CPA
Practice Advisor

PRODUCT & SERVICE GUIDE

Businesses Warned of Tax ID Thieves

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.

Dec. 10, 2020

Hackers and online thieves are increasingly trying to use stolen business names and data to file fraudulent tax returns, and the IRS is warning 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. 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 include:

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

More information is available at FTC's Cybersecurity for Small Businesses.

Businesses should especially be alert to any COVID-19 or tax-related phishing email scams that 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 the Form 14039-B, Business Identity Theft Affidavit, that will allow companies to proactively report possible identity theft to the IRS when, for example, the e-filed tax return is rejected.

Businesses should file the Form 14039-B if it 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.
- 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 Identity Theft Central's Business section.

Although the 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. It also may be found at Identity Theft Central's Business section.

Finally, Security Summit partners urge businesses to keep their EIN application information current. Changes of address or responsible party may be reported using 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 IRS, state tax agencies, the private sector tax industry, including tax professionals, work in partnership as the Security Summit to help protect taxpayers from identity theft and refund fraud. This is the third in a week-long series of tips to raise awareness about identity theft. See IRS.gov/securitysummit for more details.

Product & Service Guide • Tax • News