immediately and follow an established process for helping the IRS protect their clients.

Aug. 22, 2019

Tax professionals are being advised by the IRS that they should report data theft immediately and follow an established process for helping the IRS protect their clients.

If notified promptly, the IRS can help stop fraudulent tax returns from being filed in clients' names, thereby avoiding refund delays and other problems for the affected tax professional. But this action requires the cooperation of the tax professional with the IRS.

The IRS, state tax agencies and the private-sector tax industry are calling on all tax

criminal syndicates running these identity theft scams. Despite our progress, this is no time to let down our guard in the tax community. We need your help."

Creating a data theft recovery plan is the fifth and final action item in this summer's Security Summit series. Previous checklist topics included: deploying the "Security Six" safeguards, creating a written data security plan, educating yourself on phishing scams and recognizing the signs of data theft.

Checklist Item 5: Create a data theft recovery plan

Rather than wait for an emergency, tax professionals should consider creating a data theft recovery plan in advance and make calling the IRS an immediate action item. Having an action plan can save valuable time and protect your clients and yourself. Should a tax professional experience a data compromise – whether by cybercriminals, theft or just an accident – there are certain basic steps to take. These include:

Contacting the IRS and law enforcement:

- Internal Revenue Service. Report client data theft to local IRS Stakeholder Liaisons, who will notify IRS Criminal Investigation and others within the agency on the tax professional's behalf. Speed is critical. If reported quickly, the IRS can take steps to block fraudulent returns in clients' names, helping your firm and your clients.
- Federal Bureau of Investigation, local office (if directed).
- Secret Service, local office (if directed).

Contacting states in which the tax professional prepares state returns:

- State revenue agencies. Any breach of personal information could have an effect on the victim's tax accounts with the state revenue agencies as well as the IRS. To help tax professionals find where to report data security incidents at the state level, the

Federation of Tax Administrators has created a special email address as a contact

- Insurance company. Not only to report the breach, but to check if the insurance policy covers data breach mitigation expenses.

Contacting clients and other services:

- Federal Trade Commission for guidance for businesses. For more individualized guidance, contact the FTC at idt-brt@ftc.gov.
- Credit / identity theft protection agency. Certain states require offering credit monitoring and identity theft protection to victims of identity theft.
- Credit bureaus. Notifying them if there is a compromise and your clients may seek their services.
- Clients. At a minimum, send an individual letter to all victims to inform them of the breach but work with law enforcement on timing. Clients should complete IRS Form 14039, Identity Theft Affidavit, but only if their e-filed return is rejected because of a duplicate Social Security number or they are instructed to do so.
- Remember: IRS toll-free assisters cannot accept third-party notification of tax-related identity theft. Again, preparers should use their local IRS Stakeholder Liaison to report data loss.

The objective of the "Taxes-Security-Together" Checklist is to ensure all tax professionals, whether a one-person shop or a major firm, understand the risk posed by national and international criminal syndicates, take the appropriate steps to protect their clients and business and understand the laws around their obligation to secure that data.

"The number of tax professionals reporting data thefts to the IRS remains too high, and it puts tens of thousands of taxpayers at risk for identity theft," Rettig said. "We hope tax professionals will use the Summit checklist as a starting point, not an end point, to protect their client's data — and themselves. It's not only a good business practice, it's the law."

Reporting schemes helps everyone

trick tax professionals and taxpayers into divulging sensitive information.

Additional Resources

The Security Summit reminds all tax professionals that they must have a written data security plan as required by the Federal Trade Commission and its Safeguards Rule. Get help with security recommendations by reviewing the recently revised IRS Publication 4557, Safeguarding Taxpayer Data, and Small Business Information Security: the Fundamentals by the National Institute of Standards and Technology.

Publication 5293, Data Security Resource Guide for Tax Professionals, provides a compilation of data theft information available on IRS.gov. Also, tax pros should stay connected to the IRS through subscriptions to e-News for Tax Professionals and Social Media.

Reminder: The Taxes-Security-Together Checklist

During this special Security Summit series, the checklist highlighted these key areas:

- Deploy "Security Six" basic safeguards
- Create data security plan
- Educate yourself on phishing scams
- Recognize the signs of client data theft
- Create a data theft recovery plan, and call the IRS immediately

Technology

Sponsors.