FTC SAFEGUARDS · CPA & TAX

The CPA & Tax Pro's FTC Safeguards Cheat Sheet

Everything a 1–10 person accounting, tax, or bookkeeping firm in SW Riverside County actually has to do to protect client financial data — and what it costs you if you don't. In plain English, on one page.

You got licensed to do tax and accounting work, not to read federal cybersecurity rules. Here's the whole picture without the binder — so you know the right questions to ask before the FTC, the IRS, or a breach decides it for you.

1 The Mandate — What Law Applies

Yes — a tax or accounting firm is a "financial institution" under federal law. Three bodies can come at you, and none care how small you are.

- **FTC Safeguards Rule (16 CFR Part 314), under GLBA:** because you handle clients' nonpublic personal information (NPI) — SSNs, income, bank/brokerage data — the FTC classifies tax preparers, CPAs, accountants, and bookkeepers as **financial institutions**. Enforced by the **Federal Trade Commission (FTC)**.
- **IRS — Pub. 4557/5708 + e-file rules:** every paid preparer must maintain a **Written Information Security Plan (WISP)**, tied to your **EFIN**. The IRS can **suspend or revoke your e-file privileges**. Pub 5708 now explicitly requires **MFA** for all users touching customer data.
- **California Board of Accountancy (CBA):** a breach or failure to protect client information can become a **professional-discipline matter** against your CPA license.

Plain English: a single breach at a small tax firm is a **three-front problem** — a federal data-security regulator, the IRS holding your e-file privileges, and your state license board.

2 What Compliance Requires — The Must-Do List

The FTC Safeguards Rule names nine elements. For a small firm:

- **A Written Information Security Plan (WISP)** — your master document; the IRS requires it too (one WISP satisfies both). Not a one-time PDF.
- **A designated Qualified Individual (QI)** — one named, accountable person (the technical role can be supported by your IT provider).
- **A risk assessment** — where client NPI lives and what could go wrong. **5,000+ "consumers" must put this in writing** — and the count is **cumulative across years of returns** (spouses + dependents count), so a small office crosses 5,000 quietly.
- **Access controls + encryption** — least-privilege, **no shared logins**, MFA, encryption of NPI **in transit and at rest** (laptops + backups). **Vendor oversight** — written assurance your IT/cloud/backup/software vendors protect the data.
- **Continuous monitoring OR annual pen-test + biannual vuln scans** (required at 5,000+; SSS default = monitoring), plus a **written incident-response plan**, **workforce training**, and **secure disposal**.

The SSS throughline: most of this is the **technical layer we own for you** — encryption, MFA, monitoring, backup, vendor security — plus we help stand up and maintain the WISP the FTC and IRS ask to see.

The Penalties — What It Costs to Get This Wrong

2026 figures. No patient-style private lawsuit here — the exposure is the regulator, the IRS, and your license.

SOURCE	WHAT IT IS	THE NUMBER
FTC civil penalty	Statutory maximum **per violation** (a continuing violation can count as more than one)	**up to $53,088 / violation**
FTC consent decree	The real cost: years of mandatory third-party audits, public naming, oversight	**open-ended**
IRS	Suspension/revocation of your EFIN (e-file privileges)	**loss of e-filing**
CA Board of Accountancy	License discipline tied to a breach / failure to protect data	**license exposure**

FTC per-violation figure $53,088 — the 2025 inflation-adjusted amount, which remains in effect for 2026 (the federal 2026 adjustment was cancelled, OMB Memo M-26-11; 2025 levels apply through Jan 14, 2027). Verify before relying.

THE BREACH-REPORTING TRAP

Since **May 2024**, the Safeguards Rule requires notifying the **FTC within 30 days** of discovering a breach of **unencrypted** customer info affecting **500+ consumers** — and that report is **public**. Encryption is your **safe harbor**.

WHY MOST FIRMS GET HIT

It's rarely a one-shot mega-fine. It's **losing your EFIN in February**, or signing a multi-year **FTC consent decree** that defines your year. Most of what prevents it is *technical* — and most firms have never documented it.

The 5,000-Consumer Line — and the WISP the FTC Asks For First

The Safeguards Rule scales: cross **5,000 "consumers"** and four heavy items become mandatory (written risk assessment, continuous monitoring or pen-testing, written IR plan, annual report). The count is **cumulative across years of returns** — spouses and dependents included — so a small office crosses it quietly. When the FTC or IRS asks, the first thing they want to see is your **current WISP** and named Qualified Individual.

Honest bottom line: for a small firm, losing your EFIN in February or signing a multi-year FTC consent decree defines your year. Most of what prevents it is technical — and most firms haven't documented it.

WAIT — BUT WHAT ABOUT...

"My IT guy handles this."

Maybe. Ask him: *"Do we have a current WISP, who's our named Qualified Individual, and is our client data encrypted on every laptop and backup?"* General IT keeps computers running; the Safeguards items — encryption, MFA, access logs, vendor oversight, the WISP on file — are a different job, the one the FTC and IRS ask about first. And your **PTIN renewal makes you attest** you have a WISP that meets federal rules. No document = you don't have it.

"We're too small — and we outsource our software."

Two myths. The Rule covers **any** firm significantly engaged in financial activities — no small-firm exemption; a solo preparer is squarely in scope. And outsourcing software doesn't outsource the obligation: the Rule makes *you* responsible for overseeing service providers. Your software vendor secures *their* platform — not your network, email, laptops, or staff.

Not sure where YOUR firm actually stands? Find out for free — before the IRS or the FTC does.

We'll do a **free FTC Safeguards / WISP technical security review** of your firm — a local specialist looks at your actual setup (network, backup, encryption, MFA, email, vendor coverage, and whether you have a current WISP and named Qualified Individual) and tells you in plain English **(1)** whether your WISP and safeguards would hold up, and **(2)** whether you've crossed the **5,000-consumer threshold** that triggers the heavier rules. A **plain-English findings list** — where you're solid, where the gaps are. No sales pitch, no obligation. **We never ask for client or taxpayer information** on the call.

Book your free security review →

simonsayssystems.com/cpa-review · or call/text Craig direct: (951) 717-3576

Local to Menifee. Remote-first, on-site across Temecula, Murrieta, Wildomar, Lake Elsinore & Sun City. We already speak UltraTax, Lacerte, Drake, ProSeries, CCH Axcess & QuickBooks.