Rhode Island Department of Revenue
Division of Taxation

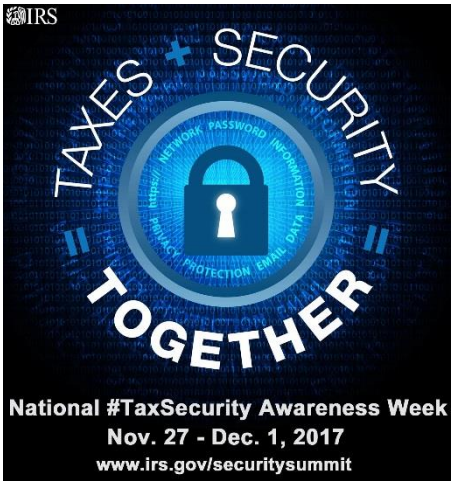
ADV 2017-42
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
NOVEMBER 29, 2017

Steps to take after a data breach

Tips for taxpayers and tax professionals from the Security Summit

PROVIDENCE, R.I. – The number of data breaches was already on a record pace for 2017 before the reported theft of nearly 145 million Americans' names, addresses, and Social Security numbers brought the issue to the forefront.



Every day, data thefts large and small put people's personal and financial information at risk.

Fortunately, there are steps that data theft victims may take to protect their financial accounts and their identities once cybercriminals have their names and other sensitive information.

The Rhode Island Division of Taxation, the Internal Revenue Service, and the tax community – partners in the Security Summit – are marking "National Tax Security Awareness Week" with a series of reminders to taxpayers and tax professionals.

In today's installment, the topic is data breaches.

DATA BREACHES

In the first half of 2017, the number of data breaches increased by 29 percent, to a record 791 incidents, according to Identity Theft Resource Center (ITRC) and CyberScout, which sponsored the report. For the past five years, ITRC has tracked data breaches in five key sectors.

Generally, thieves want to take advantage of the stolen data as quickly as possible. That may mean selling the data on the Dark Web for use by other criminals. It may mean the crook tries to access financial accounts for withdrawals or credit cards for charges. It may also mean a thief quickly files a fraudulent tax return in victims' names for a refund.

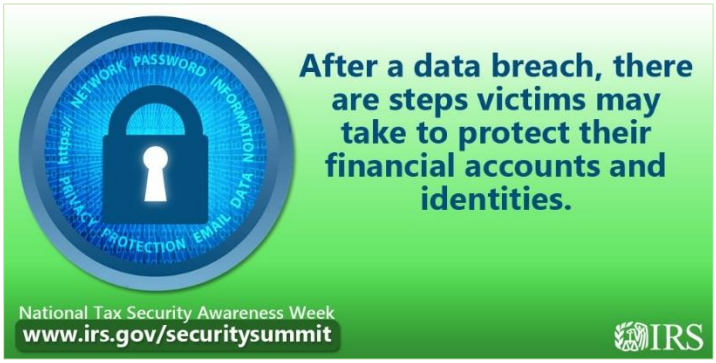
THOSE WHO ARE VICTIMS SHOULD CONSIDER THESE STEPS:

- If possible, learn what information was compromised. Was it emails and passwords, or more sensitive data, such as names and Social Security numbers?

- Take advantage of any credit monitoring offers made by the company that was breached.

- Place a freeze on credit accounts to prevent access to credit records. There may be a fee for requesting one. This varies by state. At a minimum, place a fraud alert on credit accounts by contacting one of the three major credit bureaus. A fraud alert on credit records is not as secure as a freeze, but a fraud alert is free.

- Reset passwords on online accounts, especially financial, email, and social media accounts. Experts recommend at least 10-digit passwords, mixing letters, numbers and special characters. Use different passwords for each account. Use a password manager, if necessary.



- Use two-factor authentication wherever it is offered on financial, email, and social media accounts. Two-factor authentication requires entry of a username and password and then a security code, generally sent via text to a mobile phone you've pre-registered.

The scale of a major credit bureau's breach, which was reported this summer, has prompted many questions, especially about how a victim's taxes may be affected. Because of the work by the Security Summit, more protections are in place to protect taxpayers from tax-related identity theft. Thieves will need more than a name, address, birth data, and Social Security number to file a fraudulent tax return.

TIPS FOR THE 2018 TAX SEASON; WILL FILING EARLY HELP?

The Security Summit reminds taxpayers that they should file their tax return as early as they can, but not before they are sure they have all the proper information and supporting Forms W-2 and 1099. Taxpayers should always file an accurate tax return. Filing before all information is received puts taxpayers at risk of needing to file an amended tax return, paying interest or penalties, or even receiving a notice or audit.

The IRS and states have put many new defenses in place to help protect taxpayers from identity theft. The new protections have worked well to protect taxpayers, and some key indicators of identity theft on tax returns have dropped by around two-thirds since 2015.

These protections are especially helpful if criminals only have names, addresses, and SSNs – which was the information stolen in recent incidents. However, there are continuing concerns that cybercriminals will try to build on this basic information by trying to obtain more specific financial details from taxpayers and tax professionals to help the criminals file fraudulent tax returns.

In addition, no one yet knows what thieves may do with information from the data breaches. The Summit partners believe cybercriminals will increasingly look to steal more detailed information from taxpayers, tax professionals, and businesses to help file a fraudulent tax return. The volume of victims means everyone – the tax agencies, tax professionals, and taxpayers – must be vigilant going into the 2018 tax filing season and be alert to any unusual activity.

HERE ARE A FEW SIGNS OF TAX-RELATED IDENTITY THEFT:

- An electronically filed tax return rejects because a return with the taxpayer's SSN already has been filed;
- Taxpayers receive a letter from the IRS or from a state tax agency asking them to confirm whether they submitted a tax return being held for review;
- Taxpayers receive a notice from the IRS or a state tax agency indicating that they owe additional tax, have a refund offset, or have a collection action for a year in which they did not file a tax return; and/or
- Taxpayers receive a notice from the IRS or a state tax agency that they received wages from an employer for whom the taxpayer did not work.

Taxpayers should file a Form 14039, Identity Theft Affidavit, only if their return rejects because a return using their SSN already has been filed or if told to do so by the IRS. This form is how a taxpayer reports that he or she is an identity-theft victim.

The IRS stops the vast majority of fraudulent returns. Each year, the IRS stops returns it deems suspicious and asks the filer to verify whether they filed the return. The IRS will send a notice asking taxpayers to confirm whether they filed the return.

The IRS, state tax agencies, and the tax industry are working together to fight against tax-related identity theft and to protect taxpayers. Everyone can help. Visit the "Taxes. Security. Together." awareness campaign or review IRS Publication 4524, Security Awareness for Taxpayers, to learn more.

The Rhode Island Division of Taxation office is at One Capitol Hill in Providence, R.I., diagonally across from the Smith Street entrance to 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, or call (401) 574-8829.