

Mayolo & Associates LLC
795 Morgantown Road Uniontown, Pa 15401
Ph: 724-439-3455 Fax: 724-439-3467
Email: pete@mayolocpa.com
Web: www.mayolocpa.com

January 2017

Re: **Protecting Yourself Against Tax-Related Identity Theft**

Dear Client:

Tax-related identity theft continues to be an ever-growing national crisis.

The Government Accountability Office (GAO) estimated that in tax year 2013, fraudulent tax refunds misdirected to identity thieves was about \$5.8 billion and impacted over 2.4 million U.S. taxpayers. Unfortunately, this fraudulent activity has continued to rapidly expand since 2013. All taxpayers must be diligent in further protecting themselves from becoming identity theft victims.

As a valued client, we want to share with you some proactive steps and resources to help in your defense of tax-related identity theft. However, should you become aware that you are a victim of identity theft or that your private financial information has been compromised, please contact us immediately for additional information and assistance.

Suggestions to Protect You and Your Family from Identity Theft

Secure private personal information. Safeguard family names and birthdates, account numbers, passwords, and Social Security numbers. Carefully consider all requests to provide your Social Security number before giving it out and don't hesitate to ask why your private information is being requested. Secure your Social Security card in a safe or safety deposit box and never in your purse or wallet. Proactively shred all documents that contain personal data before disposing of them, even solicitations and "junk" mail that may unknowingly contain account numbers and personal information.

Monitor personal information shared on social media. Cybercriminals methodically gather data from online sources, including commonly used identifiers such as birthdate, maiden name, pet name, hometown, significant other, and/or children's information. Be cautious who you communicate with online and be selective before accepting electronic invitations from people you do not know or recognize. Separate what you post publicly from what you post with your personal contacts. Do not post personal and family data.

Secure your computer. Use current versions of antivirus, malware protection, and firewalls and update these programs frequently. Consider having this software updated automatically, as well as using different computers for business and finances than you do for social media and personal matters. Use strong passwords, change them frequently, and do not share them with others. Review [IRS Publication 4524, Security Awareness for Taxpayers](#), for additional tips.

Beware of impersonators. Criminals utilize sophisticated computer technology, such as dialers and automated questions, to contact thousands of targets daily. Do not provide personal information to callers you do not know. If any caller requests that you verify personal information, be extremely cautious and

ask for further confirmation of their identity, such as their telephone number, website, email address, supervisor's name, and mailing address. The IRS never initiates contact by telephone.

Beware of unsolicited emails and current phishing scams. Don't open attachments or electronic links unless you know the sender. Internet sites should have a lock symbol to show the site is encrypted. Always beware of entering sensitive data. Forward emails received from IRS impersonators to phishing@irs.gov. The IRS never initiates contact by email, text message, or social media channels. For more guidance on phishing scams, go to irs.gov/uac/report-phishing.

Monitor your personal information. Review your bank and credit card statements often.

Consider electronic transmission of financial information. No sensitive tax or personal information should be sent via unsecured email, even information being transmitted to CPAs, bankers, and/or financial advisors. A secure portal, encrypted email, or physical mailing of sensitive information is necessary.

Order your free annual credit report. Call 1-877-322-8228 or go to www.annualcreditreport.com to request your report and/or search for creditors you do not know. Choose to use only the last four digits of your Social Security number on your report. Consider placing a credit card freeze on your account so only creditors you approve are allowed to access your file.

What to Do if You Become a Victim of Tax-Related Identity Theft

You may learn that your identity has been compromised by receiving a letter in the mail from the IRS. Alternatively, your CPA may contact you when your personal income tax return is electronically filed and subsequently rejected. If you receive a notice indicating identity theft, please contact us immediately to schedule a meeting to receive assistance in taking the appropriate steps with the IRS to resolve the matter.

Other ways you may discover your identity has been stolen include:

- Finding purchases on your credit card that you did not make
- Discovering withdrawals from an account that you did not make
- Seeing that your address has been changed for certain accounts, or no longer receiving your regular bills. (Cyber criminals may change your address when filing a return.)

The unfortunate reality is that personal data is already at risk everywhere, but we will work with you to reduce the likelihood of you being victimized by cyber criminals. As your CPA and trusted advisor, we understand the need to protect your privacy and take data protection very seriously. Our security and data integrity meets the highest industry standards established by the IRS and Federal Trade Commission. We have also established protocols to guard access to client files.

Please don't hesitate to contact us at 724-439-3455 with questions or concerns or if you would like to meet with us to discuss this issue or any financial or tax needs.

Regards,

Mayolo & Associates LLC
Peter J. Mayolo CPA, President