Rhode Island Department of Revenue
Division of Taxation

ADV 2019-19
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
AUGUST 21, 2019

Tax professionals urged to create data theft recovery plan

Security Summit says having plan in place can save valuable time and protect clients

PROVIDENCE — Rather than wait for an emergency, tax professionals should consider creating a data theft recovery plan in advance, the Security Summit recommends. Having an action plan can save valuable time and protect your clients and yourself.

The IRS, the Rhode Island Division of Taxation, tax agencies in other states, and the private-sector tax industry are calling on all tax professionals to pause this summer to review their security measures and make appropriate changes. Acting as the Security Summit, the partners created a special "Taxes-Security-Together" checklist to help tax professionals with this review.

"Our objective is to get every tax professional to stop and think about client data security. The 'Taxes-Security-Together' checklist is intended as a starting point, spelling out the basic steps necessary to start a security review," said Chuck Rettig, IRS Commissioner. Practitioners are the first line of defense against organized criminal syndicates running these identity theft scams. Despite our progress, this is no time to let down our guard in the tax community. We need your help," Rettig said.

Should a tax professional experience a data compromise – whether by cybercriminals, theft, or just an accident – there are certain basic steps to take, said Rhode Island Tax Administrator Neena Savage.

Contacting the IRS and federal law enforcement:

- Internal Revenue Service. Report client data theft to local IRS Stakeholder Liaisons, who will notify IRS Criminal Investigation and others within the agency on the tax professional's behalf. Speed is critical. If notified promptly, the IRS can help stop fraudulent tax returns from being filed in clients' names, thereby avoiding refund delays and other problems for the affected tax professional. But this action requires the cooperation of the tax professional with the IRS.
- Federal Bureau of Investigation, local office (if directed).
- Secret Service, local office (if directed).

Contacting Rhode Island officials

- 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. Notify them as quickly as possible, but no later than 45 calendar days after confirmation of the breach. For Rhode Island state notification requirements, see Rhode Island General Laws § 11-49.3 and http://www.riag.ri.gov/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 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.
- Remember: Any breach of personal information could have an effect on the victim's tax accounts with the state revenue agencies as well as the IRS. Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to other states.

Contacting experts:

- Security expert. They can help determine the cause and scope of the breach as well as stop the breach and prevent further breaches from occurring.
- Insurance company. Not only to report the breach, but to check if the insurance policy covers data breach mitigation expenses.

Contacting clients and other services:

- Federal Trade Commission for guidance for businesses. For more individualized guidance, contact the FTC at idt-brt@ftc.gov.
- Credit / identity theft protection agency. Certain states require offering credit monitoring and identity theft protection to victims of identity theft.
- Credit bureaus. Notify them if there is a compromise – and let them know that your clients may seek their services.
- Clients. At a minimum, send an individual letter to all victims to inform them of the breach but work with law enforcement on timing. Clients should complete IRS Form 14039, Identity Theft Affidavit, but only if their e-filed return is rejected because of a duplicate Social Security number or they are instructed to do so.
- Remember: IRS toll-free assisters cannot accept third-party notification of tax-related identity theft. Again, preparers should use their local IRS Stakeholder Liaison to report data loss.

The objective of the "Taxes-Security-Together" checklist is to ensure that all tax professionals, whether in a one-person shop or a major firm, understand the risk posed by national and international criminal syndicates, take the appropriate steps to protect their clients and business, and understand the laws around their obligation to secure that data.

"The number of tax professionals reporting data thefts to the IRS remains too high, and it puts tens of thousands of taxpayers at risk for identity theft," Rettig said. "We hope tax professionals will use the Summit checklist as a starting point, not an end point, to protect their client's data — and themselves. It's not only a good business practice, it's the law."

Reporting schemes helps everyone

The IRS, the states, and the tax industry share information about scams and schemes through their Identity Theft Tax Refund Fraud Information Sharing and Analysis Center, which allows the partners to rapidly respond to emerging threats. When tax professionals report data thefts to the IRS, it enables the partners to identify new schemes.

The ability to share information about emerging threats is critical to the ability to combat identity theft and refund fraud. Thieves are constantly creating new scams to trick tax professionals and taxpayers into divulging sensitive information.

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

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.

Publication 5293, Data Security Resource Guide for Tax Professionals (PDF), provides a compilation of data theft information available on IRS.gov.

Reminder: The Taxes-Security-Together Checklist

During this special Security Summit series, the checklist highlighted the following key areas:

- Deploy "Security Six" basic safeguards
- Create data security plan
- Educate yourself on phishing scams
- Recognize the signs of client data theft
- Create a data theft recovery plan (this is today's installment of the series)

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.