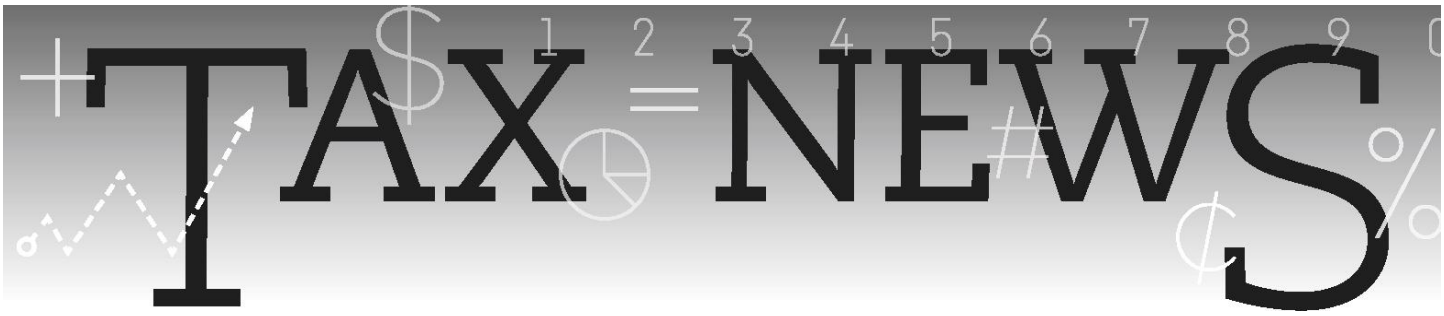

FALL 2019

Dear Client:

On July 1st, The Taxpayer First Act of 2019 was signed into law by President Trump. This bill provides for improvements to the operations of the Internal Revenue Service, better interactions with taxpayers, and more safeguards to protect the integrity of the tax system. We have provided some of the key points from the bill, which impact all taxpayers.
We continue to address the major legislation from the last tax filing season, The Tax Cuts and Jobs Act. The impact to the individual taxpayer is felt in the changes to the Schedule A, Itemized Deductions, with the limitation on the state and local taxes, and elimination of various deductions such as tax preparation fees, investment fees, job hunting costs, and unreimbursed employee expenses. For the business taxpayer the changes were seen in the purchase of assets, elimination of the expenses for entertainment, and the new deduction for qualified business income.
If you have rental property, the IRS has issued new recordkeeping guidelines to help determine whether the rental operations are to be considered an active trade or business or if it remains a passive activity. If you feel you may meet the guidelines, contact our office to determine the appropriate actions to take.
Finally, we address the issue of data breaches and working in a secure computer environment. We are committed to maintaining a safe environment whereby our client data is protected. The IRS is working diligently to provide timely information. We employ additional safeguards in the sharing of information and documents with our clients which may necessitate strong passwords or the use of secure transmissions which may require additional authentication.
Contact our office if you have any questions regarding the information provided, or any other tax situation that you may be facing. We are available to assist with tax planning, tax projections and understanding the legislative and tax changes that may impact you and/or your business.

Taxpayer First Act of 2019

The Taxpayer First Act of 2019 (TFA) was signed into law on July 1, 2019. The focus of the bill is to enact changes in the IRS's organizational structure which includes customer service, enforcement procedures, management of information technology, and improving interactions with taxpayers.

Some of the changes have already gone into effect as of the date of the enactment of the Act, some were effective 45 days after the date of the enactment of the Act. Other changes are to be built into the new organizational plan for the agency and are applicable by December 31, 2020.

While the TFA is a comprehensive bill which includes changes for the IRS, the tax professional community and the individual taxpayer, following are some provisions which will affect the individual taxpayer:

IRS Independent Office of Appeals: An independent administrative appeals function at the IRS (these rules had been carried in the agency's internal rules) is formalized. The IRS Office of Appeals is renamed the "IRS *Independent* Office of Appeals." When a taxpayer requests an appeals hearing, the TFA requires that the administrative case file referred to the IRS Independent Office of Appeals be made available to eligible individual and small business taxpayers. Eligible taxpayers are those that, for the tax year to which the dispute relates, are: (1) individuals with adjusted gross income not exceeding $400,000, and (2) entities with gross receipts not exceeding $5 million for the tax year.

Offers-in-Compromise: Taxpayers with incomes below 250% of the Federal poverty level are not required to submit the application fee and initial payment when proposing an OIC to the IRS.

Increased Penalty for Improper Disclosure or Use of Information by Preparers of Returns: In the case of disclosure of taxpayer identity information by a return preparer where the information is used in an identity theft crime, whether or not related to the filing of a tax return, increased civil penalties will apply. The increase in penalty is to enlist the participation of all tax preparers in securing their client's information.

Notice to Taxpayer of IRS Contact with Third Party: The IRS may not contact any person, other than the taxpayer, regarding the determination or collectibility of a tax liability without providing the taxpayer with notice at least 45 days notice. This replaces the vague requirement that reasonable notice must be provided "in advance" to the taxpayer.

Misdirected Tax Refund Deposits: The IRS is to establish procedures for taxpayers to report instances where they did not receive their refund, or a refund was erroneously delivered to the wrong taxpayer. The IRS is to coordinate with financial institutions in order to (1) identify the accounts to which transfers were made, (2) recovery of the amounts transferred, and (3) facilitate the payment of the refund to the correct account of the taxpayer.

Notification of Suspected Identity Theft: If a determination is made by the agency that there has been unauthorized use of the identify of any individual or their dependents, as soon as practical they are to notify the individual of such determination, provide instructions on how to file a report with law enforcement, and offer assistance with the process of responding to the various agencies.

Identity Protection Personal Identification Numbers (IP PIN): Currently, the IP PIN program does not protect victims whose identify has been stolen but have not yet had their social security number compromised. This provision requires the IRS to establish a voluntary process under which any taxpayer can request an IP PIN to use in filing a tax return. The Act expands voluntary access to IP PINs nationwide over the next five years.

Single Point of Contact for Tax-Related Identity Theft Victims: Procedures will be developed and implemented to ensure that any taxpayer whose return has been delayed or otherwise adversely affected due to tax-related identity theft has a single point of contact at the IRS throughout the processing of the taxpayer's case. The single point of contact shall track the taxpayer's case to completion and coordinate with other IRS employees to resolve case issues as quickly as possible.

Payment of Taxes by Debit and Credit Cards: The TFA allows the IRS to directly accept credit and debit cards for taxes, provided the transaction fees are paid by the taxpayer. Currently, the IRS uses a third-party processor to accept debit and credit card payments. The IRS is directed to minimize the fees when entering into contracts to process credit and debit card transactions.

Modernization of Internal Revenue Service Organization Structure: A comprehensive written plan to redesign the organization of the Internal Revenue Service is to be submitted to Congress. The plan shall: (1) ensure the successful implementation of the priorities specified by Congress, (2) prioritize taxpayer services to ensure that all taxpayers easily and readily receive the assistance that they need, (3) streamline the structure of the agency which includes minimizing the duplication of services and responsibilities within the agency, (4) position the IRS to combat cybersecurity and other threats to the agency, and (5) address whether the Criminal Investigation Division (CID) should report directly to the Commissioner.

Please contact the office if you have any questions regarding these provisions, or any other changes, of the Taxpayer First Act.

Maintaining a Secure Computer Environment

The IRS has released a series of security related articles to assist both taxpayers and tax professionals in creating a secure computer environment. They encourage everyone to review the security protocols you have in place, what steps you are taking to protect your private information, and how to make your online presence more secure.

1. Anti-virus software

Although details may vary between commercial products, anti-virus software scans computer files or memory for certain patterns that may indicate the presence of malicious software and looks for patterns based on the signatures or definitions of known malware from cyber criminals. Anti-virus vendors find new issues and update malware daily, so it is important that you have the latest updates installed on your computer.

Once users have installed an anti-virus package, they should scan their entire computer periodically by doing:

- Automatic scans – Most anti-virus software can be configured to automatically scan specific files or directories in real time and

prompt users at set intervals to perform complete scans.

- Manual scans – If the anti-virus software does not automatically scan new files, users should manually scan files and media received from an outside source before opening them. This manual process includes:

Saving and scanning email attachments or web downloads rather than opening them directly from the source.

Scanning portable media, including CDs and DVDs, for malware before opening files.

Sometimes the software will produce a dialog box with an alert that it has found malware and asks whether users want it to "clean" the file (to remove the malware). In other cases, the software may attempt to remove the malware without asking first.

When selecting an anti-virus package, users should learn about its features, so they know what to expect. Keep security software set to automatically receive the latest updates so that it is always current.

A reminder about spyware, a category of malware intended to steal sensitive data and passwords without the user's knowledge: Strong security software should protect against spyware. But remember, never click links within pop-up windows, never download "free" software from a pop-up, never follow email links that offer anti-spyware software. The links and pop-ups may be installing the spyware they claim to be eliminating.

A reminder about phishing emails: A strong security package also should contain anti-phishing capabilities. Never open an email from a suspicious source, click on a link in a suspicious email or open an attachment – or else you could be a victim of a phishing attack and you and your clients' data could be compromised

2. Firewalls

Firewalls provide protection against outside attackers by shielding your computer or network from malicious or unnecessary web traffic and preventing malicious software from accessing your systems. Firewalls can be configured to block data from certain suspicious locations or applications while allowing relevant and necessary data through.

Firewalls may be broadly categorized as hardware or software. While both have their advantages and disadvantages, the decision to use a firewall is far more important than deciding which type you use:

Hardware – Typically called network firewalls, these external devices are positioned between a computer and the internet (or another network connection). Hardware-based firewalls are particularly useful for protecting multiple computers and control the network activity that attempts to pass through them.

Software – Most operating systems include a built-in firewall feature that should be enabled for added protection even if using an external firewall. Firewall software can also be obtained as separate software from a local computer store, software vendor or ISP. If downloading firewall software from the internet, make sure it is from a reputable source (such as an established software vendor or service provider) and offered via a secure website.

While properly configured firewalls may be effective at blocking some cyber-attacks, don't be lulled into a false sense of security. Firewalls do not guarantee that a computer will not be attacked. Firewalls primarily help protect against malicious traffic, not against malicious programs (malware), and may not protect the device if the user accidentally installs malware. However, using a firewall in conjunction with other protective measures (such as anti-virus software and safe computing practices) will strengthen resistance to attacks.

3. Two-factor authentication

Many email providers now offer customers two-factor authentication protections to access email accounts. Two-factor authentication helps by adding an extra layer of protection beyond a password. Often two-factor authentication means the returning user must enter credentials (username and password) plus another step, such as entering a security code sent via text to a mobile phone. The idea is a thief may be able to steal the username and password but it's highly unlikely they also would have a user's mobile phone to receive a security code and complete the process.

4. Backup software/services

Critical files on computers should routinely be backed up to external sources. This means a copy of the file is made and stored either online as part of a cloud storage service or similar product. Or, a copy of the file is made to an external disk, such as an external hard drive that now comes with multiple terabytes of storage capacity.

5. Drive encryption

Drive encryption, or disk encryption, transforms data on the computer into unreadable files for an unauthorized person accessing the computer to obtain data. Drive encryption may come as a stand-alone security software product. It may also include encryption for removable media, such as a thumb drive and its data.

6. Virtual Private Network (VPN)

A VPN provides a secure, encrypted tunnel to transmit data between a remote user via the Internet and the company network. Search for “Best VPNs” to find a legitimate vendor; major technology sites often provide lists of top services.

Finally, it is strongly recommended that you contact an IT specialist to test your system for any weaknesses. The best defense is a strong offense against malicious attacks to your computer system. While you may not think the information you have on your computer is valuable; the access to your personal information, bank accounts and credit cards is the only entre’ the hackers need to steal your identity and create havoc in your personal life.

It is the policy in our office that we do not download any unknown or unsecured files onto our network. We employ secure transmission protocols that all clients are required to use when transmitting files to our office.

Check Your Beneficiary Designations Now, Before Disaster Strikes

You should probably take one very important estate planning action as soon as you finish reading this.

Check the beneficiary designations for your:

- bank accounts,
- brokerage firm accounts,
- tax-favored retirement accounts,
- company benefit plans,
- life insurance policies,
- annuities, and
- 529 college savings accounts.

If you have not yet turned in the forms to designate beneficiaries, do so today. If the forms are out of date, change them to reflect current reality before it’s too late.

If you need motivation, here are two real-life horror stories to light a fire under you.

Real-Life Horror Story 1

Dad failed to change the beneficiary designations for his Boeing Corporation pension benefits and life insurance after his divorce, so Dad’s former wife was still the named beneficiary.

Two months later, Dad died in a car crash. The Supreme Court ruled 7-2 that the beneficiary designations trumped a state law that would have automatically disinherited the ex-wife. So, the ex-wife received the money, and the kids were handed the bills for an unsuccessful legal fight that went all the way to the Supreme Court.

Real-Life Horror Story 2

In another real-life case, the ex-spouse collected $400,000 from Dad’s company savings and investment plan even though the ex-spouse had specifically waived any interest in the plan under the divorce agreement.

Believing the divorce agreement was the last word on the subject, Dad failed to turn in the form to officially change the plan beneficiary from his ex-spouse to his daughter.

He died seven years after the divorce. The company plan document stipulated that beneficiaries could be changed only by submitting the required form.

The Supreme Court unanimously ruled that the hideously outdated beneficiary designation trumped the divorce agreement. So, the ex-spouse received the $400,000, and the daughter received nothing.

The Disaster Avoidance Message

Divorce is not the only situation where failing to turn in or update beneficiary designation forms can cause heartache for your intended heirs—it’s just the most obvious situation.

For example, the same basic issue exists if you become disenchanted with an adult child who has decided to become a professional Frisbee golfer on top of marrying someone you cannot stand.

Or you might now decide to leave more of your life insurance benefits to an adult child who just had twins and less to your childless offspring.

You get the idea. When things in your life change, you may need to refresh your beneficiary designations.

Avoids Probate

Another big reason to designate beneficiaries: it avoids probate. Also, consider naming contingent beneficiaries. These are individuals who stand in line behind your primary beneficiaries.

Warning

Do not rely on a will or living trust document to override outdated beneficiary designations. As a general rule, whoever is named on the most recent beneficiary form (which may not be nearly recent enough) will get the money automatically when you die—regardless of what other documents might say.

Takeaways

Check your designations at least once a year or whenever significant life events occur.

It usually takes only a few minutes to conduct a checkup and make any needed changes. Often you can access the necessary forms online. But if you wait, it could be too late, as illustrated by the real-life horror stories presented earlier. Don't wait!

Rental Real Estate Safe Harbor for the Qualified Business Income Deduction

(Code Section 199A)

One of the major provisions of the Tax Cuts and Jobs Act was the creation of a new deduction (Code Section 199A) for business owners operating as a sole proprietor, as a shareholder in an S Corporation or a partner in a partnership venture. This new deduction also extended to the owners of rental real estate; however, the initial guidelines were unclear as to what properties qualified and how to substantiate the activities of the rental owner.

Subsequently, the IRS has released safe harbor guidelines for those who think they may qualify for the new deduction. Solely for the purposes of the qualified business income deduction, Section 199A, a rental real estate enterprise will be treated as a trade or business if the following safe harbor requirements are satisfied during the taxable year with respect to the rental real estate enterprise:

- Separate books and records are maintained to reflect income and expenses for each rental real estate enterprise;
- 250 or more hours of rental services (see below for listing) are performed per year with respect to the rental enterprise; and
- The taxpayer maintains contemporaneous records, including time reports, logs, or similar documents, regarding the following: (i) hours of all services performed; (ii) description of all services performed; (iii) dates on which such services were performed; and (iv) who performed the services. Such records are to be made available for inspection at the request of the IRS.

Rental services include: (i) advertising to rent or lease the real estate; (ii) negotiating and executing leases; (iii) verifying information contained in prospective tenant applications; (iv) collection of rent; (v) daily operation, maintenance, and repair of the property; (vi) management of the real estate; (vii) purchase of materials; and (viii) supervision of employees and independent contractors. Note that travel to and from the rental property(ies) does not count towards the 250 hours.

Real estate used by the taxpayer as a residence for any part of the year is not eligible for this safe harbor. Real estate rented or leased under a triple net lease is also not eligible for this safe harbor (however, it may still qualify as a trade or business based on the activities of the owner). A triple net lease includes a lease agreement that requires the tenant or lessee to pay taxes, fees, and insurance, and to be responsible for maintenance activities for a property in addition to rent and utilities. This includes a lease agreement that requires the tenant or lessee to pay a portion of the taxes, fees, and insurance, and to be responsible for maintenance activities allocable to the portion of the property rented by the tenant.

If the taxpayer elects the safe harbor method, they must include a statement attached to the return on which it claims the section 199A deduction. The IRS has created a new form, Form 8995, *Qualified Business Income Deduction*, to be used when claiming this deduction.

Contact the office to verify if you would meet this new criteria for claiming the deduction and the paperwork we will need when preparing your income tax return.

For more information, please contact me.

Contact the office if you have any questions regarding these issues or any changes in your household that may have an impact on your tax filing requirements.

As your tax professional, I assure you that I will be keeping a watchful eye on Congress and on IRS actions which may affect your business and your tax filings in the New Year. I will be happy to address any concerns and answer questions you have about any of the issues covered in this newsletter. Thank you for the opportunity and privilege of allowing me to serve as your tax professional this past year.

Best regards,
Stephen W. McKown

TAX CENTER
Fast & Professional Tax Preparation™
Tax Center of Cary and Morrisville
1103 Grace Park Dr.
Morrisville, NC 27560
Phone 919-380-0073
TaxCenterofCary.com