CADEX

FRIEDMAN ■ FRAMME ■ THRUSH ■

ATTORNEYS AT LAW

CLLA · November 2026

Cybersecurity on the Front Lines of Commercial Collections

Protecting Your Firm, Your Clients, and Your Data



WHY IT MATTERS

Why Creditors' Rights Professionals Are a Target



A goldmine of sensitive data

Creditors' rights attorneys, commercial collection agencies, and legal networks hold financial records, personal data, account histories, and privileged communications — exactly the assets criminals monetize fastest.

Law firms and collection agencies sit at the top of today's ransomware, extortion, and business-email-compromise target lists — **and the threats are getting sharper, faster, and more expensive.**

65% of law firms have already suffered a cyber incident

$2.5M average ransom demand made to a law firm

+47% more ransomware cases posted in 2025 vs. 2024

THE THREAT LANDSCAPE

The Threats Most Likely to Hit Your Firm

Ransomware & Data Extortion

Encrypted case files, halted operations, six-figure demands — increasingly paired with threats to leak stolen client data.

Business Email Compromise

Impersonation of partners, clients, or debtors to redirect funds or trick staff into handing over data.

Wire Fraud & Payment Diversion

Fraudulent wire instructions slipped into settlements or disbursements — money sent is rarely recovered.

Vendor & Third-Party Breaches

Your weakest vendor is your weakest link. Court-filing, e-discovery, and IT providers are all in scope.

Extortion-Only & 'Fake IT' Vishing

New crews steal data without encryption and pose as IT by phone — bypassing traditional ransomware defenses.

Credential Theft & Insider Risk

Reused passwords, phishing, and hidden inbox rules give attackers a quiet foothold for weeks before they strike.

THE SCALE OF THE PROBLEM

The Threat, By the Numbers

Recent industry and government data on attacks against legal and financial-services firms.

6,330

ransomware cases posted to leak sites by Oct 2025 — up ~47% YoY

200+

ransomware incidents against law firms in 2025–early 2026

$2.47M

average ransom demand made to a law firm

$447K

average loss per real-estate wire-fraud (BEC) incident

100+

law-firm attacks by a single data-extortion crew since 2022

$2.4B

annual U.S. losses reported to the FBI from BEC scams

IT HAPPENED TO THEM

Real Case Files

Recent breaches and cyber events at debt collectors, law firms, and the financial-services partners you work with every day — and the lessons each one leaves behind.

CADEX

Sources on the final slide



REAL CASE FILES · DEBT COLLECTORS

When the Collector Becomes the Victim

Third-party collection agencies concentrate sensitive data — one breach cascades to hundreds of clients.

4.2M

Financial Business & Consumer Solutions

2024 · PENNSYLVANIA DEBT COLLECTOR

A two-week intrusion exposed names, SSNs and DOBs. Estimates ballooned from 1.9M to 4.2M and swept in Comcast and Truist customers; 14+ lawsuits followed.

1.9M

Professional Finance Company (PFC)

2022 · HEALTHCARE COLLECTIONS

A ransomware attack hit 657 healthcare clients. PFC settled the class action for $2.5M — a direct preview of the legal exposure a single incident creates.

560K+

Nationwide Recovery Service (NRS)

2024 · VENDOR-TO-CLIENT CASCADE

Attackers exfiltrated data over six days. NRS waited 7 months to notify clients — one city canceled its contract and threatened litigation over the delay.

3.7M

Receivables Performance Management

2022 · UNDETECTED 18 MONTHS

A breach went unnoticed for a year and a half before discovery — a stark reminder that detection, not just prevention, is what limits the damage.

REAL CASE FILES · LAW FIRMS

Law Firms in the Crosshairs

Attorney-client data is uniquely coercive — clients, opposing parties, and the bar all become pressure points.

$8M



Orrick, Herrington & Sutcliffe

2023 · GLOBAL LAW FIRM

A two-week intrusion exposed 600,000+ people's data held for the firm's own clients. Orrick settled consolidated class actions for $8M.

$42M



Grubman Shire Meiselas & Sacks

2020 · REvil RANSOMWARE

REvil stole 756 GB of celebrity client files and demanded $21M — then doubled it to $42M. A textbook 'double-extortion' attack on a marquee firm.

$20M



Silent Ransom Group (Luna Moth)

2025–26 · 100+ FIRMS TARGETED

This crew steals data without any malware, poses as IT staff by phone, and extorts. One firm paid $20M; the FBI issued two FLASH alerts in 13 months.

10



INC Ransom — Legal Sector Campaign

2026 · SUPPLY-CHAIN CLUSTER

INC listed 10 law firms on its leak site within a 48-hour window — a likely shared-vendor compromise hitting multiple firms through one upstream breach.

CADEX

REAL CASE FILES · WIRE FRAUD & BEC

The Quietest Loss: Business Email Compromise

No malware, no encryption — just a convincing email or a fake identity, and the money is gone.

WilmerHale — Identity Deception

5 states

2026 · NO HACK REQUIRED

An employee gave client data — including SSNs — to someone who simply misrepresented their identity. Proof that budget and size are not the defense.

Holland & Knight — Intercepted Closing

$3.1M

2020 · STOCK-TRANSACTION WIRE

A fraudster intercepted email with the real sellers, impersonated them, and supplied new wire instructions to a Hong Kong account. $3.1M diverted.

Real-Estate Closing Fraud

$447K

2023–25 · AVERAGE LOSS

Attackers monitor a mailbox for weeks, then send 'updated wire instructions' timed to a real closing. Real estate is now the highest-loss BEC category.

14-Person Firm — Reused Password

$98K

REPRESENTATIVE · SMALL FIRM

A reused password, a hidden inbox-forwarding rule, no MFA and no call-back verification cost a small firm $98K in a single afternoon.

CADEX

ACROSS ALL 13 REAL CASES

How the Bad Actors Got In

The sobering pattern: for **8 of the 13 breaches the entry point was never disclosed** — but where it is known, it comes back to the same few doors.

INITIAL-ACCESS VECTOR	SEEN / IMPLIED IN	WHAT STOPS IT
Remote access without MFA (VPN / RDP)	Rodenburg (Akira), CML (Meow), Stevens & Lee	Phishing-resistant MFA on every remote service
Stolen / brute-forced credentials	Akira & Meow playbooks; Stevens & Lee	Unique passwords, MFA, lockout & monitoring
Phishing / malicious loaders	PFC (Conti / Quantum), Meow playbook	Email filtering, user training, EDR
Unpatched internet-facing software	IC System (MOVEit zero-day) — confirmed	Emergency patching, attack-surface mgmt
Undisclosed (8 of 13 incidents)	FBCS, RPM, NCB, Convergent, NRS, Credit Control, DHCA, Berman & Rabin	Assume all of the above — defense in depth

The real enabler was dwell time: *RPM sat ~34 days and CML ~11 months undetected. However they got in, weak detection let them stay long enough to do maximum damage.*

WHAT'S AT STAKE

More Than Just Money



Client Trust

Reputational damage outlasts the breach. Clients expect their counsel and agencies to safeguard their data — full stop.



Regulatory & Ethical Duties

State bars, the FTC, GLBA, and state privacy laws all impose data-security obligations — with real penalties for falling short.



Operational & Financial Loss

Downtime, ransom payments, breach-notification costs, litigation, and lost revenue from halted collections operations.

WHAT'S CHANGED SINCE AUGUST 2026

Regulatory Update: The Bar Keeps Rising

Federal

FTC Safeguards Rule

30-day breach notice (500+ consumers) being renewed for 3 years; new FTC Rule Guidance Program.

GLBA Exemption Shrinking

CT (Jul 2026) and DE (Jan 2027) drop the entity-level GLBA exemption — only GLBA data stays exempt.

CFPB / Regulation F

Rule unchanged; deregulatory agenda. Collection complaints nearly doubled in 2025 — states fill the gap.

State

NY DFS Part 500

Fully in effect: MFA for all users and asset inventory. New 2026 risk-assessment guidance.

California

DFPI expects cyber incident reports within 48 hours. CCPA annual cybersecurity audits and risk assessments now in force.

24 States & Counting

New 2026 laws in OK, LA, AL and VT. CT SB 4 took effect Oct 1; DE lowers threshold to 10,000 consumers.

Enforcement & Clients

LabCorp Settlement

44 AGs, $2.3M over a collection-vendor breach; new vendor terms took effect Oct 1, 2026.

Client Demands

Annual SOC 2 Type 2 or HITRUST, NIST data purge and written deletion certifications now in contracts.

AI Under Exam

State bank regulators' AI exam framework asks for AI inventories, vendor terms and AI incident response.

Cyber Insurance

Carriers now require MFA, EDR, tested backups and IR plans before they will bind coverage.

Bottom line: *states and settlements — not new federal rules — are now setting the cybersecurity bar for collectors.*

ETHICS & PROFESSIONAL RESPONSIBILITY

Cybersecurity Is Now Professional Responsibility

The ABA Model Rules increasingly treat cybersecurity not as an IT issue, but as a lawyer-management obligation.



Rule 1.1

Competence

Lawyers must understand the benefits and risks of technology — now including cybersecurity, cloud, AI tools, email security, and protection of electronically stored information (ESI).



Rule 1.6

Confidentiality

Attorneys must make reasonable efforts to prevent unauthorized access or disclosure of client information — extending to email, cloud, laptops, mobile devices, and third-party software.



Rule 1.4

Communication

Significant cyber incidents may require disclosure to affected clients. The key question: does the incident materially affect the client's interests?

Bottom line: *"We didn't know" is becoming a difficult defense when reasonable safeguards are available.*

ABA MODEL RULES IN PRACTICE

The Five Rules Every Attorney Should Know

Rule 1.1	**Competence**	Includes understanding technology and cyber risk.
Rule 1.6	**Confidentiality**	Reasonable efforts to protect client information from unauthorized access or disclosure.
Rule 5.1	**Supervision**	Partners must establish reasonable measures ensuring attorneys comply with ethical duties.
Rule 5.3	**Non-Lawyer Assistance**	The same oversight applies to staff, cloud providers, MSPs, and e-discovery vendors.
Rule 1.4	**Communication**	Clients may need to be informed when cyber events affect confidential information.

Practical Reality

- Ethics complaints
- Malpractice exposure
- Breach of fiduciary duty claims
- Client attrition
- Reputational damage

AFTER THE BREACH

What Bar Counsel, Regulators & Plaintiffs' Lawyers Will Ask

When a law firm experiences a breach, the investigation is rarely about the technology itself.

- Did the firm require MFA?
- Was there a written cybersecurity policy?
- Was an incident-response plan in place?
- Were compromised clients notified appropriately?
- Were laptops and devices encrypted?
- Had personnel received security training?
- Were vendors evaluated before handling client data?
- Who in firm leadership owned oversight?

The question behind every question: *"Did the firm take reasonable measures expected of a competent lawyer under the circumstances?"*

DEFENDING YOUR FIRM

Concrete Steps to Strengthen Your Defenses



01 **Identity & Access**

Enforce MFA everywhere, use unique passwords via a manager, and strictly limit administrator accounts.



02 **Backup & Recovery**

Keep tested, offline, immutable backups — and rehearse the restore, don't just assume it works.



03 **Train Your People**

Run phishing simulations, mandatory out-of-band wire-verification, and clear escalation paths for anything suspicious.



04 **Detect & Respond**

Deploy endpoint detection, monitor the alerts, and keep a tested incident-response plan ready to launch.

BEST PRACTICES & INDUSTRY-LEADING STANDARDS

The Modern Cybersecurity Standard of Care

Organized around the **NIST Cybersecurity Framework 2.0** — from essential hygiene to cutting-edge controls.

Govern

Risk owned by leadership

- Written Info Sec, AI-use policies with committee
- Board / partner risk reporting
- Cyber insurance aligned to exposure

Identify

Know what you protect

- Asset & data inventory (CIS 1–2)
- Classify privileged & client data
- Vendor & supply-chain register

Protect

Close the common doors

- Phishing-resistant MFA (FIDO2 / passkeys)
- Zero-Trust, least-privilege access
- Encryption everywhere; security training

Detect

Catch intruders early

- 24/7 MDR / XDR monitoring
- Endpoint detection & response (EDR)
- Central logging; continuous vuln scans

Respond

Have a plan, rehearsed

- Tested IR plan with named roles
- Counsel & forensics on retainer
- Breach-notification playbook

Recover

Bounce back fast

- Immutable, offline backups
- Rehearsed restore drills
- Business-continuity plan

*Aligned to **NIST CSF 2.0 · CIS Controls v8.1 · CISA Zero-Trust** — the standard regulators, insurers, and courts now expect.*

KEY TAKEAWAYS · THANK YOU

Your Roadmap — and How to Reach Us

You are a target. Treat cybersecurity as a core business risk, not an IT footnote.

Basics still win. MFA, backups, training, and patching prevent most incidents.

Your vendors are your perimeter. Govern them like it — inventory, contract, and re-certify access.

Have a plan before you need one. Write your incident-response plan, then rehearse it.

Document everything. "Reasonable security" is a record you can show, not a feeling.



Andy Balthaser

Chief Compliance & Privacy Officer
Interim Chief Information Security Officer

CADEX

andy.balthaser@cadexsolutions.com

(804) 240-8960



William H. Thrush, Jr.

Managing Principal

FRIEDMAN ■ FRAMME ■ THRUSH ■
ATTORNEYS AT LAW

wthrush@fftlaw.com

(410) 559-9000