Rhode Island Department of Revenue
Division of Taxation

ADV 2019-18
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
AUGUST 6, 2019

Tips for tax professionals on how to spot signs of client data theft

Security Summit partners warn that data theft can result in filing of fraudulent tax returns

PROVIDENCE — The Rhode Island Division of Taxation, the Internal Revenue Service, and other Security Summit partners today urged tax professionals to learn the tell-tale signs that their office may have experienced a data theft that resulted in fraudulent tax returns being filed in their clients' names.

The Security Summit warned practitioners that global criminal syndicates remain active – and they are well-financed, highly skilled, and tax-savvy in their attempts to gain sensitive tax data.

"Learning the signs of identity theft is critical for anyone handling taxpayer data," said IRS Commissioner Chuck Rettig. "It can be as subtle as an unusually slow computer system or as obvious as multiple clients unexpectedly receiving the same IRS notice. Paying attention to these details is critical, and fast action alerting the IRS and calling in a security expert can help protect taxpayers and your business," he said.

Recognizing the signs of data theft is the fourth item on the Security Summit's "Taxes-Security-Together" checklist. Previous checklist items include: deploying the "Security Six" basic steps, creating a written data security plan, and educating yourself on email phishing scams.

Although the Security Summit -- a partnership between state tax agencies, the IRS, and the private-sector tax community started in 2015 -- is making major progress against tax-related identity theft, cybercriminals continue to quickly evolve, and data thefts at tax professionals' offices remain a major attack point, said Rhode Island Tax Administrator Neena Savage. Thieves use stolen data from tax practitioners to create fraudulent returns that are harder for Summit partners to detect, she said.

Recognize the signs of client data theft

The Security Summit partners have created a list of warning signs that a tax professional, or the tax professional's office, may have experienced a data theft:

- Client e-filed returns begin to be rejected by the IRS or state tax agencies because returns with their 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 to confirm their identity for a submitted tax return;
- 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. Another variation: 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 responding to emails that the firm did not send;
- Network computers running slower than normal;
- Computer cursors moving or changing numbers without touching the keyboard; and
- Network computers locking out employees.

"Tax professionals should be on the lookout for these scary scenarios that have hit firms across the country, jeopardizing data of the company and their clients," Rettig said.

Because IRS and state tax 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.

Identity thieves sometimes try to leverage the stolen data by using taxpayer information to access the IRS 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.

During the tax filing season, tax professionals should make a weekly review of returns filed with the office's Electronic Filing Identification Number, or EFIN. A report is updated weekly. 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 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.

Watch out for phishing

Tax professionals who fall victim to spear phishing email scams, a common way cybercriminals access office computer, 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 use the tax firm to expand their spear phishing scam.

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, such as the cursor moving with no one at the keyboard. The IRS is aware of many

examples in which cybercriminals gained access to practitioners' office computers, completed the pending Form 1040s, changed electronic deposit information to their own accounts, and then e-filed the returns – all performed remotely.

For information on where to report data thefts, click here.

About the Security Summit

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

Partners in the Security Summit work together to combat identity theft and fight other scams to protect the nation's taxpayers.

Additional Resources

ADDITIONAL RESOURCES: The Security Summit reminds all tax professionals that they must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. Get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data (PDF), and Small Business Information Security: the Fundamentals (PDF) by the National Institute of Standards and Technology

.

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, and is open to the public 8:30 a.m. to 3:30 p.m. business days. To learn more, see the agency's website: www.tax.ri.gov.