Rhode Island Department of Revenue
Division of Taxation

ADV 2017-22
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
JULY 25, 2017

Security Summit warns that businesses, partnerships are targets

Criminal syndicates are using stolen data to file fraudulent tax returns for refunds

PROVIDENCE, R.I. – The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit warned today that businesses, partnerships, and estate and trust filers are being targeted by national and international criminal syndicates who use stolen data to file fraudulent tax returns for refunds.

In the past year, the IRS has noted a sharp increase in the number of fraudulent Forms 1120, 1120S, and 1041, as well as Schedule K-1. Identity thieves are displaying a sophisticated knowledge of the tax code and of industry-filing practices as they attempt to obtain valuable data to help file fraudulent returns.

The IRS, state tax agencies, and the tax industry, acting as the Security Summit, are expanding their efforts to better protect these filers and to better identity suspected identity theft returns.

Recognizing signs of identity theft

As with fraudulent individual returns, there are certain signs that may indicate identity theft. Business, partnership, and estate and trust filers should be alert to potential identity theft and contact the IRS if they experience any of these issues:

- Extension-to-file requests are rejected because a return with the Employer Identification Number or Social Security Number is already on file;
- An e-filed return is rejected because a duplicate EIN/SSN is already on file with the IRS;
- An unexpected receipt of a tax transcript or IRS notice that doesn't correspond to anything submitted by the filer; and/or
- Failure to receive expected and routine correspondence from the IRS because the thief has changed the address.

Security Summit actions to protect filers

The IRS for several years has taken certain steps to help protect the Form 1120-series filers, and the Security Summit effort is part of that. For the 2017 filing season, tax software products for the first time shared more than 30 data elements with the IRS and with state tax agencies. These data points assist the IRS and states in identifying suspicious returns.

For 2018, the data elements will increase, enhancing the ability of the IRS and states not only to identify suspicious returns, but also to reduce "false positives." This will allow legitimate returns to be processed as usual.

Also for 2018, the IRS will ask those tax professionals preparing business-related returns to step up their "know your customer" procedures. Tax preparation software for business-related returns will ask the following questions:

> The Rhode Island Division of Taxation, the Internal Revenue Service, tax agencies from other states, and the tax industry are working together as the Security Summit, implementing a series of initiatives to help guard against refund fraud and tax-related identity theft.

- The name and SSN of the company executive authorized to sign the corporate tax return. Is this person authorized to sign the return?
- Payment history – Were estimated tax payments made? If yes, when were they made, how were they made, and how much was paid?
- Parent company information – Is there a parent company? If yes, who?
- Additional information based on deductions claimed.
- Filing history – Has the business filed Form(s) 940, 941, or other business-related tax forms?

These questions also will help identify suspicious returns.

Recent identity theft schemes

Criminals have long used stolen business EINs to perpetrate tax fraud by creating false Forms W-2 or 1099s or to fraudulently claim certain benefits, such as fuel tax credits. However, in the past couple of years, there has been an upswing in the filing of fraudulent Forms 1120 and 1120S.

National and international criminal syndicates are increasingly sophisticated, well-funded, and technologically adept as well as tax savvy. These well-organized gangs are increasingly targeting tax professionals to steal client data, which is one of many reasons for the increase in business-related returns fraud.

The criminals steal business return data to submit fraudulent corporate returns, such as Forms 1120 and 1120S, or fraudulent information documents, such as W-2s and 1099s, to support fraudulent individual return filings.

If the compromised business-return data included Schedule K-1 links, the criminals also will also use the K-1 shareholder's information to file fraudulent individual returns.

Estates and trusts

The Security Summit also called attention today to an increase in fraudulent trust and estate return filings. These identity theft filings involve both existing trusts and estates and bogus trusts and estates that were established using stolen individual taxpayer information.

As with identity theft filings for individuals, the goal of the perpetrators is to obtain a fraudulent refund through the filing of a Form 1041. The Security Summit reminds businesses, individuals, and tax professional to protect their computers and data to protect against identity theft and refund fraud. More information is available on IRS.gov

"It's especially difficult to identify any tax return as fraudulent when criminals are using information stolen from tax preparers," said IRS Commissioner John Koskinen. "The stolen data allows criminals to better impersonate the legitimate taxpayers." So far for 2017, the IRS has identified approximately 10,000 business returns as potential identity theft through June 1, compared to about 4,000 for calendar year 2016 and 350 for calendar year 2015.

While the number of businesses affected was relatively low, the potential dollar amounts were significant: $137 million for 2017, $268 million for 2016 and $122 million for 2015. "We need help from the tax community to combat cybercriminals and raise security awareness," Koskinen said. "That's why we launched a campaign this summer aimed at tax professionals called Don't Take the Bait," he said.

"We want all tax professionals to be aware of the threats and to take the necessary security steps to protect their clients' most sensitive information," said Rhode Island Tax Administrator Neena Savage.

For more information:

https://www.irs.gov/uac/newsroom/information-on-identity-theft-for-business-partnerships-and-estate-and-trusts

and:

https://www.irs.gov/uac/newsroom/don-t-take-the-bait-step-3-security-summit-safeguards-help-protect-individualsrenew-focus-on-curbing-data-breaches-and-business-identity-theft

Contact Information

The Division of Taxation is located on the first floor of the Powers Building, at One Capitol Hill in Providence, diagonally across from the Smith Street entrance of the State House. The Division is typically open to the public from 8:30 a.m. to 3:30 p.m. business days. The main phone number is (401) 574-8829. (For questions about personal income tax, choose option # 3.) To see a list of phone numbers and email addresses to various sections within the agency, use the following link: http://www.tax.ri.gov/contact/. For refund status, see: https://www.ri.gov/taxation/refund/.