INTERNAL REVENUE SERVICE

IRS News Release

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

Tax Return Preparers: Data Thefts and Protecting Client Tax Information

FS-2015-24, October 2015

The Internal Revenue Service reminds tax return preparers that they are prime targets for identity thieves who seek data to use on fraudulent tax returns.

The IRS recommends preparers create a security plan. Publication 4557, Safeguarding Taxpayer Data, offers many helpful suggestions including a check list.

Safeguarding Taxpayer Data

As part of that security plan, the publication recommends preparers have:

- Top-notch security software that includes a firewall, anti-malware and anti-virus programs; make sure they are set to automatically update so that the software can stay current against the latest threats; consider having firewalls for both hardware and software.
- An education program for all employees to ensure they understand the dangers of phishing emails and other threats to taxpayer data. Publication 4557 has several items related to employees such as halting their access to the preparer's computer systems if they leave employment.
- Strong passwords that are changed periodically; consider having different levels of password protection. For example, have one password to access the computer system and a separate password to access tax software or client files. That way if the computer system is breached perhaps not all of the information will be exposed.
- Secure wireless connection – if Wi-Fi is used, protect taxpayer data by making sure it is password protected and encrypted email programs to exchange PII information with taxpayers.

Return preparers should also be sure to:

- Back up taxpayer data frequently, perhaps on an external hard drive and ensure that the hard-drive is kept in a secure location with limited access by others.
- Store any paper files in a secure location.
- Access IRS e-services weekly during the filing season and periodically throughout the year to see the number of returns filed using the preparer's EFIN. If the number is excessive, contact the e-Help Desk for e-Services immediately.

Federal Laws Apply

Preparers also should be aware of the federal laws that require safeguards.
In the Gramm-Leach-Bliley Act, the "Safeguards Rule" requires individuals involved in providing financial products or tax preparation services to ensure the security and confidentiality of customer records and information.

The Act's "Financial Privacy Rule" requires return preparers and others to give their customers privacy notices that explain the financial institution's information collection and sharing practices. In turn, customers have the right to limit some sharing of their information.

Section 7216 of the Internal Revenue Code (IRC) imposes criminal penalties on tax preparers who unauthorized disclosures or uses of information furnished to them in connection with the preparation of an income tax return.

IRC Section 6713 imposes monetary penalties on the unauthorized disclosures or uses of taxpayer information by any person engaged in the business of preparing or providing services in connection with the preparation of tax returns.

Develop Data Theft Plan

The IRS also recommends preparers create a data theft plan that they could enact should they experience a data loss.

The Federal Trade Commission outlines best practices for businesses that experience data theft. Its main guidance is available at "Information Compromise and the Risk of Identity Theft: Guidance for Your Business." They include notifying:

- **Law Enforcement** – If local police are not familiar with investigating information compromises, contact the local office of the FBI or the U.S. Secret Service. Also, contact local IRS Stakeholder Liaison so they can contact IRS Criminal Investigation.
- **Affected Businesses** – For example, alerting the major credit bureaus that a data theft involving Social Security Numbers has occurred and that clients will be advised to place fraud alerts on their accounts.
- **Individual Clients** – This is the hard part, but the earlier clients are notified, the faster they can take action to mitigate any damage. Also:
    - Discuss the timing with law enforcement to avoid impeding the investigation;
    - Designate a person responsible for releasing information. Communications is critical. The FTC has a model letter that can be used as a template to notify clients about the data theft.
    - Describe in any notice to clients what is known about the compromise, including how it happened, what information was taken and what actions have been taken to remedy the situation.

- Consider additional steps such as offering free credit monitoring for clients.

Contact

The IRS has updated its guidance to preparers including new procedures should they suffer a data theft. Preparers should contact the IRS Stakeholder Liaison for their state. Contact information is available on IRS.gov, keyword search Stakeholder Liaison.

—30—