IRS News Release

Internal Revenue Service
Media Relations Office
Washington, D.C.
Media Contact: 202.317.4000
Public Contact: 800.829.1040
www.irs.gov/newsroom

Security Summit reminder: Identity theft red flags tax pros should know

IR-2023-143, Aug. 8, 2023

WASHINGTON — In the fourth of a special series, the Internal Revenue Service and the Security Summit partners today urged tax professionals to learn the signs of data theft so they can respond quickly to protect clients.

Tax professionals have a precious commodity that identity thieves desperately want — client tax information. With stronger fraud defenses put in place by the IRS and Security Summit partners, identity thieves need this essential information to help complete their crime.

"It's important for tax professionals to protect their systems from identity thieves who always look for new methods to steal data," said IRS Commissioner Danny Werfel. "There are practical ways for practitioners to keep on top of the latest trends and signs of data and identity theft."

The IRS, state tax agencies and the nation's tax industry – working together as the Security Summit – reminded tax professionals that they should contact the IRS immediately when there's an identity theft issue while also contacting insurance or cybersecurity experts to assist them with determining the cause and extent of the loss.

This is the fourth in a five-part "Protect Your Client; Protect Yourself" summer series from the Security Summit, a public-private partnership that works to protect the tax system against tax-related identity theft and fraud.

The news release series and the IRS Nationwide Tax Forums, which begin today in the Washington, D.C., area, provide important information to help protect sensitive taxpayer data that tax professionals hold while also protecting their business from identity thieves. This marks the eighth year that the Security Summit partners have worked to raise awareness about these issues through the "Protect Your Clients; Protect Yourself" campaign.

Tax professional victims have frequently shared their concern with IRS that they did not immediately spot the signs of data theft. Here are some things that can help.

Tax pros: Know the warning signs

Tax pros should be on the lookout for these critical warning signs from their clients:

- Clients receive notice that an IRS Online Account was created without their consent or that:
  - Someone accessed their IRS Online Account without their knowledge.
  - The IRS disabled their Online Account.
- Clients receive a tax transcript they didn't request.
- Balance due or other notices from the IRS are received that are not correct based on the tax return filed.
- Clients respond to calls or emails the tax pro didn't make.
- Clients receive refunds without filing a tax return.

Tax professionals should also watch for these red flags when their business experiences:

- Slow or unexpected computer or network responsiveness such as:
  - Software or actions take longer to process than usual.
  - Computer cursor moves or changes numbers without touching the mouse or keyboard.
  - Unexpectedly being locked out of a network or computer.
- Client tax returns being rejected because their Social Security number was already used on another return.
- IRS authentication letters (5071C, 6331C, 4883C, 5747C) being received even though a tax return hasn't been filed.
- Getting more e-file receipt acknowledgements than the tax pro filed.

While these are only a few examples, tax pros should ensure they have the highest security possible and be ready to react quickly to protect themselves and their clients. To help tax pros, the Summit partners created the Written Information Security Plan or WISP is a 28-page, easy-to-understand document developed by and for tax and industry professionals to keep customer and business information safe and secure.

Report immediately

If a tax pro or their firm are the victim of data theft, they should:

- Report it to their local IRS Stakeholder Liaison. Speed is critical. IRS Stakeholder Liaisons will ensure all the appropriate IRS offices are alerted. If reported quickly, the IRS can take steps to block fraudulent returns in the clients' names and will assist tax pros through the process.

- Email the Federation of Tax Administrators at StateAlert@taxadmin.org. They will provide guidance on reporting to state tax agencies. Most states require that the state attorney general be notified of data breaches.

- Tax professionals should be pro-active with clients that could have been impacted and suggest appropriate actions, such as obtaining an IP PIN or completing a Form 14039, Identity Theft Affidavit, if applicable.

Find more information at Data Theft Information for Tax Professionals.

Additional resources

- Publication 5293, Data Security Resource Guide for Tax Professionals, provides an overview and resources about how to avoid data theft.
- Tax professionals can also get help with security recommendations by reviewing IRS Publication 4557, Safeguarding Taxpayer Data, and the IRS' Identity Theft Central pages for tax pros.
- Small Business Information Security: The Fundamentals, by the National Institute of Standards and Technology.
- Tax professionals should stay connected to the IRS through subscriptions to e-News for Tax Professionals and its social media sites.

-30-