ADV 2018-27
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 10, 2018

Security Summit launches new awareness campaign

Partners urge tax professionals to step up protections for client data

PROVIDENCE, R.I. – The Internal Revenue Service, the Rhode Island Division of Taxation, and other partners in the Security Summit today kicked off a summertime security awareness campaign for tax professionals with a new, expanded guide that provides critical steps to protect client data and highlights available resources.

The new effort by the IRS, state tax agencies, and the nation's private-sector tax industry follows continued security threats to tax and financial data held by tax professionals. Data thefts at tax practitioners' offices continue to rise and result in fraudulent tax returns that can be especially difficult for the IRS and states to detect.

The IRS, the Rhode Island Division of Taxation, and other partners in the Security Summit urge all tax professionals to take stronger security steps to protect themselves and their clients. "With the help of the Summit partnership, major progress has been made protecting taxpayers in the battle against tax-related identity theft. But the threat remains, and we need the help of tax professionals to take basic steps to safeguard their systems and taxpayer data," said Rhode Island Tax Administrator Neena S. Savage.

Help to combat fraud

Today's announcement represents the first in a series called "Protect Your Clients; Protect Yourself: Tax Security 101." The Security Summit awareness campaign is intended to provide tax professionals with the basic information they need to better protect taxpayer data and to help prevent the filing of fraudulent tax returns.

This series builds and expands upon earlier Security Summit awareness campaigns aimed at tax professionals and taxpayers. In addition, this campaign follows recommendations made by the Electronic Tax Administration Advisory Committee in June, which noted that tax professionals "are at increasing risk" of security vulnerability.

Although the Security Summit effort 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 taxpayer data to create fraudulent returns that are harder to detect. Identity thieves are technically sophisticated, helped by well-funded and tax-savvy criminal syndicates based here and abroad.

To mark the start of this awareness campaign, the IRS revised Publication 4557, "Safeguarding Taxpayer Data", to better reflect the current threats to tax professionals. The guide outlines basic steps that tax professionals should take, and how to take them.

Helping tax professionals

The guide also provides details on how to comply with requirements for a data security plan. The IRS also created a new product, Publication 5293, "Data Security Resource Guide for Tax Professionals", which highlights a compilation of IRS.gov resources for tax preparers.

The IRS reminds professional tax preparers that the Financial Services Modernization Act of 1999, also known as Gramm-Leach-Bliley Act, requires certain financial entities – including professional tax return preparers – to create and maintain a security plan for the protection of client data. The Federal Trade Commission administers this law and its "Safeguards Rule" regulations.

Both Publication 4557 and Publication 5293 promote the basic security steps endorsed by the Security Summit partners for tax professionals. These include the following:

- Learn to recognize phishing emails, especially those pretending to be from the IRS, a tax software provider, cloud storage provider, or a state tax agency. Never open a link or any attachment from a suspicious email. Remember: Neither the IRS nor the Rhode Island Division of Taxation initiates initial contact with a tax professional via email.
- Create a data security plan using IRS Publication 4557, "Safeguarding Taxpayer Data, and Small Business Information Security – The Fundamentals", by the National Institute of Standards and Technology.
- Review internal controls for their business:
    - Install anti-malware/anti-virus security software on all devices (laptops, desktops, routers, tablets, and phones) and keep software set to automatically update.
    - Create passwords of at least eight characters; longer is better. Use different passwords for each account, use special and alphanumeric characters, use phrases, password protect wireless devices, and consider a password manager program.
    - Encrypt all sensitive files/emails and use strong password protections.
    - Back up sensitive data to a safe and secure external source not connected full-time to a network.
    - Wipe clean or destroy old computer hard drives and printers that contain sensitive data.
    - Limit access to taxpayer data to individuals who need to know.
    - Check IRS e-Services account weekly for number of returns filed with EFIN.
- Report any data theft or data loss to the appropriate IRS Stakeholder Liaison.
- Stay connected to the IRS through subscriptions to e-News for Tax Professionals, Quick Alert and Social Media.

The importance of these basic steps was highlighted yet again this year when a sophisticated cybercriminal gang breached numerous practitioner offices by gaining remote control access of

computers and stealing taxpayers' 2016 tax information. The thieves used that information to file 2017 tax returns using all the taxpayer real data, including their bank accounts for direct deposit.

The thieves then called the taxpayers, trying to trick them into returning the fraudulent refunds. In some cases, the thieves had stolen so much information, they could access the clients' bank accounts online and steal the fraudulent refunds. In many cases, the tax pros never even knew their client data was stolen.

By taking the steps outlined here and in Publication 4557 , tax professionals can help prevent the common tactics used by cybercriminals. But even with the strongest security measures, the key to good security is an individual trained and alert to potential risks and threats.

Additional Resources:

- Identity Protection: Prevention, Detection and Victim Assistance
- Protect Your Clients, Protect Yourself – main
- Protect Your Clients, Protect Yourself: Tax Security 101 – 2018 awareness campaign
- Don't Take the Bait – 2017 awareness campaign
- Security Summit

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.