# Careful WISP(er) -- Professional Responsibility and Data Security: Practitioners' Obligation to Have a Written Information Security Plan

Internal Revenue Service (IRS) sent this bulletin at 11/14/2023 06:03 PM EST

Having trouble viewing this email? View it as a Web page.

SHARE

Alerts from Office of Professional Responsibility (OPR) November 14, 2023

## OPR Resources

Circular 230 Tax Professionals

Circular No. 230 (Rev. 6-2014)

Frequently Asked Questions

Latest News and Guidance from OPR

Disciplinary Sanctions - IRB

OPR Webinars

## Issue Number: 2023-10

## Inside This Issue

**Careful WISP(er) - Professional Responsibility and Data Security: Practitioners' Obligation to Have a Written Information Security Plan**

To fulfill their professional obligations, practitioners—attorneys, certified public accountants, enrolled agents, and tax return preparers who participate in the Internal Revenue Service's Annual Filing Season Program—must comply with Circular 230, Regulations Governing Practice before the Internal Revenue Service (31 CFR Subtitle A, Part 10), which is administered and enforced by the IRS's Office of Professional Responsibility (OPR).

Several provisions of Circular 230 implicate a practitioner's obligations when dealing with data security and confidential client information. These provisions complement not only the privacy and penalty provisions of the Internal Revenue Code—including the penalties in IRC 6713 (civil) and IRC 7216 (criminal) for unauthorized disclosure of taxpayer information—but also nontax legislation enacted in 1999 that gave the Federal Trade Commission (FTC) authority to prescribe regulations establishing requirements of data safeguarding for various businesses including professional tax return preparers. This article discusses how the FTC's implementing regulations and complementary guidance issued by the IRS affect the duties and restrictions imposed on tax practitioners by Circular 230.

**Circular 230**

Section 10.35 provides that a practitioner must possess the necessary competence to engage in practice before the IRS, and overall competence

has been construed in related contexts to encompass technological competency.[1] In addition, section 10.36 imposes an obligation on practitioners who have or share the principal authority and responsibility for a firm's tax practice to have in place "adequate procedures" to ensure compliance by its members, associates, and employees—including contractors—with Circular 230. While not framed as a mandatory requirement ("must") but as an aspirational standard ("should"), section 10.33 provides that tax advisors should adhere to "best practices" in providing advice and preparing or assisting in the preparation of a submission to the IRS, including compliance with Circular 230's standards of practice and the obligation to maintain client confidences.

**Gramm-Leach-Bliley Act and the FTC's Safeguards Rule**

Under the Financial Services Modernization Act of 1999, more commonly called the Gramm-Leach-Bliley Act, financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—must comply with the FTC's Standards for Safeguarding Customer Information (the so-called Safeguards Rule). Accountants and other firms in the business of completing income tax returns are defined as covered financial institutions in section 314.2(h)(2)(viii) of the Safeguards Rule.[2] Accordingly, they must implement safeguards, including a "written information security plan" (WISP), to protect the security, confidentiality, and integrity of information. *See* 16 C.F.R. Part 314 (2002). The Safeguards Rule also elaborates that companies covered by the rule are responsible for taking steps to ensure that their affiliates and service providers also safeguard customer information in their care.

**WISP: Practical Guidance for Safeguarding Confidential Taxpayer Information**

To protect the tax system from tax-related identity theft and fraud, in 2015, the IRS created a public-private partnership that works to safeguard confidential taxpayer information. The IRS Security Summit consists of the IRS, state tax agencies, and the commercial tax community, including tax preparation firms, software developers, payroll and tax financial product processors, tax professional organizations, and financial institutions. (Total membership is the IRS, 42 state agencies, and 20 industry organizations.). In furthering the FTC's Safeguards Rule, the Security Summit continually reminds tax professionals to establish and maintain an up-to-date Written Information Security Plan or WISP. To assist tax professionals, the Security Summit prepared a document providing guidance on creating a WISP along with a sample template, which the IRS published as Publication 5708. The 28-page, easy-to-understand document was developed by and for tax and industry professionals to keep customer and business information safe and secure. The sample template is designed to help tax professionals, especially smaller practices, make data security planning easier.

A related IRS document, *Publication 4557, Safeguarding Taxpayer Data: A Guide for Your Business*, seeks to help tax professionals understand basic security steps and how to take them, recognize the signs of data theft and how to report data theft, respond and recover from a data loss, and understand and comply with the FTC Safeguards Rule.

**Data Security Protocols**

A good WISP should identify the risks of data loss for the types of information handled by a firm or company and focus on employee management and training, information systems, and detecting and managing system failures. There is no static, "one-size-fits-all" solution to tax practitioners' data security challenges. Rather, a security plan should be scaled to the business's size, scope of activities, complexity, and the sensitivity of the customer data it handles and should be updated as business or technology changes dictate.[3] That said, as a general matter, certain protocols should be considered:

- Do not collect more "Personally Identifiable Information" (PII) of clients than is necessary for your business operations, and do not retain PII longer than necessary or legally required for business purposes.
- Protect the PII you collect, use, disclose, and retain. For example, store PII in a locked room or file cabinets (with information secured at the end of each workday).
- Restrict access to PII to only those individuals with a business need to access the information.
- Dispose of PII appropriately, such as shredding documents and wiping (or destroying) old hard drives, fax machines, printers, and other equipment.
- Use qualified and vetted contractors, including physical and data security consultants.
- Instill awareness and train employees (professional and nonprofessional alike) on properly handling PII.
- Establish security protocols for electronic programs and files, including server locks, password policies,[4] guidance on phishing / malware schemes, and laptop and mobile device security.
- Develop and enforce email policies and procedures that comply with federal and state laws.
- Continually monitor computer networks to identify and redress potential security issues (e.g., software updates, antivirus software, firewalls, security patches, scan engines).
- Establish guidelines related to Internet browsing, use of "smart" devices, and use of social media and professional networking sites.
- Maintain good records and have policies and procedures in place for what to do in case of a data breach (including timely notification of the business's insurance carrier).[5]
- If your employees work remotely, adopt policies relating to the use of —
    - virtual private networks (VPNs) to securely conduct business;
    - separate personal and business computers, mobile devices, and email accounts; and
    - "smart" devices.
- Establish security policies related to physical files and other records kept at home.

**Conclusion**

Federal law, enforced by the FTC, requires tax preparers to create and maintain a written data security plan. Having a WISP protects businesses and their clients while providing a blueprint for action in the event of a security incident. In addition, a WISP can help if other events seriously disrupt a tax professional's ability to conduct normal business, including fire, flood, tornado, earthquake, and theft.

Failure to maintain a WISP to protect private financial information may not only put clients at risk for identity theft and fraud, it may also expose a practitioner to liability for violating the Safeguards Rule and the terms of their malpractice insurance coverage. In addition, it could subject a practitioner, in circumstances of willfulness, to discipline under Circular 230. Given section 10.35's competence requirement and the obligation imposed by section 10.36 to have procedures in place to ensure compliance with Circular 230 by everyone involved in a tax practice, we encourage practitioners to pay heed to the requirement to adopt a WISP and implement appropriate data security programs.

---

[1] That section 10.35's competence standard incorporates a duty to maintain technological competence aligns with other professional standards imposed on attorneys, accountants, and enrolled agents by their professional associations. *See* American Bar Association (ABA), *Model Rule of Professional Conduct* 1.1 (Competence) (Comment 8 to the rule states, "a lawyer should keep abreast of changes in the law and practice, including the benefits and risks associated with relevant technology"); ABA *Model Rule* 1.6 (Confidentiality of Information) (Rule

1.6(c) provides that a lawyer "shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or access to, information"); ABA Formal Ethics Opinion 483 (2018) (noting the duty to notify clients of data breaches); American Institute of Certified Public Accountants (AICPA), *Code of Professional Conduct* ET 1.700.001 (Confidential Client Information Rule); AICPA *Statements on Standards for Tax Services* No. 1.3 (Data Protection) (Standard 1.3.4 provides that a CPA "should make reasonable efforts to safeguard taxpayer data, including data transmitted or stored electronically"); National Association of Enrolled Agents (NAEA) *Code of Ethics* 4 (EAs "will maintain the confidentiality of professional relationships"); and NAEA *Rules of Professional Conduct* 3 (EAs "will maintain a confidential relationship between themselves and their clients or former clients" and "will instruct employees that information acquired in their duties is confidential and will ensure that confidentiality is maintained").

[2] 16 C.F.R. 314.2(h)(viii) ("An accountant or other tax preparation service that is in the business of completing income tax returns is a financial institution because tax preparation services are a financial activity listed in 12 C.F.R. 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G)").

[3] Visit the IRS's Security Summit webpage for detailed information on safeguards to protect confidential information.

[4] Tax professionals should generally observe the following guidelines concerning passwords:

- USE STRONG PASSWORDS. Never share usernames or passwords with others. Strong passwords consist of a random sequence of upper and lower-case letters that include numbers and special characters. Ideally, passwords should be at least 14 characters long. For systems or applications that have sensitive information, use multiple forms of identity verification (multifactor or dual-factor authentication).

- CHANGE DEFAULT PASSWORD. Many devices come with default administrative passwords. Change them immediately and regularly thereafter. Default passwords are easily found or known by hackers.

- CHANGE PASSWORDS OFTEN. Every three months is recommended. Consider using a password management application to store passwords. Passwords to devices and applications that contain business information should not be reused.

[5] A good resource for understanding and adopting post-breach responsibilities is the FTC's Data Breach Response Guide.

Back to Top

---