on a tax-free basis, sufficient funds to pay medical expenses that would not be paid by the insurer under an HDHP. Such expenses can easily amount to thousands of dollars per year. An HSA is a critically important tool for personal financial planning. Losing the tax deduction for an HSA would severely disrupt that individual's ability to meet their financial obligations. The mandate under Maryland law threatens the tax deductibility of all HSAs associated with Maryland HDHPs.

MSATP and other financial professionals are unanimous in sounding the alarm about the validity of HSAs in Maryland. They cannot, in good conscience, advise their clients to make contributions to HSAs without knowing the enforcement policy of the IRS on this important issue. Unless or until the IRS responds to the Maryland Insurance Administration, the risk will remain.

MSATP has reached out to Senator Thomas "Mac" Middleton, Finance Committee Chair, who will be hearing the bill on the issue. The bill, we believe, will be sponsored by Senator Ed Reilly. Senator Reilly sponsored a bill in 2017 but it died in committee. MSATP is part of a coalition of organizations who is seeking a bill to modify the language while preserving the tax-deductible treatment of the HSA.

With the legislative session beginning on Wednesday, January 10, 2018, the hearing to address the issue will not be until mid-January. MSATP CPR Committee members continue to work and discuss the issue with members of the General Assembly when they attend various legislative events.•

CLICK HERE TO ACCESS IMPORTANT CONTACT INFORMATION for COMPTROLLER OF MARYLAND REVENUE ADMINISTRATION DIVISION

2017-2018 MSATP Board of Directors

William M. Feehley, CPA
President

Ellen Silverstein, CPA
First Vice President

Richard Gottfried, CPA
Second Vice President

Dave Churchman, EA
Secretary

Barbara J. Smith, CPA
Treasurer

Thomas Bray, EA
Delegate

C. Emily McComsey, EA
Delegate

Donya Oneto, CPA
Delegate

Dan Shaughnessy, EA
Delegate

Betty Kohls Stehman, CPA
Delegate

Ron Grafman, EA
Board of Trustees Delegate

Robert Medbery, CPA
Immediate Past President

Alverta "Sandy" Steinwedel
Executive Director

How to Prep Your Clients for the New Mileage Rates

by Marin Perez

While the new tax laws are expected to change things for a lot of clients, one aspect remains clear: if your self-employed clients drive for work, their miles are worth a lot at tax time.

The 2018 Mileage Rates

The 2018 standard mileage rates are:

- 54.5 cents per business mile, up 1 cent from 2017
- 18 cents per mile for medical or moving reasons, up 1 cent from 2017
- 14 cents per charity drive.

Because the business mileage rate is the highest it has been since 2015, that could lead to some major tax savings for your clients who drive a lot.

How to Get Clients to Actually Keep A Mileage Log

I'm sure you get accurate mileage logs from your clients that are recorded contemporaneously and land on your desk in a legible format? For the few of you who nodded "yes," congratulations. The rest of us know how difficult this can be.

Logging your miles is worth it but it may not seem like it for many people. Having to write down every single drive may not seem hard but it can be. Just think about if you're running late for a meeting or even if there's a great song playing as you get to your destination—the last thing you're thinking about is writing down your mileage.

That's why we're seeing increased popularity of mileage tracking apps. This uses something almost everybody has when they're driving (smartphones) to handle a tedious, yet important, chore.

But not all mileage tracking apps are created equal. Try them out for yourself before making recommendations. In particular, look for apps that automatically track mileage in the background. If an app requires people to start and stop tracking with each drive, it's going to suffer the same problems as a manual mileage log.

The best thing about a mileage tracking app with automatic tracking is that your client can do their job as they normally would and they get a contemporaneous mileage log created for them. Of course, they still have to go in and add things like the business purpose but apps make this so much easier.

Best of all, a mileage tracking app provides digital mileage logs for you that are accurate and can hold up to IRS scrutiny. You'll also appreciate how your clients can just email you a spreadsheet with all their tax-related mileage for the year.

The Actual Expense Method?

The new tax laws may offer some advantages for clients who want to buy a new vehicle for the expanded bonus depreciation. With that said, it likely makes sense for the majority of self-employed and small business owners to utilize the standard mileage rate. Using mileage tracking apps makes this drop-dead simple for them and for tax professionals.

MileIQ for Tax Professionals

As a tax professional, I'd like to invite you to become a part of the MileIQ for Tax Professionals program for free. MileIQ is the leading app for automatic mileage tracking! MileIQ is an accurate mileage tracking app that automatically logs your miles, so you can easily classify business miles to maximize your tax deductions. With MileIQ for Tax Professionals, you get access to a FREE premium account to use MileIQ so you can confidently recommend it to your clients who take the mileage deduction at a discount.

Being a part of the program, you'll receive:

- Free MileIQ Premium Subscription (a $59.99 value)
- Special 20% discount code for your clients
- Access to valuable resources and tax tips for your clients

Automatic logging means an accurate, contemporaneous record of all your business miles, no filling in the blanks later, no mixing business and personal drives. At tax time your clients can generate mileage reports full of IRS mileage standards.

Join the growing numbers of tax professionals who use and recommend MileIQ to their clients. Apply at mileiq.com/taxpros for your free account and never deal with the mileage headache again.•

Having the Energy to Stick to Your New Year's Resolutions

by Joe Tabeling

The New Year is traditionally the time to set and reach your goals. Here are a few energy tips from CQI to help you get there.

Thermostat - Set your thermostat to 68°F while you are awake and lower while you are asleep or away from home. The lower the interior temperature, the slower the heat loss. So, the longer your house remains at the lower temperature, the more energy you save.

Power strips – Don't let your peripheral, energy-sucking devices like televisions, computers, lamps, toasters, and cell phone chargers use energy while they are off. Utilize a power strip and control your usage with one switch. Over time, the savings will add up.

For other energy savings tips go to www.cqienergy.com.•

5 Steps to Prepare for Winter Storms

by Dave Kile

We often don't get a lot of notice with arrival of winter storms. These events can leave us cut-off from the office or from our employees. Many organizations can successfully operate and be productive in any situation. Is your office prepared? Follow these steps to weather the winter storms.

1. Keep an Off-Site List of Contacts

You probably have thousands of customers and vendors. Keeping an off-site contact list will allow you to stay in touch with them and keep your business running during periods of downtime. This list should contain vendors you need to contact every week, and any customers with current, unresolved issues. A printed paper version can be important and don't forget to keep a list of employee phone numbers too.

2. Back Up Critical Data Off-Site or in the Cloud

You have only a day or two to prepare after forecasters tell you a storm has a high chance of hitting your area. Power failures, melting floods, and even looting are all risks to your infrastructure and data that come with a severe storm.

A thorough disaster recovery plan will already accommodate the offsite storage of critical data. If you don't have such a plan, you'll want to back up critical data to an off-site location as soon as possible. This will give the data time to fully transfer before the storm hits.

One of the best options is to store your backups in the cloud. Data saved in the cloud is also readily available and redundantly stored.

3. Keeping the team productive

Most of our accounts already hold Office 365 subscriptions, and this is one of the easiest ways to keep the team productive in an emergency. Rarely used, but Office 365 provides a browser-based version of Office for subscribers. A great tip for subscribers is to test and use this if they must suddenly have to work from home for several days. This version provides email, Word, Excel, PowerPoint, OneDrive and other horizontal applications most organizations use every day. Most importantly, this device is independent and secure. So, an employee could log in from home and get to these applications from any computer.

4. Have a Communication Plan

Work with your employees to create primary and secondary methods of communication during the storm. You might want to forward your phone numbers or extensions to cell phones. Many newer VoiP phones systems provide a lot of options, including just carrying your office phone home and plugging it into your home Internet connection.

Email and even texting should be part of the triage plan. You not only want to have plans that include employees, but also, what is your message to your customers? Some companies have used social media such as Facebook and Twitter as methods to stay in touch as well. Consider changing your voicemail greeting to set expectations with your clients if an emergency hits.

5. Practice Your Plan

Test restoring your data to your servers. Ensure your local and remote backups can be used to restore operations if you suffer extended downtime. Stepping through your recovery plan makes everyone familiar with what needs to be done to get your company back up and running in the least time possible. Review and share the communication plan with your employees.

Need help with your own disaster recovery plan? Automated backups are your best defense against massive data loss. These systems mean one less headache when worrying about your business during a winter storm. Contact us quickly, and we'll help you set up a complete data backup procedure to ensure you don't lose data if a catastrophic event occurs. Contact Ease Technologies today at 301-854-0010 and learn how our Ease Cloud Workspace can help keep your business secure in the Baltimore-Washington Region.•

How to Protect Your Loved Ones From Elder Financial Abuse

by Jim Seminara

Could someone you love be a victim of elder financial abuse?

Each year, seniors lose over $36 billion to elder financial abuse and more than a third of seniors are affected by financial abuse in any five year period, according to one recent study[1]. This total includes criminal fraud, caregiver abuse, and financial exploitation, where seniors are subjected to high-pressure sales tactics and misleading marketing.

Lawmakers are paying attention. Federal and state governments have begun to pass laws to protect seniors from financial abuse. This is good news. However, these laws often protect a senior only after someone realizes that an elderly person is being exploited. An elderly person can lose a significant amount of their savings before someone close to the senior realizes what has happened.

Red Flags

In order to stop elder financial abuse, is critical that those closest to seniors be on the lookout for possible red flags. As a family member or close friend of an elderly person, you may be in the best position to detect early signs of elderly financial abuse.

Would you know the signs of elder financial abuse and exploitation? Here are some:

- The elderly person becomes dazed, nervous or fearful when discussing financial matters.
- He or she does not remember having requested certain transactions.
- The elderly person provides contradictory or questionable explanations for financial transactions.
- You observe a significant change in the senior's financial habits (such as more frequent or larger withdrawals)
- There is the appearance of a new "friend" who is insistently requesting information about the elderly person's accounts, or who tries to make changes without the senior's permission. This new "friend" could be an acquaintance, a family member, a health care provider, or even someone the elderly person met online.
- The new "friend" or family member refuses to let you speak to the elderly person, or insists on being present when you talk with the elderly individual.
- You may see questionable signatures on documents, or it may appear that numbers on financial documents have been forged or changed.
- You may learn of sudden or unexplained changes in beneficiaries on life insurance policies, or see that there have been unexplained changes of address on an elderly person's financial statements.

What to Do?

If you see any of these signs, it is critical to act quickly. There are a number of steps that you can take:

- Contact the bank or financial professional who manages the elderly person's accounts. The bank or financial professional can freeze accounts or take other action. (MassMutual has resources to help its clients with these situations. You can email ElderAbuse@massmutual.com with questions).
- Contact the Adult Protective Services agency in your state. Like Child Protective Services agencies, Adult Protective Services agencies are created to protect elderly and vulnerable adults.
- Contact your local police department if you believe that the elderly person has been a victim of fraud.
- Finally, if the elderly person has another trusted contact such as an attorney or accountant, he or she may be able to help.

Seniors lose approximately $17 billion annually to elder financial exploitation alone. Criminal fraud accounts for $13 billion and caregiver abuse is estimated at $7 billion[1]. Keeping an eye out for red flags of elder abuse can help protect the ones you love.•

[1]The True Link Report on Elder Financial Abuse 2015

As You Meet With Clients: Tax Reform and Conversation Topics

by Jerry Lotz

I've had the pleasure of meeting with a number of tax professionals this year. As I write this article in December 2017, I hear the growing angst around possible changes to the tax filing laws. Filing taxes as we know it will likely undergo some changes for the 2018 filing season.

The meetings that tax professionals and their clients schedule, beginning early January 2018, will probably consume a little more time than in years past. Whether or not there are major future changes to the 2018 tax code, preparers should be on the lookout for their clients who have residential rental, multi-family and/or commercial property, as there may be substantial tax savings opportunities for the 2017 tax year.

When you have those initial client meetings in January, be sure to include a conversation around the following topics:

1. Does the client own buildings, or did he/she buy or build a building ($250K or more) in 2017? There might be tax savings that a Cost Segregation Study will define.

2. Did the client buy or build a building after the September 27, 2017 tax reform deadline? One hundred percent (100%) bonus depreciation is eligible on all items with a 20 year tax life or less. A Cost Seg Study helps to maximize those tax savings.

3. Did the client make substantial leasehold improvements?

4. Did the client remove and dispose of portions of a building and complete further renovations?

- A Partial Asset Disposition (PAD), as outlined in the Repair Regulations, allows for the write down of the basis of what the owner removed and the costs for the removal and disposal of those items. Owners receive a tax deduction in the current year, but it is a "use it or lose it" opportunity. If you do not capture it in the current tax year, your client may lose the write down.

- In order to properly substantiate and claim dispositions, a cost segregation firm should be engaged to calculate the remaining depreciable basis of the removed/disposed assets through an engineering-based study. The contractor also needs to separate the work efforts into appropriate distinct categories:

A. Identify cost to remove/dispose old building components (labor, hauling, disposal etc…)

B. Identify cost of the labor to install new building components

C. Identify cost of new building components

- The cost to remove and discard building components can be expensed and has no bearing on the calculation of basis value of the asset that is disposed.

5. Have I put written Capitalization Policies in place for the client?

6. Do I have valuations in place for every building Unit of Property (UOP) and building system on my client's property?

7. Do I have the framework in place for making future Capitalization vs Expense decisions?

8. Do I have an opportunity to engage a cost segregation professional to scrub my client's depreciation schedule and perform Capitalization to Expense Reversals (CAP – EX REVERSALS)?

Opening up the conversation by proactively asking a few questions about the client's current 2017 situation will help calm the air in the midst of whatever the 2018 tax code holds!•

Medical Marijuana and the Workplace

by Darla McClure

With Medical Marijuana now legal in Maryland, employers question how to handle an employee who tests positive for marijuana. While many employers currently have policies in place that prohibit the use of marijuana, what does this mean if an employee is legally authorized to use marijuana for medical purposes. Unfortunately, this is only made more confusing because the use of marijuana is still illegal under federal law pursuant to the Controlled Substances Act.

Regardless of the new medical marijuana law, in Maryland, employers remain allowed to maintain a drug-free workplace and therefore are still permitted to: (1) refuse to hire someone who fails a drug test due to the presence of marijuana in their system, and (2) terminate an employee who fails a drug test due administered pursuant to company policy.

Notwithstanding, employers are getting requests to allow medical marijuana use as a reasonable accommodation under the Americans with Disabilities Act and state and local disability laws. The types of diseases and conditions that medical marijuana can treat are some of the same diseases and conditions that fall under the definition of a disability. There are some states that have addressed this disability discrimination issue explicitly by enacting statutory provisions prohibiting an employer from discriminating against an applicant or employee for using medical marijuana lawfully. Maryland however is not one of them. And so far, the courts in Maryland have also been reluctant to extend the disability protection to medical marijuana users.

With the ever-changing landscape surrounding the use of medical marijuana and marijuana use in general, it is best to contact your employment counsel to help navigate through these issues.•

Phone and Network Security

by Bob Jennings

In tax offices across the country right now there are thousands of often overlooked security holes just sitting there waiting to be taken advantage of. These small devices can compromise your business and your clients if not handled properly. I am talking about smartphones, no matter if you use iPhone or Android, your device could be the metaphorical hole in the wall of your office security.

So how exactly can these innocuous devices cause so many issues? There are multiple ways these devices could be used to compromise your business security. Let's start with the least likely and work our way up to most dangerous.

The first thing that is a possibility is a nefarious person outside your office to get onto your WiFi and network. Many android phones are able to use a simple app to try and crack the password on your WiFi if it is not secure enough. We recommend making sure your WiFi is using WPA2 encryption as this is the most secure encryption you can turn on currently. The 2nd recommendation is to turn off your WiFi access point at night, or set time rules on your device to deactivate during closed hours.

Now we come a bit more into the realm of possibility. A client comes in for a meeting, perhaps bringing their child with them. Depending on the tech level of this person it is possible for them to either ask for access to play a game, or just try and crack your password themselves. While that in itself is not necessarily a major security risk, it opens the door for a potentially infected phone or computer to access and spread onto your network. Again, the best fixes for this situation are WPA2 encryption, and having a written policy about never giving out the WiFi password to clients. If they really need access to internet you might be able to setup a guest WiFi network separate from your own, but most would just be forced to rely on their own cellphone connection.

Now we are getting into the directly dangerous items. Let's say your employee is running late for an appointment and accidentally drops their phone in the lobby. Anyone who picks up this phone could theoretically access the info on it. Say that employees phone has an email list or app that they use to communicate with your client list, which by the way that stranger now has access to. Perhaps they also use that employees phone to find a list of saved WiFi passwords, or office passwords they saved in a Notes app on their phone. All the info you or your employees have on your phone that is insecure is now available to the stranger and potentially the world. The best ways to prevent this issue is to make sure any phone with confidential info, even office email access, are protected by a 8-digit alphanumeric password and by using the phones built in encryption to prevent people getting access. We also recommend setting up the phones anti-theft protection, programs such as Apples "Find my iPhone" and an Android app like "Prey" https://play.google.com/store/apps/details?id=com.prey&hl=en. These will let you track and remotely erase the phone if it gets stolen to prevent any data loss for your company.

And the most likely issue in our opinion is that you or your employees have a phone lost or stolen that has unencumbered access to your office systems. Apps like Dropbox and One-drive have the ability to turn on a passcode in the app to prevent anyone from getting into the files stored within without entering a separate passcode in the app. If you use something like Citrix receiver app for remote access you should have security already enabled, however it never hurts to double check any of your apps that might directly connect to your business such as file storage, web portal storage, or email apps that all have their own security turned on.

I wanted to get to Fijitsu Scanners (fujitsu.com), especially the iX500 workhorse and the new flatbed and feeder scanner (SP-1425). But we will have to leave these for future editions due to lack of space and endurance of readers. The mind can only absorb the information that the rear end can endure.•

MSATP Now Offers Online Education via Learning.net

24/7 learning that fits YOUR schedule! To access the courses: Learning.net

QuickBooks Custom Reporting (3 CPE)
Learn how to make the most out of QuickBooks' standard reports.

2017 Maryland Tax Law Update (5.5 CPE)
Learn from State of Maryland representatives as they present the latest changes in Maryland law and issues facing fax professionals. This course qualifies for the Maryland Tax topic for Maryland Registered Tax Preparers.

Qualified Terminable Interest Property (QTIP) Trust

by Glen Frost

A QTIP trust, despite its silly name, is a valuable estate planning tool. QTIP, or "Qualified Terminable Interest Property" is a name derived from the tax law that legalizes the tax benefits of the trust. When property is given to a spouse outright (not subject to a trust), it qualifies for what is known as a "marital deduction." In layman's terms, the property transfers to the spouse free of estate or gift tax. For various reasons, sometimes, it isn't ideal to give assets outright to a spouse. This can create complications in estate planning, because gifts in trust typically do not qualify for the marital deduction.

A QTIP trust is a special type of trust that can be used to transfer assets in trust to a spouse free of tax during life, or more commonly, at death. When a trust is drafted to meet the requirements delineated in the tax law, it qualifies as a QTIP trust and receives the same marital deduction treatment as if the property was given outright. This type of trust is very important when planning for blended families, or for creditor protection where families are facing estate tax. The special QTIP trust can save the day.

Legally, to qualify as a QTIP trust, the trust is required to pay all of its income to the spouse beneficiary, and there can't be any other beneficiaries during that spouse's lifetime. This allows couples to ensure that a spouse is taken care of financially. However, the manner and extent to which the underlying trust assets are distributed, and when, is customizable. The trust is often drafted to control how the trust's remaining assets are distributed once the beneficiary spouse dies. This is helpful when a couple wants to ensure that their other beneficiaries (usually children from this marriage or a prior marriage) will receive an inheritance on the death of the spouse. This control element also protects the trust assets from the claim of an elective marital share in the event of remarriage without a prenuptial agreement.

Likewise, a QTIP trust can be drafted as a spendthrift trust, such that the assets in the trust are protected from creditors of the beneficiary spouse (from accident victims, to credit card companies, to future divorce). This makes inter vivos QTIP trusts a valuable tool for making lifetime gifts of assets protected from creditors. Testamentary QTIP trusts (those taking effect at death) offer the same benefits for the beneficiary spouse.

As with other types of estate planning, QTIP trusts must be specifically tailored to each client's situation. If you have any questions about QTIP trusts or other estate planning techniques, please call us at 410-497-5947 or email Leanne.Broyles@frosttaxlaw.com.•

MSATP and Financial Literacy

by Ellen Silverstein

A committee of enthusiastic volunteers from our membership stepped up to meet with Dr. Allen Cox of MD Coalition for Financial Literacy (MCFL) and Mary Anne Hewitt, Executive Director of Maryland Council on Economic Education (MCEE). We were introduced to several current students of a local Howard County High School and their teacher, Dr. Maddy Halbach. These students use a program developed in conjunction with Dr. Halbach and MCFL/MCEE which has experienced tremendous success over the past several years. Each of the students was very well-spoken and shared their enthusiasm for the programs and how impactful this type of education has been for them as they have gone through high school.

Our members are being asked to meet with teachers in various jurisdictions to share their experiences, giving students an idea of what they can expect in the world of finances (be that accounting, or investment advisory, or taxes, and/or simply identifying terms that our profession utilizes every day) and practical experiences of how this information will be useful to them in their growth; from student to working adult. A recent visit by one of our volunteers who met with students, relaying experiences and providing some interesting information, answering questions, and then, developing a working relationship with the teacher. This type of promotion will give the teacher encouragement to rely on local resources outside the school system to supplement the curriculum.

MSATP is proud to be partnering with MCFL and MCEE to work on continuing to promote financial literacy in our young students; working with them to give them the tools and solid foundation moving forward.

DOES THIS SOUND like an interesting opportunity you'd love to be involved with? Please contact our office for information: info@msatp.org.•

Cybersecurity Review

by Al Giovetti

At the end of November, the IRS sponsored National Tax Awareness Week (NTAW--https://www.irs.gov/newsroom/national-tax-security-awareness-week-2017), from November 27, 2017 to December 1, 2017. There were events and press conferences throughout the United States announcing the efforts of multiple federal, state, and local agencies in combatting tax crimes. If you were not there, do not worry; more information can be obtained from www.irs.gov/securitysummit. (Whenever accessing a website, you are advised not to click on the link but to either type in the web address or cut and paste the web address into your browser.)

In Maryland, on November 28, 2017, there was a two-hour NTAW Forum. Every participant had a PowerPoint presentation on the risks, what to do, what not to do, and impressive statistical graphs marking the rise and fall of cybercrime as it relates to taxes. The participants of the Maryland event included:

Angie Barnett, President and CEO of the Better Business Bureau (BBB) of Greater Maryland,

William Feehley (info@msatp.org), CPA, President of the Maryland Society of Accounting and Tax Professionals,

Annette Y'Vonne Harris-Davis (annettte.y.harris@irs.gov), Stakeholder Liaison, Internal Revenue Service (IRS), Small Business/Self-Employed (SBSE), Communication & Stakeholder Outreach, Baltimore, MD,

Kathleen Henry (khenry@comp.state.md.us), Assistant Director, Revenue Administration Division, Fraud Detection/Identity Theft Section, Comptroller of Maryland,

Michael Lee, Special Agent, Criminal Investigation, IRS, Identity Theft Coordinator, Washington, DC,

Courtney A. McCalla (courtney.mccalla@sba.gov), Economic Development Specialist & Veterans Business Development Officer, Baltimore District Office, U. S. Small Business Administration (SBA),

Lisa Weintraub Schifferle, Attorney, Federal Trade Commission Division of Consumer & Business Education, and

Veronica Tubman (veronica.tubman@irs.gov), Senior Stakeholder Liaison, Practitioner Lead for South Carolina, Communications Liaison, SBSE, IRS.

For each of five days during the week (NTAW), a different cyber security topic was presented:

Monday: Online security; seven steps for safety (https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-1-online-security-seven-steps-for-safety)

Tuesday: Don't take the bait; avoid phishing emails by data thieves (https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-2-dont-take-the-bait-avoid-phishing-emails-by-data-thieves).

Wednesday: Victims of data breaches should consider these steps (https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-3-victims-of-data-breaches-should-consider-these-steps)

Thursday: Employers & payroll officials should avoid the W-2 email scam (https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-4-employers-payroll-officials-avoid-the-w-2-email-scam)

Friday: Small businesses should be alert to identity theft (https://www.irs.gov/newsroom/national-tax-security-awareness-week-no-5-small-businesses-be-alert-to-identity-theft)

The government representatives showed up with a confusing litany of suggestions and multiple publications that require intense study and research to partially understand.

Cyber-security (or cybersecurity or cyber security) is such a new field of study that the field term definition can be expressed in any of the three ways shown at the beginning of this sentence – no one has decided on the correct way to express the term. Should it be one word, two words or hyphenated? To keep it simple, for the remainder of this discussion, the term will be abbreviated "CS." CS changes daily as the field evolves. The listing "must have ten years' experience" in job application requirements is almost impossible to find. This is coupled with the fact that what you learned ten years ago would be useless today, since the field is changing so quickly.

Many CS experts cannot agree on what you should do to make sure you are safe. Much of CS advice is obsolete before the solution is even widely known. A college-level CS department professor recently challenged what has been accepted in the field as the way to craft a safer password. Everyone up until this professor's argument felt that you should not use words in the dictionary. However, this professor pointed out that the programs that crack passwords do not search combinations of dictionary words. So, what was until now considered safe may be wrong, because those giving the advice did not know how password hacking software worked.

Recently the online tax preparation company TaxSlayer was prosecuted by the Federal Trade Commission (FTC) for negligence involving a data breach (https://www.consumer.ftc.gov/blog/2017/08/taxslayer-file-one-under-authentication). The FTC article, written by Lisa Weintraub Schifferle, who was one of the speakers at the Maryland NTAW Forum, cites: "TaxSlayer didn't require users to have strong passwords, didn't have a written information security program, and wasn't doing risk assessments to identify threats to customer information. The FTC's settlement requires TaxSlayer to have a written security program and safeguards to protect customer information."

IRS and FTC mention a "written information security program," or a "written cyber security plan." When the FTC and IRS are asked to define what factors are needed in an acceptable CS plan, no one seems to have any specific information. Larry Grey, a speaker on CS at the IRS tax forums, has asked 30 information technology (IT) companies if they have ever written a CS plan, and to date Larry has not found one company that has

ever written such a plan. IRS recommends that tax preparers use IRS Publication 4557, Safeguarding Taxpayer Data, to review and assess your security posture.

To be fair, IRS and FTC are prohibited from being too specific when requiring anything. For example, government agencies are not allowed to endorse specific products. I would be curious if government agencies can say what products would not be compliant to warn us from using the wrong products. In lieu of the IRS, FTC, FBI, and other government agencies endorsing software or methods or even giving you a hint of what an acceptable CS plan, there are some people who are avidly researching this area. Bob Jennings (info@taxspeaker.com) has developed a highly recommended course on CS, with checklists and other useful information on protecting your client data. The 2018 version of the CS course has been fully updated and expanded to include the latest information. Bob Jennings recommends using a password manager with a single "master" password to access the program. In the December 7, 2017 edition of PC Magazine, Neil J. Rubenking, in his review of the top ten password managers, Dashlane (www.dashlane.com) was rated 5/5; cost is $40 per user. (https://www.pcmag.com/article2/0,2817,2407168.00.asp).

At the recent NTAW Forum, Michael Lee, IRS Criminal Investigation Special Agent, said that remote access programs, such as GoToMyPC (www.gotomypc.com), were responsible for 60% of data breaches. Lee went on to say that a Virtual Private Network (VPN) is necessary to help secure Wi-Fi communications. Lee also shared that we should avoid using the public Wi-Fi networks provided in hotels, airports, and food establishments. Lee suggested that tax preparers use a dedicated node provided by Internet providers such as Verizon, AT&T, etc.

A common misconception is that the term Wi-Fi is short for "wireless fidelity;" however, this is not the case. Wi-Fi is actually the name of a popular wireless networking technology that uses radio waves to provide wireless high-speed Internet and network connections. Wi-Fi is simply a trademarked phrase that means IEEE 802.11x (https://www.webopedia.com/TERM/W/Wi_Fi.html).

In the IRS presentation, the IRS warned that while the rest of us are doing our holiday shopping, "criminals are shopping for credit card, financial accounts, social security numbers, and other data to claim fraudulent IRS refunds." While those listeners were informed and perhaps even forewarned, the procedures needed to protect consumers while shopping were not presented.

IRS also warned about phishing schemes that are designed to get your financial information. One recently reported phishing scheme was to send an email asking you to update your online financial accounts, download a document from a cloud storage provider, or suggesting you have an IRS refund and that the IRS needs information about your insurance policy to provide the refund. While unstated, the best defense for email phishing schemes is to refuse to click on any link within an email. The "no click policy" is the best way to protect yourself. Clicking on a link can launch all types of malware into your computer without you knowing what you have done with that one click.

Phishing schemes can be foiled by adopting a no click policy for email communications or any link on the internet. Email programs have higher security settings that disable links to prevent inadvertent clicking on links by employees, tax payers and tax preparers. Bob Jennings illustrates how to activate the higher security settings in Outlook with the Outlook Junk Email filter: go to "Junk," go to "Junk Email Options." Select "High" and the "Disable Links" option will automatically be selected by Outlook.

Using a portal to circumvent email communications going into and out of the tax preparation office will also provide protection. Jennings recommends ShareFile's (www.sharefile.com) portal solution. Other portals include SafeSend (www.safesend.com) and Dropbox (www.dropbox.com) – but be aware that Dropbox has been hacked, and is responsible for a large portion of email accounts being compromised and for sale on the dark web.

"After a data breach, there are steps that victims may take to protect their financial accounts and identities." Several months ago, Carol Campbell, Director of the IRS Return Preparer Office, issued a plastic information card with the steps the office recommends tax preparers use should they find their information breached. "If you have a data breach or other security incident, contact: your local IRS stakeholder liaison, your local office of the Federal Bureau of Investigation, file a police report with your local police (although Federal Trade Commission attorney Lisa Weintraub Shifferle advises against filing a police report), email the Federation of Tax Administrators (statealert@taxadmin.org), who will notify state tax agencies, contact your state's attorney general, and notify your insurance carrier to check if your insurance policy covers data security incidents." See Data Theft Information for Tax Professionals on irs.gov.

Many insurance carriers now offer data security policies that cover a data security breach with up to $1 million dollars of services to comply with federal, state, and local laws. (Forrest T. Jones offers such a policy for an annual premium of about $1,000.) Insurance carriers will provide you with additional advice on how to be more secure. Now is the time to sign up for a CS insurance policy. Do not wait until it is too late.

Data breaches do not always lead to filing fraudulent tax return refund claims. "Businesses may have their sensitive information used to open credit card accounts or file fraudulent tax returns for bogus refunds." IRS Stakeholder Liaison Annette Harris suggested that tax preparers should share data security information and precautions with their clients, who may also be targets for cyber criminals. Harris suggested that tax preparers and taxpayers shred all paper with a cross-cut shredder before trashing. Harris said, "Criminals now target tax pros, payroll pros, and employers to get Form W-2 information to file fraudulent tax returns." The criminals could use the data to make money from other cybercrimes.

Raef Meeuwisse, in his book Cybersecurity for Beginners, says that the theft of the information is not the end of the crime. The cybercriminal must sell the information, usually on the Dark Web, to another individual to make money from the theft. Most cybercriminals who steal data are not equipped to use the data to file the fraudulent returns or other schemes used to turn the sensitive information into cash. (Experian has a good definition of the Dark Web at https://www.experian.com/blogs/ask-experian/what-is-the-dark-web/.)

Veronica Tubman, IRS Senior Stakeholder Liaison SB/SE, Communications Liaison, Practitioner Lead for South Carolina, spoke of spear phishing emails, account takeovers, remote access takeover, exploiting the lack of a firewall or anti-virus, and other common schemes that "bad actors attempt to gain access to tax preparer accounts to alter return information and divert refunds." Tubman said, "spear phishing targets a specific audience; 91% of all cyber attacks/data breaches start with spear phishing email, appears as a trusted source (fellow tax practitioners, software provider, potential or current client, or IRS e-Services) with the objective of enticing you to open a link or download an attachment." One such phishing scheme appeared as IRS e-Services asking tax preparers to update their e-Services account information or be subjected to the closing of their e-Services account. Should you receive a phishing email, the Service asks that you forward the email to phishing@irs.gov. Do not click on any link or part of the email. Do not open the email or any attachments.

Account takeover targets your EFIN (Electronic Filing Identification Number). Please "maintain your EFIN: Keep your EFIN current." "Update your EFIN within 30 days of any personnel, address or telephone changes." Remember your "EFIN is not transferable." A separate "EFIN application is required for

each office location where e-File transmissions occur."

Tubman also discussed ransomware. "Ransomware is a type of malicious software from cryptovirology that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. While some simple ransomware may lock the system in a way which is not difficult for a knowledgeable person to reverse, more advanced malware uses a technique called cryptoviral extortion, in which it encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them.[1][2][3][4] In a properly implemented cryptoviral extortion attack, recovering the files without the decryption key is an intractable problem – and difficult to trace digital currencies such as Ukash and Bitcoin are used for the ransoms, making tracing and prosecuting the perpetrators difficult." (https://en.wikipedia.org/wiki/Ransomware).

What do you do if your computer is infected with ransomware? Immediately call the IRS Stakeholder Liaison for your area. One tax preparer attending the NTAW Forum told her story of a ransomware incident where she contacted the FBI, Microsoft, and the IRS stakeholder liaison, and Microsoft was able to retrieve all her data without paying the ransom within a few days. Bill Feehley, President of the Maryland Society of Accountants and Tax Professionals, spoke about his protection against ransomware which involved daily backups. The backups were segregated in the cloud and not on his local computer. Bill makes daily physical backups that he takes off premises at night. Bill also said it was necessary to check the backups routinely, since a backup that will not restore is worthless.

A remote access attack is where the tax preparer routinely uses remote access software to access the tax preparation software on the server at the office. IRS estimates that 60% of cybercrime attacks that steal data hijack low-cost commercial remote access software, which is notoriously free of any cybercrime protection. Never use low-cost remote access software. A relatively expensive virtual private network that involves encryption is not as vulnerable.

Antivirus software is not enough to protect users against all malware. Antivirus software only protects all your digital devices, such as computers, tablets, and smart phones, against viruses. Malware encompasses all types of software that can compromise client data. In addition to viruses, malware consists of worms, adware, ransomware, etc. Only a security suite can adequately protect tax preparers and tax payers from a data breach or cybercrime.

Neil J. Rubenking, PC Magazine, December 11, 2017, reviewed nearly four dozen advanced security suites and still recommends ten top security suites, all of which had at least 4 out of 5 ratings. These include top rated (4.5/5) Bitdefender Internet Security and Total Security (www.bitdefender.com), MacAfee LiveSafe and Total Protection (www.macafee.com), Symantec Norton Security Premium and Deluxe (www.symantec.com), Trend Micro Internet and Maximum Security (www.trendmicro.com), Webroot SecureAnyware Internet Security Complete (www.webroot.com). All other software reviewed had problems, including Windows Defender, which was rated as "not great." The author reminded us that Windows Defender "doesn't truly qualify as a suite" and therefore was not recommended.

Tubman suggested reviewing "Small Business Information Security – The Fundamentals" at the National Institute of Science and Technology (NIST.gov) and IRS Publication 4557, "Safeguarding Taxpayer Data" at IRS.gov. NIST has five action item categories: identify, protect, detect, respond, and recover.

"Identify and control who has access to your business information. Conduct background checks on new employees. Require individual user computer accounts for each employee. Create policies and procedures for information security." (nist.gov) Notice that nothing is said about how to create those policies and procedures which appear to go beyond the first three sentences.

NIST.gov continues: "Protect by limiting employee access to data and information." Specifically how you limit employee access is not explained. "Keep software and security programs updated. Install firewalls on all business networks. Secure all wireless access points. Set up web and email filters." I haven't got a clue how to secure all wireless access points or set up web and email filters. Double check all requests for information with face-to-face communication or a phone call. You can verify if the person you are talking to is really from the IRS by phoning your IRS stakeholder liaison.

NIST.gov goes on to suggest that you "use encryption for sensitive business information. Dispose of old computers and media safely." Old computers should have their hard drives removed and destroyed by physical destruction of the hardware. "Train your employees." Use passwords that are at least 16 characters long, and use alpha numeric characters and symbols.

To help with security breach detection, NIST.gov says "install and update anti-virus, spyware and other malware programs" and "[m]aintain and monitor logs," which was not explained.

To prepare for the possibility of a breach, NIST.gov recommends that you "develop a plan for disasters and information security incidents by reviewing Publication 4557, Safeguarding Taxpayer Data. Develop response plan should you have a data breach by reviewing 'Data Breach Information for Tax Professionals' on IRS.gov."

NIST.gov recover action involves "[mak[ing] full backups of important business data (information). Make incremental backups of important business data (information). Consider cyber insurance. Make improvements to processes, procedures and technologies."

Rubenking discusses firewalls in his PCMag article. Firewalls "monitor all network traffic to prevent inappropriate access from outside the network" and watches "running applications to make sure they don't misuse your network." Bob Jennings recommends "Sonicwall TZ300, which is the latest generation (generation 6) of wired firewall at high-speed (1GB) and a built-in Virtual Private Network for secure remote access." The cost for this hardware-based firewall is about $500. A good hardware firewall monitors inappropriate incoming and outgoing traffic. Software-based firewalls such as Windows firewall does not completely protect your systems.

Some tax preparers are increasing security on their systems by using cloud-based programs and leaving the security and portals up to the professionals. For $1000 per month, Ease Technologies will provide a secure portal and will host your tax and other accounting software and sensitive data on their cloud-based servers (www.easetech.com).

So how can you protect yourself? Do not click on any links in an email. Set your email software to the highest level of security possible which will prevent inadvertently clicking on email links. Use 256-bit encryption. Use one of the highest rated security suites, such as the Bitdefender or Symantec Norton products referenced above. Get a hardware based firewall. Use a secure portal or encrypt all emails. Consider cloud-based hosting of all your sensitive data.

There are many more ways to protect sensitive information. Do your homework and get all the information you can absorb.•

Bibliographies

https://www.natptax.com/EventsAndEducation/Documents/IRS_FTC_NATP_WebinarInstructors.pdf

What to do after a data breach:

https://www.consumer.ftc.gov/blog/2016/09/data-breaches-and-you-new-video