ADV 2020-57
SECURITY SUMMIT

ADVISORY FOR TAXPAYERS AND TAX PROFESSIONALS
DECEMBER 3, 2020

Security Summit urges businesses to tighten data security

Most cyberattacks are aimed at businesses with 100 or fewer employees

PROVIDENCE — The Rhode Island Division of Taxation, the Internal Revenue Service, and other partners in the Security Summit today urged businesses to be on guard as thieves try to use names and data stolen from businesses to file fraudulent tax returns.

The Security Summit partners today marked the fourth day of National Tax Security Awareness Week with a warning to businesses to enact the strongest measures possible to protect their data and systems. The IRS also is planning additional steps to help businesses combat cybercriminals trying to steal their data.

"As the IRS and our partners have strengthened our security standards, identity thieves have looked for new ways to find sources of information, and businesses need to stay alert," said IRS Commissioner Charles Rettig.

"Businesses, just like individuals, can be victims of identity theft," said Rhode Island Tax Administrator Neena Savage. "Thieves may steal enough information to file a business tax return for refund or use other scams using the company's identity."

More than 70% of cyberattacks are aimed at businesses with 100 or fewer employees. Thieves may be targeting credit card information, the business identity information, or employee identity information.

Business are encouraged to follow best practices from the Federal Trade Commission (FTC), which include the following:

- Set your security software to update automatically;
- Back up important files;
- Require strong passwords for all devices;
- Encrypt devices; and
- Use multi-factor authentication.

More information is available at the FTC's "Cybersecurity for Small Business" webpage: https://www.ftc.gov/tips-advice/business-center/small-businesses/cybersecurity.

Businesses should especially be alert to any phishing email scams that are related to the coronavirus (COVID-19) pandemic, or that are tax-related, in which thieves attempt to trick employees into opening embedded links or attachments. IRS related scams may be sent to phishing@irs.gov.

Starting Dec. 13, 2020, the IRS will begin masking sensitive information from business tax transcripts, the summary of corporate tax returns, to help prevent thieves from obtaining identifiable information that would allow them to file fake business tax returns.

Only financial entries will be fully visible. All other information will have varying masking rules. For example, only the first four letters of each first and last name – of individuals and businesses – will display. Only the last four digits of the Employer Identification Number will be visible.

The IRS also has publicly launched a business identity theft affidavit form that will allow companies to proactively report possible identity theft to the IRS when, for example, the e-filed tax return is rejected. (See: https://www.irs.gov/pub/irs-pdf/f14039b.pdf.)

Businesses should file the Form 14039-B if the business receives a:

- Rejection notice for an electronically filed return because a return already is on file for that same period;
- Notice about a tax return that the entity didn't file;
- Notice about Forms W-2 filed with the Social Security Administration that the entity didn't file; and/or
- Notice of a balance due that is not owed.

This form will enable the IRS to respond to the business much faster than in the past and work to resolve issues created by a fraudulent tax return. Businesses should not use the form if they experience a data breach but see no tax-related impact. For more information, see: https://www.irs.gov/identity-theft-central.

W-2 theft scheme

Although tax scams can come and go, all employers should remain alert to Form W-2 theft schemes. In the most common version, a thief poses as a high-ranking company executive who emails payroll employees and asks for a list of employees and their W-2s. Businesses often don't know they've been scammed until a fraudulent return shows up in employees' names.

There is a special reporting procedure for employers who experience the W-2 scam. See: https://www.irs.gov/identity-theft-central.

Finally, Security Summit partners urge businesses to keep their employer identification number (EIN) application information current. Changes of address or responsible party may be reported using the following form: https://www.irs.gov/forms-pubs/about-form-8822-b.

Reminder: Changes in the responsible party must be reported to the IRS within 60 days. Current information can help the IRS find a point of contact to resolve identity theft and other issues.

The Security Summit consists of the IRS, the Rhode Island Division of Taxation, other states' tax agencies, and the tax community -- including tax preparation firms, software developers, 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.