Guardian Compliance for RIAs and Financial Advisors

How PTS Guardian tiers cover the FTC Safeguards Rule, SEC Reg S-P and S-ID, and CIS Controls v8.1 for small financial institutions.

The business problem: Three regulators expect a documented cybersecurity program from your firm. The FTC Safeguards Rule requires a written information security program with nine specific elements and 30-day breach reporting. The SEC's amended Regulation S-P now requires written incident response policies and client notification, with full enforcement for smaller advisers by June 2026. Reg S-ID requires a documented identity theft prevention program. Most RIAs and small financial firms have the intent but not the documented controls, evidence, or program to prove it during an SEC exam or after an incident.

The PTS answer: Guardian Compliance is our tier purpose-built for SEC-registered advisers, FTC-regulated financial institutions, and small RIAs. It combines our managed help desk, cybersecurity, backup, M365 E5 cloud, and vCIO management with the written policies, audit-ready evidence, and air-gapped recovery your examiner, custodian, and cyber insurance carrier expect. **Compliance is the tier built to satisfy FTC Safeguards, SEC Reg S-P, and Reg S-ID end-to-end.**

THE SOLUTION

Why the Compliance tier

Compliance is the Guardian tier built end-to-end for financial institutions. Six capabilities make the difference between intent and examiner-defensible evidence:

- **M365 E5 with Purview, DLP, and Message Encryption.** Native customer-information data loss prevention, audit log retention, and encrypted external email. The control set FTC examiners, SEC staff, and custodian auditors expect.
- **Written Information Security Program (WISP).** Documented policies covering the nine elements required by 16 CFR §314.4 and the written incident response policies required under amended Reg S-P. Not a template, an applied program.
- **Air-gapped monthly server backups, performed and tested by PTS.** Demonstrable contingency planning under §314.4(h) with monthly restore evidence. Defensible against ransomware and SEC exam questions.
- **Annual risk assessment and 5-year IT lifecycle plan.** Documented risk assessment required by §314.4(b), refreshed annually. The single most-cited gap in FTC enforcement actions.
- **Qualified Individual designation and board reporting.** Required by §314.4(a). PTS provides the fractional Qualified Individual of record with annual board-level written report covering program status, risks, and incidents.
- **Identity hardening, MFA, and access controls.** Phishing-resistant MFA, conditional access, and least-privilege baselines under Reg S-P custom-information safeguards. Required by FTC Safeguards 314.4(c) and SEC custodial-rule due diligence.

WHAT YOU GET

Inside the Compliance tier

A single managed-service bundle that delivers the help desk, security, backup, M365 E5 cloud, and vCIO management your FTC Safeguards and SEC Reg S-P program depend on. Each layer is included in the monthly fee.

Service Layer	What you get
Help Desk	Remote, on-site, and emergency support within monthly limits. Acknowledge under 1 business hour, on-site under 8 business hours. 25% discount on after-hours emergency.
Cybersecurity	Advanced endpoint detection and response, 24/7 managed detection and response, phishing simulations and training, application allow-listing, DNS filtering, full-disk endpoint encryption, SIEM with compliance logging, network monitoring.
Backup	Image-based cloud backup (workstations and servers), 3x 2TB external drives included, monthly air-gapped server backups performed by PTS, monthly restore testing logged for examiner and custodian evidence.
Cloud (M365 E5)	M365 E5 licensing, Purview audit logs, DLP, Message Encryption, email and file backup, DDoS protection, DNS and domain management.
vCIO / Qualified Individual	Quarterly TBR, PTS firewall and network standards, vendor management, 100+ policy templates including FTC Safeguards WISP, Reg S-P incident response, and Reg S-ID identity theft prevention program. Annual written report to the board or owner.

Why one bundle, not piecemeal tools

Most RIAs and small financial firms inherit a patchwork: an MSP for the help desk, a separate backup vendor, an EDR the IT consultant recommended, and a WISP template purchased after the last FTC update. Guardian Compliance replaces that stack with one accountable provider whose evidence binder maps directly to your WISP and Reg S-P incident response policies.

What it takes	Piecemeal	Phantom Bundle
Vendor count	6 to 10 separate contracts: MSP, SOC, EDR, backup, M365, training	One contract, one invoice, one accountable provider
WISP and policies	Customer assembles WISP and S-P policies from each tool's documentation	PTS maintains WISP, S-P incident response, S-ID identity theft program
Restore testing	Backup vendor sells software; customer self-tests or skips	Monthly air-gapped restore performed and logged by PTS
Exam response	Firm scrambles to collect logs and policies from each vendor	One call to PTS, evidence delivered from existing binder
Qualified Individual	Owner or compliance officer wears the security hat alone	PTS fractional Qualified Individual of record, board-level reporting
Single point of escalation	Incident response routes through each vendor's separate support	P1-P4 escalation through one MSP, attorney-first protocol on day one

One contract. One WISP. One accountable provider. That is the difference between a tool stack and an examiner-ready program.

THE PROOF

The cost of getting it wrong

Cybersecurity enforcement against financial institutions is real and escalating. The figures below are public-record settlements from the SEC, FTC, FINRA, and state attorneys general. Small advisors are not exempt, they just settle for less than the headlines.

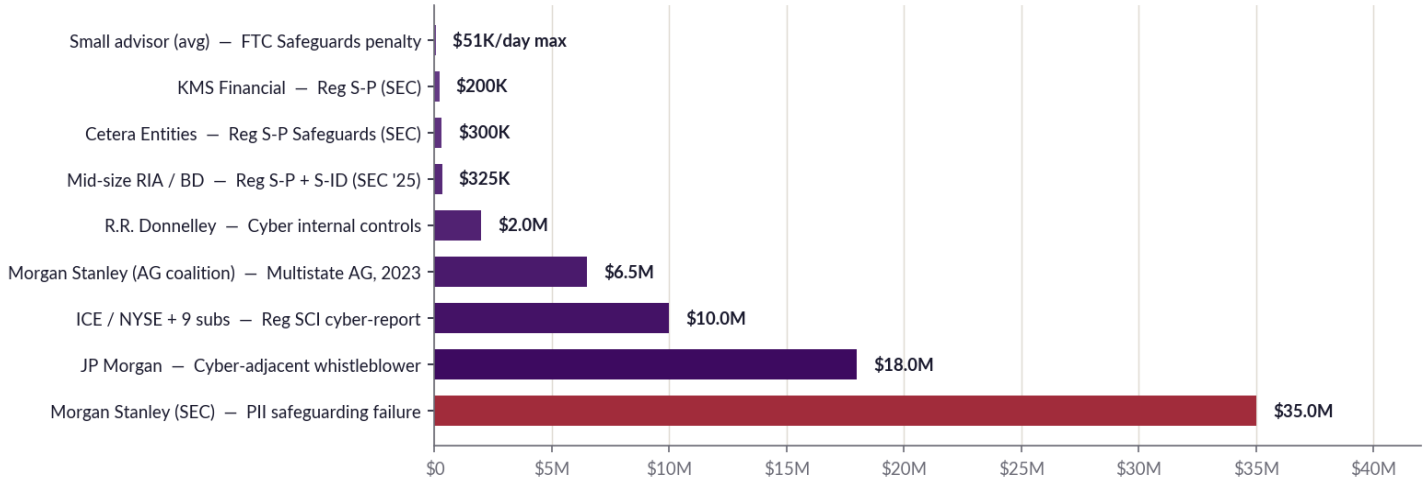
$51,744
Maximum FTC Safeguards Rule penalty per violation, per day

30 days
Maximum window to notify the FTC after a 500-customer breach

4 days
Maximum window to file SEC Form 8-K for a material cyber incident

$2B+
SEC recordkeeping penalties since 2021, including cyber-adjacent cases

Public-record financial services cyber enforcement.



Settlement amounts from SEC orders, FTC consent decrees, and state AG announcements. Beyond the penalty, every entity above also accepted multi-year compliance monitoring, mandatory program updates, and public consent orders. Legal fees, client departure, and reputational damage typically exceed the disclosed number.

Three patterns SEC and FTC examiners keep citing

PATTERN 01

No current Written Information Security Program

The most cited failure across every Reg S-P settlement. 16 CFR §314.4 and Reg S-P both require a documented, current WISP. Stale or template-without-tailoring is the same finding.

PATTERN 02

No designated Qualified Individual

16 CFR §314.4(a) requires a single designated individual responsible for the WISP. Spreading the role across IT, compliance, and outside counsel without naming one person is a documented violation.

PATTERN 03

Vendor and sub-processor blind spot

§314.4(f) requires you to oversee service providers handling customer information. Most firms have no inventory of vendors, no risk assessments, and no annual review. SEC exams now ask for this binder first.

THE DETAIL

Mapped to FTC Safeguards and Reg S-P

Each row pairs a Safeguards Rule element or SEC requirement with the Guardian capability that satisfies it, and shows which tier delivers it. Skim the Compliance column, every YES is an examiner-ready requirement covered out of the box.

FTC SAFEGUARDS RULE 16 CFR § 314.4(a)-(b) - Program ownership and risk assessment

Citation	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§314.4(a)	Designate a Qualified Individual responsible for overseeing, implementing, and enforcing the information security program.	PTS designated Qualified Individual of record, named in WISP and engagement letter, board reporting included.	NO	PART	YES
§314.4(b)	Base the information security program on a written risk assessment that identifies foreseeable threats to customer information.	Annual documented risk assessment, GRC-platform-tracked remediation, quarterly TBR with program update.	PART	YES	YES

FTC SAFEGUARDS RULE § 314.4(c) - Eight required safeguards

§314.4(c)(1)	Implement and review access controls; authenticate users; limit access to authorized individuals.	M365 identity, Entra ID conditional access, phishing-resistant MFA, role-based access, quarterly access reviews.	NO	YES	YES
§314.4(c)(2)	Identify and manage data, personnel, devices, systems, and facilities.	Full asset inventory in a secure documentation portal, M365 device inventory, vendor inventory, change-controlled.	PART	YES	YES
§314.4(c)(3)	Encrypt customer information in transit and at rest.	BitLocker endpoint encryption, M365 Message Encryption, TLS-enforced email, encrypted external backup drives.	PART	YES	YES
§314.4(c)(4)	Adopt secure development practices for in-house developed applications.	PTS firewall/network/wireless hardening standards, application allow-listing, secure-configuration baselines.	NO	PART	YES
§314.4(c)(5)	Implement MFA for any individual accessing any information system.	Phishing-resistant MFA enforced for VPN, RDP, admin consoles, M365, and all SaaS via SSO. Documented exception process.	NO	YES	YES
§314.4(c)(6)	Develop, implement, and maintain procedures for the secure disposal of customer information.	Endpoint encryption, secure-wipe procedure for retired devices, documented media disposal log.	NO	PART	YES
§314.4(c)(7)	Adopt procedures for change management.	Documented change management workflow, hardening baselines via Intune and group policy, monthly patch reporting.	PART	PART	YES
§314.4(c)(8)	Implement policies and procedures to monitor activity of authorized users and detect unauthorized access.	SIEM with integrated compliance logging, 24/7 managed detection and response, M365 Purview audit log retention.	NO	PART	YES

FTC SAFEGUARDS RULE § 314.4(d)-(h) - Testing, training, oversight, response, reporting

Citation	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§314.4(d)	Regularly test and monitor the key controls, systems, and procedures of the information security program.	Quarterly access reviews, monthly vulnerability scans, annual penetration test (Compliance only), monthly log review by PTS.	NO	PART	YES
§314.4(e)	Implement security awareness training and updates for all personnel.	Monthly phishing simulations, annual role-based training, documented completion records retained 6 years.	NO	YES	YES
§314.4(f)	Oversee service providers; select providers capable of maintaining appropriate safeguards; require by contract.	Vendor inventory, sub-processor risk reviews, contractual safeguards, annual review logged in vCIO scope.	NO	PART	YES
§314.4(g)	Periodically evaluate and adjust the program in light of testing results and material changes.	Annual program update, quarterly TBR with risk-ranked findings, vCIO-driven remediation roadmap.	PART	YES	YES
§314.4(h)	Establish a written incident response plan to respond to and recover from any security event.	Documented Incident Response Plan, P1-P4 playbooks, 24/7 managed detection and response, attorney-first protocol, annual tabletop exercise.	NO	PART	YES
§314.4(i)	Qualified Individual reports in writing to the board or governing body at least annually.	Annual board-level written report covering program status, risks, incidents, and recommendations.	NO	NO	YES
§314.5	Notify the FTC of a notification event involving 500 or more consumers, within 30 days.	Documented FTC breach notification workflow, attorney-first activation, breach notification scaffold ready to deploy.	NO	PART	YES

SEC REGULATION S-P 17 CFR § 248 - Customer information safeguards and incident response

Citation	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§248.30(a)	Adopt written policies and procedures to safeguard customer records and information.	Documented WISP covering all required controls, applied across the environment, maintained by PTS.	NO	PART	YES
§248.30(a)(3)	Implement written incident response program to address unauthorized access to or use of customer information.	Reg S-P incident response policy, breach notification scaffold, customer notification workflow.	NO	PART	YES

SEC REGULATION S-ID 17 CFR § 248.201 - Identity theft prevention program

Citation	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
§248.201	Develop and implement a written identity theft prevention program; periodically update and reassess covered accounts.	Documented Reg S-ID program template, red-flag identification process, periodic reassessment workflow.	NO	PART	YES

THE PATH FORWARD

What working with PTS looks like

From first call to ongoing program: four clear stages, no surprises. Most RIAs complete Discovery and Assessment within two weeks and reach a deployed Compliance posture in 30-90 days.

1
Discovery
60-min Safeguards and Reg S-P readiness review. We map your environment against this document.

2
Assessment
FTC Safeguards + CIS gap assessment. One-page snapshot, WISP draft outline, prioritized findings.

3
Implementation
Compliance tier deployed in 30-90 days. M365 E5, SIEM, air-gapped backups, WISP, S-P and S-ID policies.

4
Ongoing
Quarterly TBR, monthly air-gap testing, annual reorientation. Annual QI written report to your board.

Add a vCISO for examiner depth

For RIAs facing an SEC examination, a custodian onboarding questionnaire, a cyber insurance renewal, or a multi-office expansion, a fractional **Phantom vCISO** engagement layers on Qualified Individual responsibilities, board-level reporting, compliance roadmap, risk register ownership, and examiner liaison. Tiers: Foundation (quarterly), Operational (monthly), Strategic (monthly plus on-call).

Common gaps we find in RIAs and small firms

- No designated Qualified Individual named in writing
- WISP missing, generic, or last updated by a former consultant
- No documented vendor risk reviews for custodians or fintech
- MFA on email but not on RDP, custodian portal, or admin
- Backups exist, but restore testing never performed
- No annual written report to the board or owner

Important. FTC Safeguards, SEC Reg S-P, and Reg S-ID compliance are achieved by the financial institution, not by any single vendor. PTS provides the technology, documentation, and program rigor that demonstrably support your controls under 16 CFR Part 314 and 17 CFR Part 248. Final policy adoption, Qualified Individual designation, and management attestation remain the responsibility of the firm. PTS is not a registered broker-dealer or investment adviser.

Next step: 30-minute Safeguards Readiness Review

We walk your environment against this exact mapping and leave you with a one-page gap snapshot and WISP draft outline. No obligation.

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why practices choose Phantom

Since 2010
OPERATING
Indiana-based MSP serving financial services, professional services, and SMB clients.

100+
POLICY TEMPLATES
FTC Safeguards, Reg S-P, Reg S-ID, and CIS-aligned policy library applied to every engagement.

24/7
MDR COVERAGE
Partner SOC monitoring, incident response runbooks, attorney-first escalation.