ADV 2019-16
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 24, 2019

Security Summit reminds tax preparers about data-security law

Preparers must create and enact written plan to protect client data

PROVIDENCE — The Internal Revenue Service, the Rhode Island Division of Taxation, and other members of the Security Summit remind all professional tax preparers that they are required by federal law to create and implement a written information security plan to protect their clients' data.

"Protecting taxpayer data is not only a good business practice, it's the law for professional tax preparers," said IRS Commissioner Chuck Rettig. "Creating and putting into action a written data security plan is critical to protecting your clients and protecting your business."

The reminder is part of a broader campaign by the Security Summit to urge tax professionals to take time this summer to review their data security protections.

Although the Security Summit -- a partnership between the IRS, the Rhode Island Division of Taxation, other state tax agencies, and the private-sector tax community -- is making major progress against tax-related identity theft, cybercriminals continue to evolve, and data thefts at tax professionals' offices remain a major threat.

"Thieves use stolen data from tax practitioners to create fraudulent returns that can be harder for the IRS and Summit partners to detect," said Rhode Island Tax Administrator Neena Savage.

Create a data security plan under federal law

The Security Summit partners noted that many in the tax professional community do not realize they are required under federal law to have a data security plan.

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley (GLB) 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.

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, and 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.

> ➢ *Please note: The FTC currently is re-evaluating the Safeguards Rule and has proposed new regulations. Be alert to any changes in the Safeguards Rule and its effect on the tax preparation community.*

IRS Publication 4557, Safeguarding Taxpayer Data (PDF), 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. Tax professionals are asked to focus on key areas such as employee management and training; information systems; and detecting and managing system failures.

Additional data protection provisions may apply

The IRS and certain Internal Revenue Code (IRC) sections also focus on protection of taxpayer information and requirements of tax professionals. Here are a few examples:

- **IRS Publication 3112** - IRS e-File Application and Participation, states: Safeguarding of IRS e-file from fraud and abuse is the shared responsibility of the IRS and Authorized IRS e-file Providers. Providers must be diligent in recognizing fraud and abuse, reporting it to the IRS, and preventing it when possible. Providers must also cooperate with the IRS' investigations by making available to the IRS upon request information and documents related to returns with potential fraud or abuse.
- **IRC, Section 7216** - This IRS code provision imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses information furnished to them in connection with the preparation of an income tax return.
- **IRC, Section 6713** - This code provision imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.
- **IRS Revenue Procedure 2007-40** - This legal guidance requires authorized IRS e-file providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that violations of the GLB Act and the implementing rules and regulations put into effect by the FTC, as well as violations of non-disclosure rules addressed in IRC sections 6713 and 7216, are considered violations

of Revenue Procedure 2007-40. These violations are subject to penalties or sanctions specified in the Revenue Procedure.

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. For more information on state laws that businesses must follow, consult state laws and regulations.

Where to report data theft for the IRS, states

To notify the IRS in case of data theft, contact the appropriate local IRS Stakeholder Liaison. In Rhode Island:

- Contact the Rhode Island Attorney General's Consumer Protection Division at (401) 274-4400 to alert them that a data breach occurred.
- Contact your local police department to file a police report on the data breach. Keep a copy of the report as proof of the crime.
- Notify the individuals affected that their personal information has been compromised in the most expedient time possible, but no later than 45 calendar days after confirmation of the breach. For state notification requirements, see Rhode Island General Laws § 11-49.3. Also, see www.riag.state.ri.us/ConsumerProtection/About.php.
- Tell people what steps they can take, given the type of information exposed, and provide relevant contact information to them (www.IdentityTheft.gov). For a model notification letter, refer to page 10 of The Federal Trade Commission's Publication, "Data Breach Response: A Guide for Business."
- Contact your insurance company to report the breach and to check if your insurance policy covers data breach mitigation expenses.
- Contact your attorney with any questions or concerns you may have.
- Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to other states.

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

Tax professionals also can 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. Publication 5293, Data Security Resource Guide for Tax Professionals (PDF), 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, 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.