ADV 2018-35
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
AUGUST 21, 2018

Tax professionals urged to boost security education for employees

Goal is to better protect taxpayer data, thereby helping to prevent fraudulent tax return filings

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit urge tax professionals to step up security education for all office employees to better protect taxpayer data and help prevent fraudulent return filings.

There has been an increase this year in reports of data thefts from tax professionals. The Security Summit partners remind tax professionals that their clients' data and their businesses are only as secure as their least-informed employee.

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

The IRS continues to see an increase in the number of data thefts reported by tax professionals. Through August 9, 2018, there have been 217 tax professionals reporting data thefts, compared with 167 for the corresponding period in 2017, an increase of 30 percent.

All employees should be aware of the dangers related to phishing emails, especially spear-phishing emails. An employee does not have to be a tax preparer to accidentally disclose critical password information or download malware that could infect and impact all office computers and risk the theft of client data.

'Safeguards Rule'

All professional tax return preparers must adhere to the "Safeguards Rule" set out by the Gramm-Leach-Bliley Act of 1999 and administered by the Federal Trade Commission (FTC).

The FTC sets out a series of suggested areas to address, including for employee management and training. The FTC suggests following this list, and the Security Summit has added some updates specifically for tax professionals:

- Check references or conduct background checks before hiring employees who will have access to customer information.
- Ask every new employee to sign an agreement to follow the company's confidentiality and security standards for handling customer information.

- Limit access to customer information to employees who have a business reason to see it. For example, give employees who respond to customer inquiries access to customer files, but only to the extent they need it to do their jobs.
- Control access to sensitive information by requiring employees to use "strong" passwords that must be changed on a regular basis. (Tough-to-crack passwords require the use of at least six characters, upper- and lower-case letters, and a combination of letters, numbers and symbols.)
- Use password-activated screen savers to lock employee computers after a period of inactivity.
- Develop policies for appropriate use and protection of laptops, personal digital assistants, and cell phones or other mobile devices. For example, make sure employees store these devices in a secure place when not in use. Also, consider that customer information in encrypted files will be better protected in case of theft of such a device.
- Train employees to take basic steps to maintain the security, confidentiality, and integrity of customer information, including:
    - Locking rooms and file cabinets where records are kept;
    - Not sharing or openly posting employee passwords in work areas;
    - Encrypting sensitive customer information when it is transmitted electronically via public networks;
    - Referring calls or other requests for customer information to designated individuals who have been trained in how the company safeguards personal data; and
    - Reporting suspicious attempts to obtain customer information to designated personnel.
- Regularly remind all employees of the company's policy — and the legal requirement — to keep customer information secure and confidential. For example, consider posting reminders about their responsibility for security in areas where customer information is stored, like file rooms.
- Develop policies for employees who telecommute. For example, consider whether or how employees should be allowed to keep or access customer data at home. Also, require employees who use personal computers to store or access customer data to use protections against viruses, spyware, and other unauthorized intrusions.
- Impose disciplinary measures for security policy violations.
- Prevent terminated employees from accessing customer information by immediately deactivating their passwords and user names and taking other appropriate measures.

All employees within a tax professional's office should familiarize themselves with FTC regulations and IRS publications and websites that will help increase security awareness.

About this announcement

This is the seventh 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.

To improve data security awareness by all tax professionals, the IRS will host a webinar on September 26, 2018. The focus will be on the same topics as this series: “Protect Your Clients; Protect Yourself: Tax Security 101.” (The IRS will issue details about the webinar.)

The Security Summit reminds all professional tax preparers that they must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. They can get help with security recommendations by reviewing the recently revised IRS Publication 4557, “Safeguarding Taxpayer Data”, and “Small Business Information Security: the Fundamentals” by the National Institute of Standards and Technology.

IRS Publication 5293, “Data Security Resource Guide for Tax Professionals”, 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.