Guardian Compliance for Law Firms

How PTS Guardian tiers deliver the reasonable efforts ABA Model Rule 1.6(c), Formal Opinions 477R and 498, and your clients expect.

The business problem: ABA Model Rule 1.6(c) requires every lawyer to make reasonable efforts to prevent the unauthorized disclosure of client information. ABA Formal Opinions 477R, 483, and 498 spell out the specific obligations for electronic communications, post-breach client notification, and virtual practice. Sophisticated corporate clients now require security attestations before engaging outside counsel. Cyber insurance carriers will not renew without MFA, EDR, and tested backups. Most small and mid-sized firms have the intent but not the documented program to prove it during a malpractice claim, a client security audit, or after an incident.

The PTS answer: Guardian Compliance is our tier purpose-built for law firms and professional service firms with fiduciary confidentiality obligations. 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 clients, malpractice carrier, and the ABA expect. **Compliance is the tier that documents the reasonable efforts Rule 1.6(c) requires.**

THE SOLUTION

Why the Compliance tier

Compliance is the Guardian tier built end-to-end for firms with fiduciary confidentiality obligations. Six capabilities make the difference between reasonable intent and documented reasonable efforts:

- **M365 E5 with Purview, DLP, and Message Encryption.** Client-confidential data loss prevention, audit log retention, and encrypted external email. The control set sophisticated clients and cyber insurance underwriters now require.
- **Written Information Security Program and IR Plan.** Documented policies covering confidentiality, access control, and breach response. Aligns with ABA Opinion 477R electronic communications and Opinion 483 post-breach notification duties.
- **Air-gapped monthly server backups, performed and tested by PTS.** Demonstrable contingency for ransomware. The single most effective control against the law-firm-targeted ransomware that hit Grubman, Campbell Conroy, and Orrick.
- **Phishing-resistant MFA on every remote access path.** Email, VPN, RDP, admin, and SaaS via SSO. The most-exploited gap in published law firm breaches, and the first item on every client security questionnaire.
- **Sub-processor and vendor inventory with risk reviews.** Co-counsel, e-discovery vendors, court reporters, expert witnesses, and case management SaaS all touch client data. PTS maintains the inventory, contractual safeguards, and annual review log.
- **Annual training, phishing simulation, and tabletop exercise.** ABA Opinion 477R requires periodic training in secure electronic communications. Documented completion records retained for client audits and malpractice carrier reviews.

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 firm's ABA obligations 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 client and malpractice carrier evidence.
Cloud (M365 E5)	M365 E5 licensing, Purview audit logs, DLP for client-confidential data, Message Encryption, email and file backup, DDoS protection, DNS and domain management.
vCIO / IT Leadership	Quarterly TBR, PTS firewall and network standards, vendor and sub-processor management, 100+ policy templates including Confidentiality, Acceptable Use, IR Plan, and post-breach client notification scaffold under Opinion 483. Annual written report for managing partners.

Why one bundle, not piecemeal tools

Most small and mid-sized firms accumulate a patchwork: an MSP for the help desk, a separate backup vendor, an EDR the IT consultant set up years ago, and a confidentiality policy lifted from a CLE deck. Guardian Compliance replaces that stack with one accountable provider whose evidence binder maps directly to your firm's ABA obligations and client security questionnaires.

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
Documentation	Firm assembles confidentiality and IR policies from each tool	PTS maintains policy library, IR Plan, breach notification scaffold
Restore testing	Backup vendor sells software; firm self-tests or skips	Monthly air-gapped restore performed and logged by PTS
Client questionnaire response	Firm scrambles to answer each corporate client's security survey	One call to PTS, attestations and evidence delivered from binder
Sub-processor accountability	Firm tracks each vendor's security posture independently	PTS maintains sub-processor inventory and annual risk reviews
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 IR Plan. One accountable provider. That is the difference between a tool stack and the reasonable efforts Rule 1.6(c) requires.

THE PROOF

The cost of getting it wrong

Law firms are a top-five target for ransomware operators because their data is uniquely valuable and time-sensitive. The figures below are public-record settlements and ransom demands. Small firms are not exempt, they just rarely make headlines.

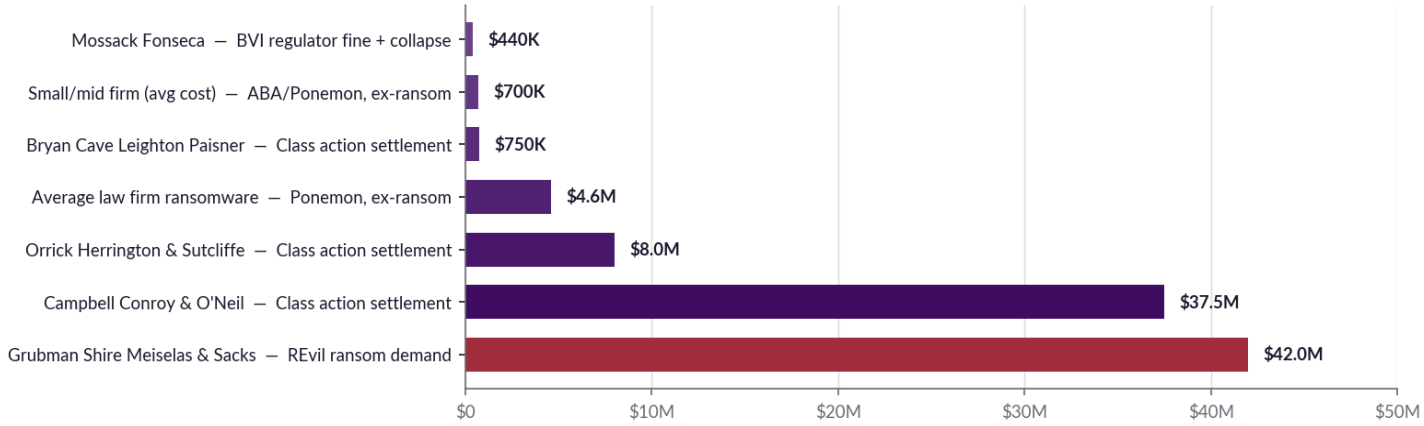
$4.6M
Average law firm ransomware cost, excluding the ransom (Ponemon)

75%+
Of AmLaw 100 firms hit by a cybersecurity incident in the last 3 years

Rule 1.6
ABA Model Rule that obligates reasonable cybersecurity efforts

Opinion 483
ABA duty to notify clients after a breach of confidential information

Public-record law firm cyber impact.



Settlement amounts and ransom demands from court filings, company statements, and the ABA. Beyond the dollar figure, each firm above also faced client departure, partner-track disruption, and reputational impact that the disclosed number does not capture. Mossack Fonseca dissolved within two years of its breach.

Three patterns we keep finding in law firms

PATTERN 01

MFA on email, not on remote access

VPN, RDP, and admin consoles still password-only. The most-exploited gap in published law firm ransomware cases including Grubman and Campbell Conroy. Phishing-resistant MFA on every remote entry point closes it.

PATTERN 02

Sub-processor and vendor blind spot

E-discovery vendors, court reporters, expert witnesses, and case-management SaaS all touch client-confidential data. Most firms have no inventory, no risk reviews, and no contract language. Client questionnaires now ask for this binder first.

PATTERN 03

No documented IR Plan or breach-notification scaffold

ABA Opinion 483 requires post-breach notification to affected clients. Most firms have no template, no decision tree, and no attorney-first protocol. The result is a frozen response when every hour matters.

THE DETAIL

Mapped to ABA Rule 1.6 and CIS Controls

Page 4 pairs each ABA obligation with the Guardian capability that delivers it. Page 5 shows the CIS Controls v8.1 baseline that implements ABA's reasonable efforts in practice. Skim the Compliance column, every YES is documented and audit-ready.

ABA MODEL RULE 1.6(c) - Reasonable efforts to prevent unauthorized disclosure

ABA Rule / Op	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
Rule 1.6(c)	Make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to client representation.	Full security stack: MFA, EDR, MDR, DLP via M365 Purview, BitLocker encryption, application allow-listing, SIEM logging, documented policies.	NO	PART	YES
Rule 1.1 Cmt 8	Maintain competence in the benefits and risks associated with relevant technology used in the practice of law.	Annual technology training included in awareness program, quarterly TBR with vCIO recommendations, 5-year IT and lifecycle roadmap.	NO	YES	YES
Rules 5.1 / 5.3	Ensure that lawyers and non-lawyer assistants comply with the rules of professional conduct, including the technology obligations.	Documented Acceptable Use Policy, role-based access, monthly phishing training for all staff, completion records retained 6 years.	NO	YES	YES

ABA FORMAL OPINION 477R - Securing electronic client communications

Op 477R ¶ 1	Use reasonable efforts when transmitting client-confidential information electronically.	TLS-enforced email, M365 Message Encryption available for sensitive messages, encrypted client portals through approved SaaS.	PART	PART	YES
Op 477R ¶ 2	Establish policies, train staff, and periodically reassess electronic communication practices.	Documented Electronic Communications Policy, annual training, quarterly TBR includes communications review.	NO	YES	YES
Op 477R ¶ 3	Use commonly available methods to disable lost or stolen devices and destroy device data.	BitLocker encryption, Intune-based remote wipe of mobile devices, documented lost-device procedure.	NO	PART	YES

ABA FORMAL OPINION 483 - Lawyer's obligations after a data breach

Op 483 Sec II	Monitor for a data breach and stop it when discovered; restore systems.	24/7 managed detection and response, SIEM with anomaly alerts, documented IR Plan with P1-P4 playbooks, air-gapped backups.	NO	PART	YES
Op 483 Sec IV	Notify affected clients when material client-confidential information is breached.	Breach notification scaffold, attorney-first protocol, customer-by-customer notification workflow, cyber insurance activation support.	NO	NO	YES

ABA FORMAL OPINION 498 - Virtual practice obligations

ABA / CIS	Requirement	How Guardian Delivers	Co-Mgd	Fund.	Compl.
Op 498	Maintain confidentiality, supervision, and competence obligations when practicing remotely or through cloud services.	Conditional access for remote work, M365 device compliance enforcement, VPN/ZTNA where required, documented remote-work policy.	NO	YES	YES

CIS 01-05 - Foundation: assets, software, data, configuration, accounts

CIS 01	Inventory and control of enterprise assets connected to the firm's infrastructure.	Full asset inventory in a secure documentation portal, M365 device inventory, change-controlled.	YES	YES	YES
CIS 02	Inventory and control of software assets; only authorized software installed and executable.	Software inventory via RMM and centrally managed endpoint policy, application allow-listing on supported endpoints.	PART	YES	YES
CIS 03	Data protection: identify, classify, securely handle, retain, and dispose of client-confidential data.	BitLocker encryption, M365 Purview DLP, encrypted email, documented client-confidential data classification, secure media disposal.	PART	YES	YES
CIS 04	Secure configuration of enterprise assets and software; patch and update systems.	Documented hardening baselines via Intune and group policy, patch management on supported endpoints, monthly compliance reporting.	YES	YES	YES
CIS 05	Account management: assign and manage credentials for user, administrator, and service accounts.	M365 identity governance, designated admin accounts, enterprise password vault with rotation, joiner-mover-leaver workflow.	YES	YES	YES

CIS 06-08 - Access control, awareness, audit logging

CIS 06	Access control: phishing-resistant MFA on all remote access, role-based access, quarterly reviews.	Entra ID conditional access, phishing-resistant MFA on email/VPN/RDP/admin, role-based access, quarterly access reviews.	YES	YES	YES
CIS 08	Audit log management: collect, alert, review, and retain audit logs.	SIEM with integrated compliance logging, M365 Purview audit log retention, 24/7 MDR, documented monthly log review.	PART	YES	YES
CIS 14	Security awareness and skills training: phishing-resistant culture, social engineering awareness.	Monthly phishing simulations, annual ABA-aligned training including Opinion 477R obligations, documented completion records.	YES	YES	YES

CIS 11 / 17 - Recovery and incident response

CIS 11	Data recovery: tested practices sufficient to restore in-scope assets to a pre-incident and trusted state.	Image-based cloud backup, monthly air-gapped server backups performed by PTS, monthly restore testing with documented log.	YES	YES	YES
CIS 17	Incident response: documented program to prepare, detect, and respond to attacks.	Documented IR Plan, P1-P4 playbooks, partner SOC threat response, attorney-first protocol, annual tabletop exercise, Opinion 483 notification scaffold.	PART	YES	YES

THE PATH FORWARD

What working with PTS looks like

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

1
Discovery
60-min ABA and CIS readiness review. We map your environment against this document's controls.

2
Assessment
ABA Rule 1.6 + CIS gap assessment. One-page snapshot, policy-library outline, prioritized findings.

3
Implementation
Compliance tier deployed in 30-90 days. M365 E5, SIEM, air-gapped backups, IR Plan, training.

4
Ongoing
Quarterly TBR, monthly air-gap testing, annual reorientation. Annual written report for managing partners.

Add a vCISO for partner-level depth

For firms facing a sophisticated-client security questionnaire, a malpractice carrier renewal, a multi-office expansion, or a lateral partner integration, a fractional **Phantom vCISO** engagement layers on board and partner-meeting reporting, compliance roadmap, risk register ownership, and incident liaison. Tiers: Foundation (quarterly), Operational (monthly), Strategic (monthly plus on-call).

Common gaps we find in law firms

- MFA on email but not on VPN, RDP, or admin consoles
- No documented IR Plan or client-notification scaffold
- Sub-processor and vendor inventory missing or stale
- Confidentiality policy lifted from a CLE, never updated
- Backups exist, but restore testing never performed
- Lateral attorneys onboarded without access reviews

Important. ABA Model Rule 1.6(c) compliance is achieved by the lawyer and the firm, not by any single vendor. PTS provides the technology, documentation, and program rigor that demonstrably support the reasonable efforts ABA Rule 1.6(c) and Formal Opinions 477R, 483, and 498 require. Final policy adoption, partner supervision, and client notification decisions remain the responsibility of the firm and its lawyers. PTS is not a law firm and does not provide legal advice.

Next step: 30-minute ABA and CIS Readiness Review

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

Talk to PTS

hello@phantomts.com
phantomts.com/guardian

Why practices choose Phantom

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

100+
POLICY TEMPLATES
ABA-aligned and CIS Controls v8.1 IG1-aligned policy library applied to every engagement.

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