Long Island Business News

Preventing tax return fraud

By: Brittany Bernstein April 24, 2017

Identity thieves have stolen more than $107 billion in the past six years, with $16 billion stolen in 2016 alone, according to the 2017 Identity Fraud Study released by Javelin Strategy & Research.

This includes tax return fraud, a pervasive scheme in which crooks steal taxpayers' identities and fraudulently file those individuals' tax returns to collect their tax refunds. In 2016, the IRS confirmed that 787,000 cases of tax return fraud made it into its tax return processing systems.

In many ways, taxpayers' "hands are tied" in preventing their identities from being stolen, because they are forced to share information with the IRS and employers, said James Taliento, founder and principal consultant at Cursive Security in Huntington.

"Everything today is digital," Taliento said. "Your employer maintains digital records, the schools that you attend maintain digital records, [as do] hospitals, insurance providers and of course the IRS."

Each of these sources possesses enough information to allow someone to steal and abuse an individual's identity and/or file a fraudulent return.

"The problem is that we almost have no choice but to entrust these entities with our information, and in doing so we have to cross our fingers and hope that they have the means to protect it," Taliento said.

The problem with institutions like schools and hospitals having a vast amount of information is that their objectives don't necessarily align with protecting information, Taliento said.

In K-12 education, for instance, it is hard for schools to justify spending money on protecting data that they could be spending on educational costs, while hospitals want to spend money on saving lives, not data. This makes healthcare and school records prime targets for hacking because of the underground economy that monetizes personal information.

What taxpayers can do, Taliento says, is be vigilant. People should check their tax transcript for changes every so often, paying extra attention to any changes in their filing status or address. People should always be skeptical of anyone asking for personal information, whether it be over phone or email, because phishing scams continue to prey on unsuspecting taxpayers.

Leslie Tayne, founder and head attorney of Tayne Law Group in Melville, which represents clients in debt management and resolution, also warned of phishing scams, reiterating that the IRS will not contact people via phone or email, but always in a letter first. If you're ever unsure, she added, there is "nothing scary" about calling your local IRS office.

"The tax return fraud is a hard one," Tayne said. "You want to be very careful. There's very little you can do. It's really unfortunate."

However, there are a couple of things taxpayers can do to try to lessen their chances of having their identities stolen, like filing earlier, shredding all documents, monitoring their credit report, limiting the amount of credit cards used, being very careful with passwords, always retrieving mail in a timely manner, reviewing credit card statements and reporting any suspicious activity right away. Taxpayers should use a reputable firm as well as a secure computer with a firewall when filing online.

“You shouldn’t be doing your taxes in a Starbucks,” Tayne said.

Tax professionals should be making sure they’re confirming the identity of clients and using secure programs. They need to be aware that they’re the ones that could be giving clients’ information up, Tayne said.

Tax service providers should have a plan in case data theft occurs and make sure that they are using the latest and most aggressive scans for any type of malware. If a data breach occurs, it is important to contact the IRS immediately, Tayne said.

Carolyn Mazzenga, partner in charge of the Melville office of Marcum, said that her public accounting firm, and many others, takes multiple precautions to protect client information.

Mazzenga said that all hard-copy paper is put into locked boxes and shredded and any tax return that is being sent to a client is not just password-protected, but also encrypted. Marcum uses a secure portal over which both clients and employees send and receive information.

Payroll companies, which Taliento says are “essentially a warehouse of personal data,” are also organizations that can fall prey to hacking and phishing scams.

“An email would go out to a payroll department or a payroll company and the email would look like it was coming from the owner of the company and the information would be provided to that company, only to find out that was a fraudulent email and that information was available to be used in fraudulent tax return information,” Mazzenga said.

She added that payroll companies should use encrypted software, and they should know who their customer is, who to contact within a company to get information and who they can send information to.

As far as taking matters into their own hands, taxpayers should avoid leaving sensitive information lying around and should verify the security of websites used for shopping and banking along with anything that asks for a Social Security number or bank account information, she said.

“I’ve seen some people who say they don’t want to have their information online but the reality is the stuff is online anyway,” Tayne said.

Four of five tax returns are expected to be filed online this year, according to the IRS.

“If someone says, ‘I’m just not going to go online – with the way of the world and the way we do business now – in some cases you have no choice,” Mazzenga said. “The old-fashioned way (hard-copy snail mail) is not much better. What’s preventing somebody from going to your mailbox and taking your mail?”

Yigal Rechtman, a forensics principal at Jericho-based Grassi & Co., said something as simple as having a birthdate publicly available on a Facebook account can leave a person vulnerable to identity theft, as a date of birth is sometimes the only information required to verify identity.

More recently, New York and a few other states have begun requiring driver's license information to e-file, in an effort to stunt rapidly growing tax return fraud because though criminals may have dates of birth and Social Security numbers, they may not have driver's license information.

"I think [the driver's license requirement] is helpful," Mazzenga said, "but who knows how long it will be before some creative person knows how to hack into that system and we'll have to deal with another way of avoiding tax fraud."

Rechtman again noted the danger of posting personal information online, citing teens who post pictures of their newly acquired licenses online.

He also warned that those who have previously had their identity compromised are more vulnerable to future attacks.

Electronic payment systems company ACI Worldwide recently estimated that 46 percent of Americans have had their card information compromised at some point in the past five years.

For those who are concerned about their identity being stolen, Rechtman recommends using a credit freeze instead of a commercial credit monitoring service.

The IRS is actively working to stop fraud by adding 37 new required data elements, expanding its W-2 verification code initiative and most recently, suspending the data retrieval tool on the Federal Application for Financial Aid that allowed applicants to complete the form using their tax information from the IRS.

The IRS commissioner suspended the tool after about 8,000 fraudulent returns were filed using FAFSA information, and some 100,000 taxpayers' information may have been compromised.

"Where there is a will, there is a way," Taliento said. "Why wouldn't an attacker abuse this system? It holds plenty of information and within a relatively short period of time an attacker could abuse that information in hopes of obtaining a big payout."

Though in many ways, taxpayers' personal information is "out of their hands," awareness is key.

"You just want to be aware of it: Don't put your head in the sand and say it's not going to happen because your information is out there," Tayne said.