FTC SAFEGUARDS · INSURANCE

The Independent Agency Owner's FTC Safeguards Cheat Sheet

Everything an independent insurance agency in SW Riverside County actually has to do to satisfy the FTC Safeguards Rule — and what it costs you if you don't. In plain English, on one page.

You sell coverage; you didn't sign up to become a cybersecurity compliance officer. Here's the whole picture without the 50-page rule text — so you know the right questions to ask before a breach, a carrier audit, or the FTC decides it for you.

1 The Mandate — What Law Applies

Yes, your agency is a "financial institution" under federal law — and a federal cybersecurity rule already applies to you.

- **FTC Safeguards Rule (16 CFR Part 314), under GLBA:** because you regularly handle customers' nonpublic personal information — SSNs, driver's licenses, DOBs, financial and claims data — the FTC classifies you as a **financial institution** and requires a **written information security program**. Enforced by the **Federal Trade Commission (FTC)**.
- **Why the FTC and not a state insurance cyber law:** many states adopted the **NAIC Insurance Data Security Model Law**, routing insurance data security through the state commissioner. **California has *not* adopted it.** That leaves the **FTC Safeguards Rule as the operative federal cybersecurity framework** for a California agency. (California still has general privacy rules — CCPA/CPRA and older DOI privacy regulations — but no state insurance-cybersecurity statute displacing the federal Rule.)
- **CA Department of Insurance (secondary):** the DOI licenses you. A serious data-security failure can become a **licensing and "fitness" problem** on top of the federal exposure.

Plain English: there is no "insurance gets a pass" here. A federal rule already names you, and it has teeth.

2 What Compliance Requires — The Must-Do List

The Rule (§314.4) centers on a WISP — Written Information Security Plan:

- **A designated Qualified Individual (QI)** — one named, accountable person (can be supported by an IT/security partner; accountability still lives on paper). **A written risk assessment** — documented, updated as the agency changes.
- **Core technical safeguards, on by default: encryption** of NPI (rest + transit), **MFA** for anyone touching customer data, least-privilege **access controls**, **audit logging/monitoring**.
- **Vendor oversight** — vet and contractually bind service providers (cloud, IT, email, your agency-management system host); reassess periodically.
- **Workforce training** and a **written incident-response plan**.
- **The 5,000-consumer line that catches agencies off guard:** under **5,000** exempts you from four heavy items (written risk assessment, continuous-monitoring/pen-testing, written IR plan, annual report). **5,000+** makes them mandatory — and "consumers" counts **cumulatively across your book and history**, so a long-running agency crosses quietly. *We make counting it the first thing we check.*

The SSS throughline: nearly all of this is the **technical layer we own for you** — encryption, MFA, access controls, monitoring, vendor contracts, and the documentation that proves it.

The Penalties — What It Costs to Get This Wrong

2026 figures. No private lawsuit (GLBA gives consumers none) — but the federal numbers are blunt, and continuing violations compound.

MECHANISM	WHAT IT MEANS	THE NUMBER
FTC civil penalty, per violation	The FTC's maximum civil penalty for the law it uses to enforce Safeguards failures	**$53,088 / violation**
Continuing violations	A continuing failure can be treated as **more than one violation**, so exposure compounds	**penalties add up**
Consent decree / order	Usual FTC outcome: binding multi-year order — security program, outside assessments, reporting	**years of oversight**
CA DOI consequence	Licensing/fitness scrutiny layered on the federal action	**your license**

FTC per-violation maximum $53,088, effective Jan 17, 2025. The federal 2026 inflation adjustment was cancelled by OMB, so the 2025 figure carries into 2026 — verify before relying.

THE REALISTIC THREAT ISN'T A ONE-SHOT FINE

It's a **breach + FTC consent order**: a multi-year security program built under supervision, plus carrier and reputational fallout, plus a DOI question mark on your license.

YOUR CARRIER IS THE SECOND AUDITOR

Increasingly your **cyber/E&O carrier asks for proof at renewal** — WISP, MFA, encryption. A documented program is far cheaper than the cleanup, and it's what gets your renewal signed.

The 5,000-Consumer Line — and the WISP Your Carrier Now Asks For

The 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 your book and history**, so a long-running agency crosses it quietly. And increasingly the first party to ask for your WISP, MFA, and encryption proof isn't the FTC — it's your **cyber/E&O carrier at renewal**.

Honest bottom line: the realistic threat isn't a one-shot mega-fine — it's a breach + a multi-year FTC consent order, carrier and reputational fallout, and a DOI question mark on your license. A documented WISP and the safeguards under it are far cheaper than the cleanup.

WAIT — BUT WHAT ABOUT...

"My IT guy handles this."
Maybe. Ask him: *"Can I see our written information security plan, and who's our designated Qualified Individual?"* General IT keeps your network up; the FTC Safeguards program — WISP, QI, encryption, MFA, vendor oversight, risk assessment on file — is a different job, the one the FTC (and increasingly your cyber/E&O carrier at renewal) asks about first. No document = you don't have it.

"Our agency-management vendor covers compliance."
Applied, Vertafore and the rest secure *their* platform. FTC Safeguards is about *your* agency: your network, laptops, email, staff logins, backups, and the WISP that ties it together. The Rule makes the **financial institution — you —** responsible for the whole program, including overseeing the vendors who touch client NPI. The AMS is one piece you oversee, not a substitute.

Not sure where YOUR agency actually stands? Find out for free.

We'll do a **free FTC Safeguards / WISP technical security review** of your agency — a local specialist looks at your actual setup (network, backup, MFA, encryption, email, vendor access to client NPI, and whether you have a WISP and a named Qualified Individual on file) and gives you a **plain-English findings list**: where your technical safeguards are solid and where the gaps are. No sales pitch, no jargon, no obligation. **We never ask for your customers' personal information** on the call.

Book your free security review →

simonsayssystems.com/insurance-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 Applied Epic, AMS360, EZLynx & HawkSoft.