Rhode Island Department of Revenue
Division of Taxation

ADV 2018-37
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
SEPTEMBER 4, 2018

Tax professionals should be alert to subtle signs of data theft

Cybercriminals leave few signs; clients are harmed when fraudulent returns are filed

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit urge tax professionals to be alert to the subtle signs of data theft. The Security Summit said that there are cases in which tax practitioners are victims of theft and don't even know it.

Cybercriminals often leave few signs of their burglary until the fraudulent tax returns are filed and clients are harmed. This is one more reason tax professionals should use strong security protections to prevent data theft from occurring, the Security Summit said.

Although the Security Summit is making progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices are on the rise. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder to detect.

Warning signs

Following are signs that your office may have experienced a data theft:

- E-filed returns begin to be rejected because returns with client Social Security numbers were already filed.
- Clients who haven't filed tax returns begin to receive taxpayer authentication letters (5071C, 4883C, 5747C) from the IRS.
- Clients who haven't filed tax returns receive refunds.
- Clients receive tax transcripts that they did not request.
- Clients who created an IRS online services account receive an IRS notice that their account was accessed or IRS emails stating their account has been disabled. Or clients unexpectedly receive an IRS notice that an IRS online account was created in their names.
- The number of returns filed with the tax professional's Electronic Filing Identification Number (EFIN) exceeds the number of clients.
- Tax professionals or clients respond to emails that the firm did not send.
- Network computers are running slower than normal.
- Computer cursors move or change numbers even though no one is touching the keyboard.
- Network computers lock out employees.

Because IRS systems will only accept one unique Social Security number, taxpayers often discover they are a victim when they attempt to e-file and their tax return is rejected because a return with their SSN already is in the system. Or, more commonly, the IRS identifies a return that could be an identity theft return and sends a letter to the taxpayer asking them to contact the agency to let the IRS know if they filed the return.

Earlier this year, tax-savvy cybercriminals stole taxpayer data from a series of tax professionals nationwide, immediately filing fraudulent returns before the tax professionals were aware of the robbery.

The crimes were first reported to the IRS by taxpayers who unexpectedly received refunds in their bank accounts. The crooks, posing as IRS contractors, tried calling the taxpayers to get them to forward the fraudulent refund to their accounts.

Identity thieves sometimes try to leverage the stolen data by using taxpayer information to access the IRS's Get Transcript system. Taxpayers who receive transcripts by mail but did not order them are sometimes victims of this approach. Get Transcript Online is protected by a robust, two-factor authentication process. But crooks may still try to use stolen identities to try to create Get Transcript accounts, which results in the IRS disabling the account and sending the taxpayer a letter.

About this announcement

This is the ninth in a series of Security Summit announcements called "Protect Your Clients; Protect Yourself: Tax Security 101."

The Security Summit awareness campaign is intended to provide tax preparers and other tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, payroll and tax financial product processors, tax professional organizations and financial institutions. Partners in the Security Summit work together to combat identity theft to protect the nation's taxpayers.

Weekly review

During the tax filing season, tax practitioners should make a weekly review of returns filed with the office's EFIN. A report is updated weekly by the IRS.

Tax preparers can access their e-File applications and select "check EFIN status" to see a count. If the numbers are inflated, practitioners should contact the IRS's e-Help Desk. Tax professionals may also notice IRS acknowledgements for returns they did not e-file. Acknowledgements are sent soon after a return is transmitted.

Tax professionals who fall victim to spear-phishing email scams, which are common ways cybercriminal access office computers, may suddenly see responses to emails they never sent. If a practitioner mistakenly provides username and password information to the thief, the thief often harvests the practitioner's contact list, stealing names and email addresses of colleagues and clients and enabling the crooks to expand their spear-phishing scam.

‘Phishing’ scams

Always be alert to phishing scams, even if the emails appear to come from a colleague or client. If the language sounds a bit off or if the request seems unusual, contact the “sender” by phone to verify rather than opening a link or attachment.

Finally, there are several signs that office computer systems may be under attack or may be under remote control. An example is when a computer cursor moves even though no computer user is present. The Security Summit is aware of many examples in which cybercriminals gained access to practitioners’ office computers, completed the pending U.S. Form 1040s, changed electronic deposit information to their own accounts, and then e-filed the returns – all performed remotely.

Tax professionals who notice any signs of identity theft should contact their state’s IRS Stakeholder Liaison immediately. The process for reporting data theft to the IRS is outlined in Data Theft Information for Tax Professionals.

In some states, data thefts must be reported to various authorities. Under the Rhode Island Identity Theft Protection Act of 2015, those who store, collect, process, maintain, acquire, use, own, or license personal information about a Rhode Island resident must implement and maintain a risk-based information security program that contains reasonable security procedures and practices appropriate to the size and scope of the organization.

About the Security Summit

The Security Summit consists of the IRS, state tax agencies, and the tax community -- including tax preparation firms, software developers, payroll and tax financial product processors, tax professional organizations and financial institutions.

Partners in the Security Summit work together as a coalition to combat identity theft to protect the nation’s taxpayers.

The Rhode Island law spells out notification and related measures that must be taken if personal information is disclosed or a security breach occurs that poses a significant risk of identity theft to any Rhode Island resident. Penalties apply for violation. (See Rhode Island General Laws Chapter 11-49.3.)

The Security Summit reminds all professional tax preparers to have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. They can also get help with security recommendations by reviewing IRS Publication 4557 (“Safeguarding Taxpayer Data”); “Safeguarding Taxpayer Data, and Small Business Information Security: the Fundamentals” by the National Institute of Standards and Technology; and IRS Publication 5293 (“Data Security Resource Guide for Tax Professionals”), which provides a compilation of data theft information available on IRS.gov.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance of the State House. It is open to the public 8:30 a.m. to 3:30 p.m. business days. To learn more, see the Division's website: www.tax.ri.gov.