



## **PREPARE FOR THIS TAX SEASON BY PROTECTING YOUR PERSONAL INFORMATION**

As we approach another tax season, it is important for us to address an issue that impacts all of our clients. That issue: data security.

As we have seen in recent years, the problems of identity theft and the fraudulent filing of tax returns have gained a lot of interest in the media. In 2015, the IRS's vulnerabilities were exposed in dramatic fashion. Between February and May, a group of hackers swiped information off over 300,000 individual online IRS accounts. After obtaining this data, the hackers filed fraudulent tax returns with the stolen identities.

Unless the IRS catches these hackers or adequately strengthens its security measures before this tax filing season begins, the almost 15,000 fraudulent returns and \$50 million in refunds already paid to the hackers will pale in comparison to the damage they could cause in the future. Currently, the IRS pays nearly \$5 billion a year in refunds for fraudulent tax returns.

As a whole, states are generally not doing much better at curbing tax identity theft. Last February, TurboTax had to halt its filing of state tax returns because of an upsurge in fraud. Regretfully, Missouri is not immune to this trend. The state Attorney General's office received 388 complaints of tax return fraud during the 2015 filing season alone.

The manner in which these criminals operate is the same at the federal and state level. A criminal obtains personal information (name, date of birth, social security number, etc.) on a victim. The criminal then files a tax return early in the year using the victim's personal information. By the time the victim gets around to filing his return, he discovers that a return with his personal information was already filed.

This process is made easier with so much "personal" information available through social media, marketing data and credit reports. This information gets tracked, saved and sold on the black market. Because social security numbers typically sell for 25 cents apiece, anyone can buy them in bulk.

UHY LLP is deeply committed to protecting you and your personal information. We devote significant time and attention to utilizing the best software, security protocol and highly-skilled professionals to ensure that the information you share with us is kept safe.

We recommend that you submit your tax information to us as early as possible so that we have the best chance to file before any criminal can. Also, use extreme caution when deciding what you share online, in surveys and through social media. Should anyone gain unauthorized access to your information and fraudulently file a tax return, then – as with any other tax concern – do not hesitate to contact us at 314.615.1200. We are here to help you.



## **TIPS FOR MINIMIZING YOUR RISK TO TAX RETURN SCAMS**

- Submit all tax documents to UHY LLP as soon as you receive them so that we can prepare your tax return before any criminal can have the opportunity to do so. This will protect your refund. It will also avoid the hassle of having to report fraud to the IRS and then wait on the IRS to rectify the situation.
- Do not believe anyone who calls you saying he is from the IRS. A common technique used by criminals is to impersonate the IRS on the phone. However, the IRS rarely calls taxpayers. Even when the IRS does actually call taxpayers, this only occurs after the IRS has already sent multiple notices to the taxpayer via the United States Postal Service.
- Do not believe anyone who sends you an email saying he is from the IRS. The IRS never uses email to make a first contact with a taxpayer. Instead, the IRS will send notices to the taxpayer via the United States Postal Service.
- Do not trust emails from various tax services – such as TurboTax – that advise you to install software on your computer. This is often malware. In addition, do not trust emails that prompt you to provide personal information. This is often how criminals obtain the data they need to file fraudulent tax returns.
- Do not use family members' names or other widely-known information about you – especially if this information can be obtained through public social media profiles – as your passwords or answers to security questions to access online accounts.
- Never hesitate to contact your professional at UHY LLP. We are here to serve you and we are happy to discuss in greater detail with you the procedures we follow to protect your personal information.