June 9, 2025

Issue Number 2025-8. How to Be a Careful WISP(er) - Professional Responsibility and Data Security: Practitioners Should Have a Written Information Security Plan

To fulfill their professional obligations, tax practitioners – attorneys, certified public accountants, enrolled agents, enrolled retirement plan agents, and tax return preparers who participate in the Internal Revenue Service's voluntary Annual Filing Season Program – must comply with Circular 230, *Regulations Governing Practice before the Internal Revenue Service*,[1] which is administered and enforced by the IRS's Office of Professional Responsibility (OPR).

Several provisions of Circular 230 involve a practitioner's obligations when dealing with data security and confidential client information. These provisions complement the privacy and penalty provisions of the Internal Revenue Code, including the penalties in IRC 6713 (civil) and IRC 7216 (criminal) for unauthorized disclosure or use of taxpayers' tax return information, the disclosure (and use) restrictions in IRC 6103(c), and civil liability under IRC 7431. Circular 230's rules also complement non-tax legislation enacted in 1999 that gave the Federal Trade Commission (FTC) authority to prescribe regulations establishing requirements of data safeguarding for various businesses, including, notably, professional tax return preparers. This article discusses how the FTC's implementing regulations and supplemental guidance issued by the IRS affect the duties and restrictions imposed on tax practitioners by Circular 230.

Circular 230

Section 10.35 (*Competence*) 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.[2] In addition, section 10.36 (*Procedures to*

[1] Codified in Title 31 of the Code of Fed'l Regulations (CFR) Subtitle A, Part 10.

[2] The treatment of section 10.35 as incorporating 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 m the law and practice, including the benefits and risks associated with relevant technology"); ABA Model Rule 1.6 (Confidentiality of Information) (paragraph (c) provides that a lawyer "shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or access to, information"); ABA Comm. on Ethics & Pro. Resp., Formal Op. 483 (2018) (identifying 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 ("Members and Associates will maintain the confidentiality of professional relationships."); NAEA Rules of Professional Conduct 3 ("Members and Associates 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.").

ensure compliance) imposes an obligation on practitioners who have or share the principal authority and responsibility for a firm or other entity's tax practice to have "adequate procedures" in place to ensure its members, associates, and employees, as well contractors, comply with Circular 230.

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

Under the Financial Services Modernization Act of 1999 (Pub. L. No. 106-102), more commonly called the Gramm-Leach-Bliley Act, financial institutions – companies that offer consumers[3] 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).[4] Accounting 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.[5] Accordingly, they must implement safeguards, including an "information security program," to protect the security, confidentiality, and integrity of information. *See* 16 CFR 314.1, 314.4 (2024). An "information security program" means "the administrative, technical, or physical safeguards . . . use[d] to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information." 16 CFR 314.2(i).[6] The Safeguards Rule also elaborates that companies covered by the rule are responsible for taking steps to make sure that their affiliates and service providers also safeguard customer information in their care. 16 CFR 314.4(a)(1), (f); *see also* 16 CFR 314.2(r) (defining a "service provider").

WISP: Practical Guidance for Safeguarding Confidential Taxpayer Information

To protect the American 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; electronic return originators (EROs);[7] processors of payroll and tax financial products; tax professional organizations; and

---

[3] The FTC defines a "consumer" as "an individual who obtains or has obtained a financial product or service from" a financial institution "to be used primarily for personal, family, or household purposes, or that individual's legal representative," including, for example, an individual who is an applicant for an extension of credit or for a loan "for personal, family, or household purposes." 16 CFR 314.2(b)(1), (2)(i)-(ii).

[4] Title 16 CFR Part 314.

[5] Section 314.2(h)(viii) states, "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)"); *see also* 12 CFR 225.28(b)(6)(vi) (2024) ("Financial and investment advisory activities [include] . . . Providing tax-planning and tax-preparation services to any person.").

[6] A "customer" is, broadly, "a consumer who has a customer relationship" with a covered financial institution. 16 CFR 314.2(c). "Customer information means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of" a financial institution or its "affiliates." 16 CFR 314.2(d).

[7] A type of Authorized IRS *e-file* Provider. Publication 3112, IRS *e-file* Application & Participation.

financial institutions.[8] (Total summit membership is 63: 42 state agencies, officials from 20 industry organizations, and the IRS.). In furthering the FTC's Safeguards Rule, the Security Summit regularly reminds tax professionals to establish and maintain an up-to-date WISP. To assist tax professionals, the Security Summit issued a document with guidance on creating a WISP, along with a sample template, which the IRS published as Publication 5708, *Creating a Written Information Security Plan for your Tax & Accounting Practice*. The 28-page, easy-to-understand document was developed for tax professionals, particularly smaller practices, to keep customer and business information safe and secure. The sample template can help make data security planning easier for tax professionals, especially those of smaller size and operations.

The related Publication 4557, *Safeguarding Taxpayer Data: A Guide for Your Business*, is another resource for use by tax professionals to understand (1) basic security steps and how to take them; (2) understand and comply with the FTC Safeguards Rule; (3) recognize the signs of data theft and how to report it; and (4) respond to and recover from a data loss.

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.[9] But as a general matter, certain protocols ought to be considered:

- Do not collect more personally identifiable information (PII)[10] of clients than is necessary for your business operations, and do not retain PII longer than needed or legally required for business purposes.

---

[8] Security Summit | Internal Revenue Service; Publication 5648, Security Summit Membership Criteria

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

[10] PII "refers to any information that can identify or trace an individual either directly (direct identifiers) or when paired with other information (indirect identifiers)." https://www.security.org (giving as examples of PII, an individual's name; residential address or other geographic indicators; SSN; telephone number; email address; gender; and birthdate); *accord* BLACK'S LAW DICTIONARY, PII (12th ed. 2024) ("information that, by itself or in combination with other information, can identify the individual to whom it relates and thereby lead to invasion of privacy or other harms, such as identity theft"); *cf.* D. Embree, Magistrate Recommends Dismissal of Nationwide Data Breach Class Action, *Galaria v. Nationwide Mutual Insurance Co.*, 35 No. 12 Westlaw Journal Computer and Internet 6, 2017 WL 5573018, at *1 (Nov. 17, 2017) ("The stolen PII included consumers' names, Social Security and driver's license numbers, birthdates, marital status and other sensitive personal information, the complaint said.").

PII also encompasses sensitive information such as financial account numbers, medical information, and, of course, tax information.

- Protect the PII you collect, use, disclose, and retain. For example, store hardcopy PII in a locked room or file cabinets (and secure the information at the end of each workday).
- Restrict access to PII to only those individuals with a business need for the information.
- Dispose of PII appropriately, such as shredding documents and wiping (or destroying) old hard drives, fax machines, printers, and other office equipment.
- Use qualified and vetted contractors, including physical- and data-security consultants.
- Instill awareness and train employees (those professionally licensed and those uncredentialed alike) on the proper handling of PII.
- Establish security measures for electronic programs and files, including server locks; password practices and policies;[11] protection against, and guidance to staff on, phishing / malware schemes; and instructions on using and transporting laptops and mobile devices.
- Develop and enforce email policies and procedures that comply with federal and state laws that may apply[12] or any applicable rules.[13]

---

[11] Tax professionals should generally observe the following password guidelines:

- KEEP THEM SECRET. Never share passwords, or usernames, with others.
- USE STRONG PASSWORDS. Strong passwords consist of a random sequence of upper and lower-case letters and 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 A DEFAULT PASSWORD. Many devices come with default administrative passwords. Change them immediately. Default passwords are easily found or known by hackers.
- CHANGE YOUR 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.

[12] Many, if not most, laws at the state level appear to relate to the use of unsolicited marketing emails (or SPAM). For example, see Florida's Electronic Mail Communications Act (Fla. Stat. Title XXXIX, Ch. 688, Part III (Electronic Mail Communications)), section 668.601 of which, on "Legislative intent," states, "This part is intended to promote the integrity of electronic commerce and shall be construed liberally in order to protect the public and legitimate businesses from deceptive and unsolicited commercial electronic mail." See also Virginia' Consumer Data Protection Act, Title 59.1, Chapter 53.

Given that the laws in this area appear, in general, to be directed at controllers or processors of the data of large volumes of consumers, presumably the laws are inapplicable to small and midsized law or accounting firms, and maybe even large ones; further, the firms may be exempt from coverage anyway, for other reasons under the statutory provisions.

[13] E.g., ABA Annotated Model Rules of Professional Conduct § 1.6, Confidentiality of Information:

> ABA Formal Opinion 477R states that for most matters unencrypted email will be acceptable for lawyer-client communication but under some circumstances, such as where highly sensitive information is involved, "reasonable efforts" may require additional security safeguards, such as encryption, or even avoiding electronic communication altogether. The opinion also provides suggestions for how to determine what security measures will be reasonable. . . . *See also* ABA Formal Ethics Op. 2011-459 (2011) ("lawyer sending or receiving substantive communications with a client via e-mail . . . ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or e-mail account, where there is a significant risk that a third party may gain access."); . . . .

"The general rule is that a lawyer may use an e-mail service provider that conducts computer scans of e-mails to generate computer advertising, if no human beings (other than the sender and recipient) review the e-mails." Legal

- Continually monitor computer networks to identify and redress potential weaknesses and vulnerabilities (e.g., through operating system and other software updates, antivirus software, firewalls, security patches, and scan engines).
- Set guidelines on Internet browsing, use of "smart" devices, and use of social media and professional networking sites.
- Maintain good records and have policies and procedures in position for what to do in case of a data breach (including timely notification of the business's insurance carrier).[14]
- If your employees work remotely, adopt rules related to the safekeeping of physical files and other records kept at home and the use of :
  - virtual private networks (VPNs) to securely perform work activities and transactions;
  - separate personal and business computers, mobile devices, and email accounts; and
  - in-home "smart" devices.

Conclusion

Federal law, enforced by the FTC, requires tax return preparers to create and maintain a written information security program[15] (aka a WISP). Having a WISP protects businesses and their clients while providing a blueprint for action in the event of a security incident. [16] In addition, a WISP can help if other events seriously disrupt a tax professional's ability to carry out normal business, including fire, flood, tornado, and earthquake damage, and vandalism or theft.

Failure to maintain a WISP to protect private financial and personal information may not only put clients at risk for identity theft and fraud committed against them, it may also expose a practitioner to liability[17] for violating the Safeguards Rule and the terms of their malpractice

---

Ethics, Lawyer's Deskbk. Prof. Resp. § 1.6-2, *Inadvertent Disclosure* (2024-2025 ed.) (citing (N.Y. St. Bar. Ass'n Comm. Prof. Ethics Op. 820 (2008)).

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

[15] 16 CFR 314.3(a) (as to those subject to the Safeguards Rule, stating, in part, "you shall develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains . . . safeguards . . . ."); 16 CFR 314.2(r).

[16] In FTC terminology, a "security event." 16 CFR 314.2(q) (one "resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.").

[17] Courts have held that the Gramm-Leach-Bliley Act does not provide a private right of action for violations of the Act. *Newcomb v. Cambridge Home Loans, Inc.*, 861 F. Supp. 2d 1153, 1163 (D. Haw. 2012); *In re Gjestvang*, 405 B.R. 316, 320 (Bankr. E.D. Ark. 2009) (citing *Dunmire v. Morgan Stanley DW, Inc.,* 475 F.3d 956, 960 (8th Cir. 2007)).

Persons (individuals and entities) that have suffered injury or harm may, however, have a cause of action in federal or state court, predicated on **negligence per se** under state law, for violations of the Safeguards Rule, if not the statute itself. *See In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 371 F. Supp. 3d 1150, 1173-74 (N.D. Ga. 2019) ("Georgia law allows the adoption of a statute or regulation as a standard of conduct so that its violation becomes negligence per se. . . . . [And] unlike the GLBA itself, the Court concludes that the Safeguards Rule provides an ascertainable standard of conduct permitting it to serve as the basis for a negligence per se claim."); *cf.*

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 maintain procedures for compliance with Circular 230 by everyone involved in a tax practice, we encourage practitioners to pay heed to the requirement to have a WISP and implement adequate data security precautions.

BLACK'S LAW DICTIONARY, Negligence (12th ed. 2024) ("Negligence per se" usually "arises from a statutory violation."); *Doe v. Lyft, Inc.*, 756 F. Supp. 3d 1110, 1125 (D. Kan. 2024) ("The basic elements of negligence per se under Kansas law are: '(1) a violation of a statute, ordinance, or regulation, and (2) the violation must be the cause of the damages resulting therefrom.'") (internal citations omitted).

"[T]the doctrine of negligence per se is not a separate cause of action, but creates an evidentiary presumption that affects the standard of care in a cause of action for negligence." *Millard v. Biosources, Inc.*, 156 Cal. App. 4th 1338, 1353 n. 2, 68 Cal. Rptr. 3d 177, 188 (2007); *Sabo v. UPMC Altoona*, 386 F. Supp. 3d 530, 562 (W.D. Pa. 2019) (applying Pennsylvania law, under which negligence per se is an evidentiary presumption that a defendant's violation of a legislative or regulatory enactment constitutes proof of a breach of duty) (internal citations and quotation marks omitted).