Rhode Island Department of Revenue
Division of Taxation

ADV 2016-28
TAX ADMINISTRATION

ADVISORY FOR TAX PROFESSIONALS
DECEMBER 8, 2016

Numerous tax scams involve identity theft and tax refund fraud

Security awareness tip from Internal Revenue Service and Rhode Island Division of Taxation

The Internal Revenue Service and the Rhode Island Division of Taxation remind taxpayers to be on the lookout for an array of evolving tax scams related to identity theft and refund fraud. Every tax season, there is an increase in schemes that target innocent taxpayers by email, by phone, and on-line.

The Internal Revenue Service, state tax agencies, and the tax industry have joined as the "Security Summit" to implement a series of initiatives to help guard against tax-related identity theft in 2017. The Security Summit partners warn tax professionals and taxpayers to be on the lookout for deceptive tax schemes.

"Whether it's during the holidays or the approach of tax season, scam artists look for ways to use tax agencies and the tax industry to trick and confuse people," IRS Commissioner John Koskinen said. "There are warning signs to these scams that people should watch out for, and there are simple steps they may take to avoid being duped into giving these criminals money, sensitive financial information, or access to computers," said Rhode Island Acting Tax Administrator Neena S. Savage.

Some of the most prevalent IRS impersonation scams include:

Requesting fake tax payments: The IRS has seen automated calls where scammers leave urgent callback requests telling taxpayers to call back to settle their "tax bill." These fake calls generally claim to be the last warning before legal action is taken. Taxpayers may also receive live calls from IRS impersonators. They may demand payments on prepaid debit cards, iTunes and other gift cards, or wire transfer. The IRS reminds taxpayers that any request to settle a tax bill using any of these payment methods is a clear indication of a scam.

"Every tax season, there is an increase in schemes that target innocent taxpayers by email, by phone and on-line."

Targeting students and parents and demanding payment for a fake "Federal Student Tax": Telephone scammers are targeting students and parents demanding payments for fictitious taxes, such as the "Federal Student Tax." If the person does not comply, the scammer becomes aggressive and threatens to report the student to the police to be arrested.

Sending a fraudulent IRS bill for tax year 2015 related to the Affordable Care Act: The IRS has received numerous reports around the country of scammers sending a fraudulent version of CP2000 notices for tax year 2015. Generally, the scam involves an email or letter that includes the fake CP2000. The fraudulent notice includes a payment request that taxpayers mail a check made out to "I.R.S." to the "Austin Processing Center" at a Post Office Box address.

Soliciting W-2 information from payroll and human resources professionals: Payroll and human resources professionals should be aware of phishing email schemes that pretend to be from company executives and request personal information on employees. The email contains the actual name of the company chief executive officer. In this scam, the "CEO" sends an email to a company payroll office employee and requests a list of employees and financial and personal information including Social Security numbers (SSN).

To reach the Rhode Island Division of Taxation, call the Division's main phone line at (401) 574-8829. The Division is normally open to the public from 8:30 a.m. to 3:30 p.m. business days, and is located at One Capitol Hill in Providence, Rhode Island, diagonally across Smith Street from the State House. To reach specific sections with the agency, by phone or email, use the following address: www.tax.ri.gov/contact/

Imitating software providers to trick tax professionals: Tax professionals may receive emails pretending to be from tax software companies. The email scheme requests the recipient download and install an important software update via a link included in the e-mail. Upon completion, tax professionals believe they have downloaded a software update when in fact they have loaded a program designed to track the tax professional's key strokes, which is a common tactic used by cyber thieves to steal login information, passwords, and other sensitive data.

"Verifying" tax return information over the phone: Scam artists call saying they have your tax return, and they just need to verify a few details to process your return. The scam tries to get you to give up personal information such as a SSN or personal financial information, including bank numbers or credit cards.

Pretending to be from the tax preparation industry: The emails are designed to trick taxpayers into thinking these are official communications from the IRS or others in the tax industry, including tax software companies. The phishing schemes can ask taxpayers about a wide range of topics. E-mails or text messages can seek information related to refunds, filing status, confirming personal information, ordering transcripts and verifying PIN information.

If you receive an unexpected call, or an unsolicited email, letter, or text message from someone claiming to be from the IRS, here are some of the tell-tale signs to help protect yourself. The IRS will never:

- Call to demand immediate payment using a specific payment method such as a prepaid debit card, gift card, or wire transfer, or initiate contact by e-mail or text message. Generally, the IRS will first mail you a bill if you owe any taxes.
- Threaten to immediately bring in local police or other law-enforcement groups to have you arrested for not paying.
- Demand that you pay taxes without giving you the opportunity to question or appeal the amount they say you owe.
- Ask for credit or debit card numbers over the phone.

If you get a suspicious phone call from someone claiming to be from the IRS and asking for money, here's what you should do:

- Do not give out any information. Hang up immediately.
- Search the web for telephone numbers that scammers leave in your voicemail asking you to call back. Some of the phone numbers may be published online and linked to criminal activity.
- Contact TIGTA to report the call. Use their "IRS Impersonation Scam Reporting" web page or call 800-366-4484.
- Report it to the Federal Trade Commission. Use the "FTC Complaint Assistant" on FTC.gov. Please add "IRS Telephone Scam" in the notes.
- If you think you might owe taxes, call the IRS directly at 800-829-1040.

If you receive an unsolicited email that appears to be from either the IRS or an organization closely linked to the IRS, such as the Electronic Federal Tax Payment System (EFTPS), report it by sending it to phishing@irs.gov.

The Security Summit partners recently announced "National Tax Security Awareness Week." As part of the Security Summit effort, the IRS, the states, and the tax community will share a variety of information throughout this week to educate taxpayers on steps they should take to protect themselves from identity theft and tax scams as well as protect their valuable financial data in advance of the upcoming filing season. To learn more about protecting your personal and financial data, see: https://www.irs.gov/individuals/taxes-security-together.