

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Jul. 23, 2019



Professional tax preparers are being reminded that federal law requires them to create a written information security plan to protect their clients' data.

As such, the IRS and its Security Summit partners are urging tax professionals to take time this summer to review their data security protections. To help them in this complex area, the Summit created a special "Taxes-Security-Together" Checklist as a starting point.

"Protecting taxpayer data is not only a good business practice, it's the law for professional tax preparers," said IRS Commissioner Chuck Rettig. "Creating and putting into action a written data security plan is critical to protecting your clients and protecting your business."

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Create a data security plan under federal law

The Security Summit partners noted that many in the tax professional community do not realize they are required under federal law to have a data security plan.

The Financial Services Modernization Act of 1999, also known as the Gramm-Leach-Bliley (GLB) Act, gives the Federal Trade Commission authority to set information safeguard regulations for various entities, including professional tax return preparers. According to the FTC Safeguards Rule, tax return preparers must create and enact security plans to protect client data. Failure to do so may result in an FTC investigation. The IRS also may treat a violation of the FTC Safeguards Rule as a violation of IRS Revenue Procedure 2007-40, which sets the rules for tax professionals participating as an Authorized IRS e-file Provider.

The FTC-required information security plan must be appropriate to the company's size and complexity, the nature and scope of its activities and the sensitivity of the customer information it handles. According to the FTC, each company, as part of its plan, must:

- designate one or more employees to coordinate its information security program;
- identify and assess the risks to customer information in each relevant area of the company's operation and evaluate the effectiveness of the current safeguards for controlling these risks;
- design and implement a safeguards program and regularly monitor and test it;
- select service providers that can maintain appropriate safeguards, make sure the contract requires them to maintain safeguards and oversee their handling of customer information; and
- evaluate and adjust the program in light of relevant circumstances, including changes in the firm's business or operations, or the results of security testing and monitoring.

The FTC says the requirements are designed to be flexible so that companies can

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

that all tax professionals should enact. The publication also includes information on how to comply with the FTC Safeguards Rule, including a checklist of items for a prospective data security plan. Tax professionals are asked to focus on key areas such as employee management and training; information systems; and detecting and managing system failures.

Additional data protection provisions may apply

The IRS and certain Internal Revenue Code (IRC) sections also focus on protection of taxpayer information and requirements of tax professionals. Here are a few examples:

- **IRS Publication 3112** – IRS e-File Application and Participation, states: Safeguarding of IRS e-file from fraud and abuse is the shared responsibility of the IRS and Authorized IRS e-file Providers. Providers must be diligent in recognizing fraud and abuse, reporting it to the IRS, and preventing it when possible. Providers must also cooperate with the IRS' investigations by making available to the IRS upon request information and documents related to returns with potential fraud or abuse.
- **IRC, Section 7216** – This IRS code provision imposes criminal penalties on any person engaged in the business of preparing or providing services in connection with the preparation of tax returns who knowingly or recklessly makes unauthorized disclosures or uses information furnished to them in connection with the preparation of an income tax return.
- **IRC, Section 6713** – This code provision 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.
- **IRS Revenue Procedure 2007-40** – This legal guidance requires authorized IRS e-file providers to have security systems in place to prevent unauthorized access to taxpayer accounts and personal information by third parties. It also specifies that

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us

Where to report data theft for the IRS, states

To notify the IRS in case of data theft, contact the appropriate local IRS [Stakeholder Liaison](#).

In some states, data thefts must be reported to various authorities. Email the Federation of Tax Administrators at StateAlert@taxadmin.org to get information on how to report victim information to the states.

Tax professionals also can 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 professionals should stay connected to the IRS through subscriptions to [e-News for Tax Professionals](#) and [Social Media](#).

The Taxes-Security-Together Checklist

During this special Security Summit series, the checklist highlights these key areas for tax professionals:

- [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

Hello. It looks like you're using an ad blocker that may prevent our website from working properly. To receive the best experience possible, please make sure any blockers are switched off and refresh the page.

If you have any questions or need help you can email us