Rhode Island Department of Revenue
Division of Taxation

ADV 2018-36
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
AUGUST 28, 2018

Tax professionals have obligation to protect client data

Security Summit issues reminder about safeguard regulations for return preparers

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 aware of their obligations to protect client data.

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.

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley Act, gives the Federal Trade Commission authority to set information safeguard regulations for various entities, including professional tax return preparers.

According to the FTC Safeguards Rule, tax return preparers must create and enact security plans to protect client data. Failure to do so may result in an FTC investigation. The IRS also may treat a violation of the FTC Safeguards Rule as a violation of IRS Revenue Procedure 2007-40, which sets the rules for tax professionals participating as Authorized IRS e-File Providers.

Members of the IRS Electronic Tax Administration Advisory Committee in June noted that they believe "far fewer than half of tax professionals are aware of their responsibilities under the FTC Safeguards rule and that even fewer professionals . . . have implemented required security practices."

FTC requirements

The FTC-required information security plan must be appropriate to the company's size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles. According to the FTC, each company, as part of its plan, must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation, and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program and regularly monitor and test it;

- select service providers that can maintain appropriate safeguards, make sure the contract requires them to maintain safeguards, and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The FTC says the requirements are designed to be flexible so that companies can implement safeguards appropriate to their own circumstances. The Safeguards Rule requires companies to assess and address the risks to customer information in all areas of their operations.

IRS Publication 4557 ("Safeguarding Taxpayer Data") details critical security measures that all tax professionals should enact. The publication also includes information on how to comply with the FTC Safeguards Rule, including a checklist of items for a prospective data security plan.

Many state laws govern or relate to the privacy and security of financial data, which includes taxpayer data. They extend rights and remedies to consumers by requiring individuals and businesses that offer financial services to safeguard nonpublic personal information.

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 this announcement

This is the eighth 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 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 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.