SEILER LLP
CERTIFIED PUBLIC ACCOUNTANTS

TAX ALERT

6/25/2018

Tax-related Identity Theft Continues in 2018

The 2017 tax filing due date may have passed, but businesses and individuals are still at risk of becoming identity theft victims. We'll show you common tax-related scams and how to protect yourself and your company.

What is tax-related identity theft?

Tax-related identity theft typically occurs by a thief using a stolen social security number in order to file a false tax return and fraudulently receive a tax return. As a victim, you may not become aware of the occurrence until you file your true tax return, only find out that one has already been completed using your SSN. Alternatively, the IRS may send a letter stating that it has received a suspicious return using your specific SSN.

In addition to individual tax fraud, businesses are also at risk of becoming victimized. At larger companies, fraudsters may target human resources employees or the payroll department to collect employee data. For smaller businesses, scammers may pursue their employer identification numbers.

In order to protect yourself, your company, and your employees, it's important to learn what types of scams these individuals are implementing to phish information.

Scams Targeting Individual Tax Payers

Scam artists use multiple channels to conduct their tax-related identity theft against individuals. Here are the most common schemes to be aware of:

Phone schemes. This past April, less than 10 days after the tax return filing deadline, the IRS highlighted a new phone scam conducted by fraudsters who program their computers to display the phone number of the local IRS Taxpayer Assistance Center (TAC) on the taxpayer's Caller ID. If the taxpayer questions the legitimacy of the caller's demand for a tax payment, the caller directs him or her to IRS.gov to verify the local TAC phone number.

The perpetrator hangs up, calls back after a short period — again "spoofing" the TAC number — and resumes the demand for money. These scam artists generally require payment on a debit card, which allows them to directly access the victim's bank account.

In another phone scheme, the criminals claim they're calling from the IRS to verify tax return information. They tell taxpayers that the agency has received their returns and simply needs to confirm

a few details to process them. The taxpayers are prompted to provide personal information such as a social security number and bank or credit card numbers.

Digital schemes. Emails that appear to be from the IRS are part of phishing schemes intended to trick the recipients into revealing sensitive information that can be used to steal their identities. The emails may seek information related to refunds, filing status, transcript orders, or PIN information.

The scammers have developed twists on this approach, too. The emails might seem to come from an individual's tax preparer and request information needed for an IRS filing. Or the information request could arrive via text messages. Whether by text or email, the communication states that "you are to update your IRS e-file immediately" and includes a link to a fake website that mirrors the official IRS site. Emails also could include links that cause the recipients to download malware that infects their computers and tracks their keystrokes or allows access to files stored on their computers.

Scams Targeting Businesses

For several years now, criminals have employed different spoofing techniques known as business email compromise (BEC) or business email spoofing (BES). They disguise an email to a company's human resources or payroll department so it seems to come from an executive in the company. The email requests a list of all employees and their Forms W-2 — information that can be used to file returns in the employees' names.

Scammers also are pursuing businesses' employer identification numbers. They then report false income and withholding and file for a refund in the companies' names. Even worse for the companies, the IRS could go after them for payroll taxes reported as withheld but not remitted.

Additionally, the IRS recently announced that it has seen a sharp increase in the number of fraudulent filings of certain business tax forms, including Schedule K-1 and those filed by corporations and partnerships. As a result, the IRS may ask businesses for additional information (such as the driver's license numbers of owners) to help identify suspicious tax returns.

How to Identify True IRS Communications

The IRS has made it clear that it will not do any of the following:

- Threaten to bring in law enforcement to have someone arrested for nonpayment of taxes
- Revoke a driver's license, business license, or immigration status for nonpayment
- Demand a specific payment method, such as a prepaid debit card, gift card or wire transfer
- Request a debit or credit card number over the phone
- Demand the payment of taxes without the opportunity to question or appeal the amount owed (the IRS usually mails a bill when a taxpayer owes taxes)
- Send unsolicited emails, texts or messages through social media channels suggesting taxpayers have refunds or need to update their accounts
- Request any sensitive information online

The IRS may call or visit a home or business, but only in very limited circumstances. It might do so, for example, if a taxpayer has a severely overdue tax bill, to secure an employment tax payment, or to tour a business as part of an audit or a criminal investigation. But even in those special situations, the IRS generally sends several notices by mail first.

With these tips in mind, you should be well-prepared to navigate any suspicious phone calls, emails, or letters from anyone claiming to be an IRS representative.

What to Do If Your Tax Information has been Compromised

If you know or suspect you've fallen prey to tax-related identity theft, you'll need to file IRS Form 14039, "Identity Theft Affidavit." You can also report this kind of theft to the IRS through the FTC's IdentityTheft.gov website. Remember, though, that filing the affidavit doesn't eliminate the need to pay your taxes.

In addition, you can file a complaint on the FTC's website and contact one of the three major credit bureaus (TransUnion, Experian and Equifax) to place a fraud alert on your credit records. This process is the same regardless of what type of identity theft you or your business has experienced.

You also should contact your financial institutions and close any financial or credit accounts opened or tampered with by identity thieves. After your accounts have been updated for accuracy, check to make sure all of the corrections are reflected in your credit reports as well.

Even if you don't fall for an email scam, you should still report it. The IRS urges individuals who receive unsolicited emails purporting to come from the IRS to forward the messages to phishing@irs.gov before deleting. That can help prevent future scams from affecting other individuals and companies.

Next Steps

We can help you avoid tax-related identity theft. If you receive a suspicious communication from the IRS or other taxing authority, contact your Seiler tax advisor for confirmation of its validity and advice on how to proceed.