THE TAXBOOK News
Release Date: 8/10/22

Signs of ID Theft

Cross References

- IR-2022-144, August 2, 2022

With identity thieves continuing to target the tax community, Internal Revenue Service Security Summit partners are urging tax professionals to learn the signs of data theft so they can react quickly to protect clients.

The IRS, state tax agencies and the 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.

"Tax pros must be vigilant to protect their systems from identity thieves who continue to look for ways to steal data," said IRS Commissioner Chuck Rettig. "Practitioners can take simple steps to remain on the lookout for signs of data and identity theft. It's critical for tax pros to watch out for these details and to quickly take action when tell-tale signs emerge. This can be critical to protect their business as well as their clients against identity theft."

This is the third in a summer series of five Security Summit news releases aimed at raising awareness among tax professionals about data security. The special Protect Your Client; Protect Yourself campaign is designed to help protect against tax-related identity theft by increasing attention on basic security steps that tax professionals and others should take to protect sensitive information.

One common concern the IRS hears from tax professionals is that they did not immediately recognize the signs of data theft.

Summit partners are urging tax professionals to watch out for these critical signs:

- Client e-filed returns rejected because client's Social Security Number was already used on another return.
- More e-file acknowledgements received than returns the tax pro filed.
- Clients responded to emails the tax pro didn't send.
- 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 locked out of a network or computer.

Tax professionals should also watch for warning signs when clients report they've received:

- IRS Authentication letters (5071C, 6331C, 4883C, 5747C) even though they haven't filed a return.
- A refund even though they haven't filed a return.
- A tax transcript they didn't request.
- Emails or calls from the tax pro that they didn't initiate.

- A notice that someone created an IRS online account for the taxpayer without their consent.
- A notice the taxpayer wasn't expecting that:
  - Someone accessed their IRS online account,
  - The IRS disabled their online account,
  - Balance due or other notices from the IRS that are not correct based on return filed or if a return had not been filed.

These are just a few examples. Tax pros should ensure they have the highest security possible and react quickly if they sense or see something amiss.

If the tax pro or their firm are the victim of data theft, immediately:

- **Report it to the local IRS Stakeholder Liaison.** Liaisons will notify IRS Criminal Investigation and others within the agency on the practitioner's behalf. Speed is critical. 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.** Get information on how to report victim information to the states. Most states require that the state attorney general be notified of data breaches. This notification process may involve multiple offices.
- 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.