_____ PROGRAM MATERIALS
Program #36172
October 19, 2026

The Aftermath of Scams and Cybercrime; A Practical Guide to Response and Recovery

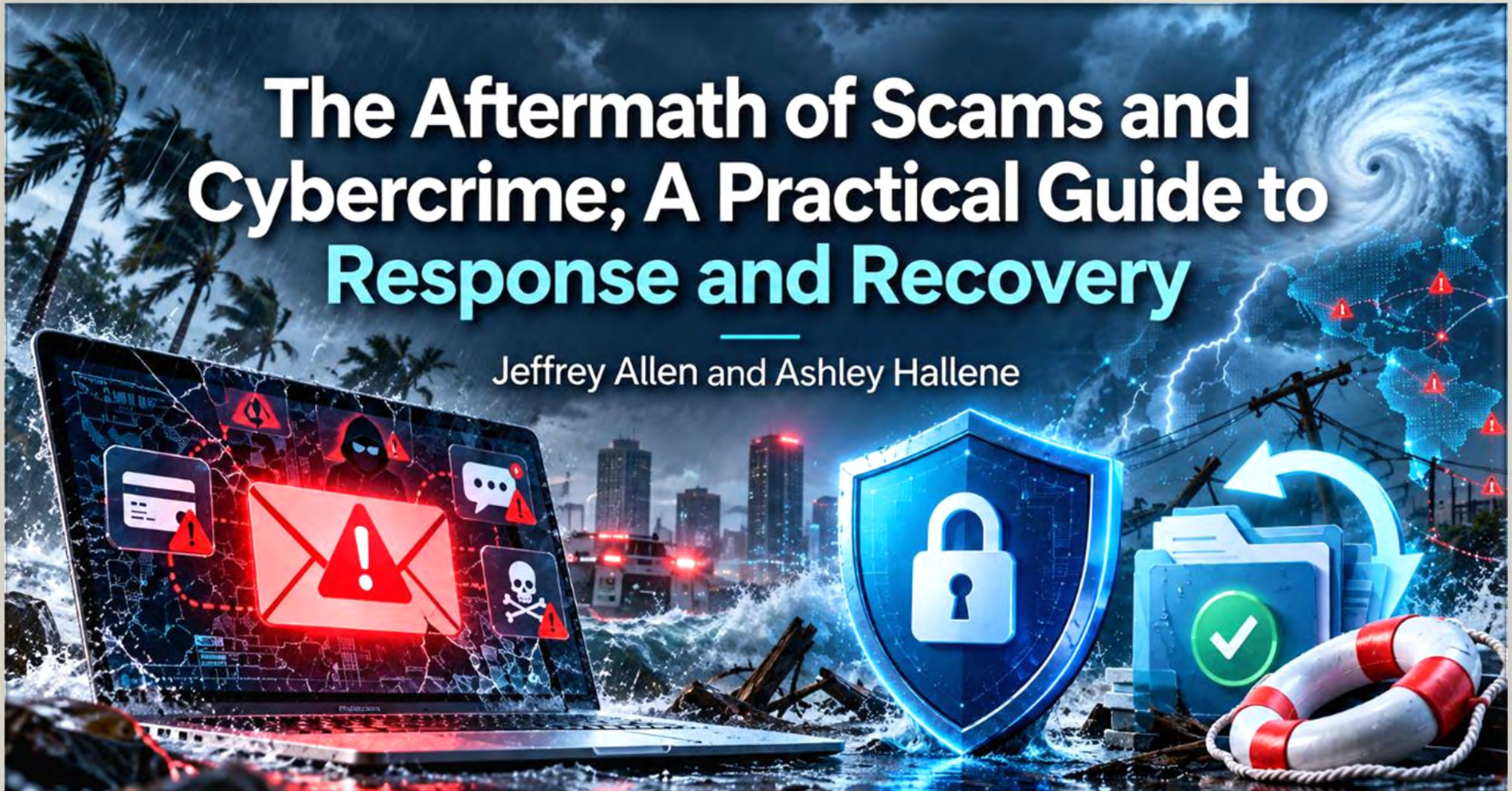
Copyright ©2026 by

- Jeffrey Allen, Esq. - Graves & Allen Attorneys and Counselors at Law
- Ashley Hallene - Demeter Land Development

All Rights Reserved.
Licensed to Celesq®, Inc.

Celesq® AttorneysEd Center
www.celesq.com

5301 North Federal Highway, Suite 150, Boca Raton, FL 33487
Phone 561-241-1919



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

PRESENTERS



JEFFREY ALLEN

GRAVES & ALLEN

ATTORNEY | ARBITRATOR | MEDIATOR

jallenlawtek@aol.com

(510) 610-8777

- Attorney, Arbitrator & Mediator
- Author and Legal Technology Advisor
- Cybersecurity, Privacy & Risk Management
- Co-Editor, ABA Cybersecurity Handbook, 4th Ed.

ASHLEY HALLENE

ATTORNEY & ADVISOR

ahallene@gmail.com

(281) 433-6220

- Attorney, Writer & Educator
- Cybercrime, Compliance & Ethics
- Legal Practice & Technology
- Advocate for Senior & Solo Attorneys



EMPOWERING LAWYERS. • MITIGATING RISK. • PROTECTING CLIENTS.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

A cyber incident rarely stays in one lane.

NEARLY

$21B

reported U.S. cyber-enabled crime losses in 2025

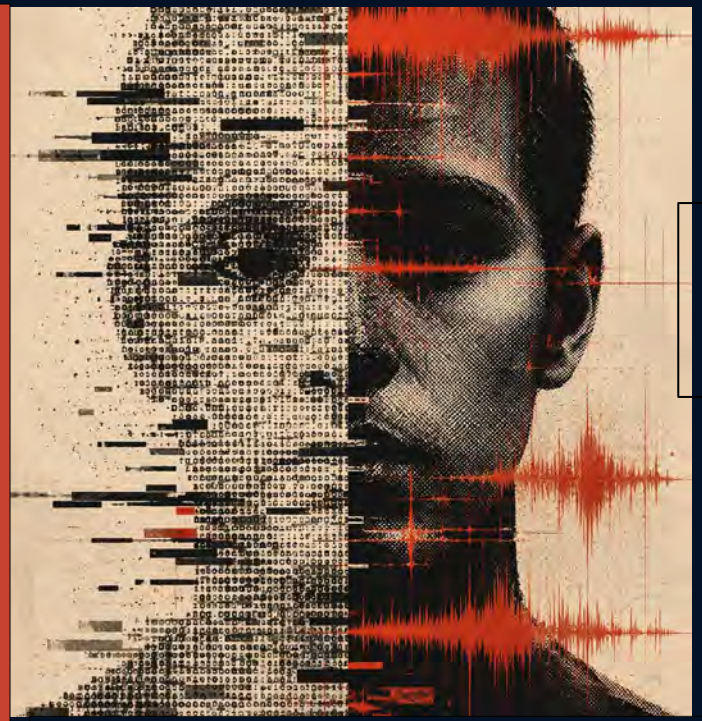
MONEY	fraud, extortion, interruption
DATA	privacy, privilege, trade secrets
DUTIES	notice, ethics, contracts, regulators
PEOPLE	clients, employees, victims, witnesses



Sources: FBI IC3 2025 Report

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

GenAI makes familiar fraud faster, cheaper, and more convincing.



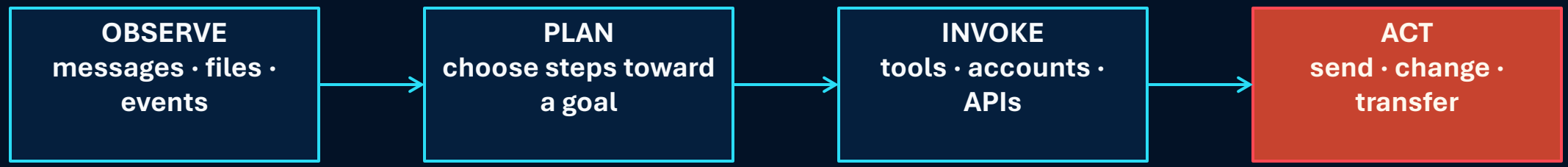
QUALITY	plausible language, cloned voices, synthetic evidence
SPEED	rapid testing, translation, personalization
SCALE	many targets, many variants, low marginal cost
$893M	reported losses tied to 22,364 AI-related IC3 complaints in 2025

For lawyers using AI, traditional duties including competence, confidentiality,communication, supervision, and reasonable fees apply.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Agentic AI moves from content to action.

GenAI answers. Agents can decide, call tools, and change the environment.



The legal question shifts from "What did the model say?" to "What did the system do—and under whose authority?"

PRIVILEGE CREEP

more access than required

INDIRECT INJECTION

untrusted content redirects the agent

OBSCURE RECORDS

actions outpace auditability

Sources: CISA Agentic AI Guidance

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Cyberinsurance creates response infrastructure not just reimbursement.

FIRST-PARTY

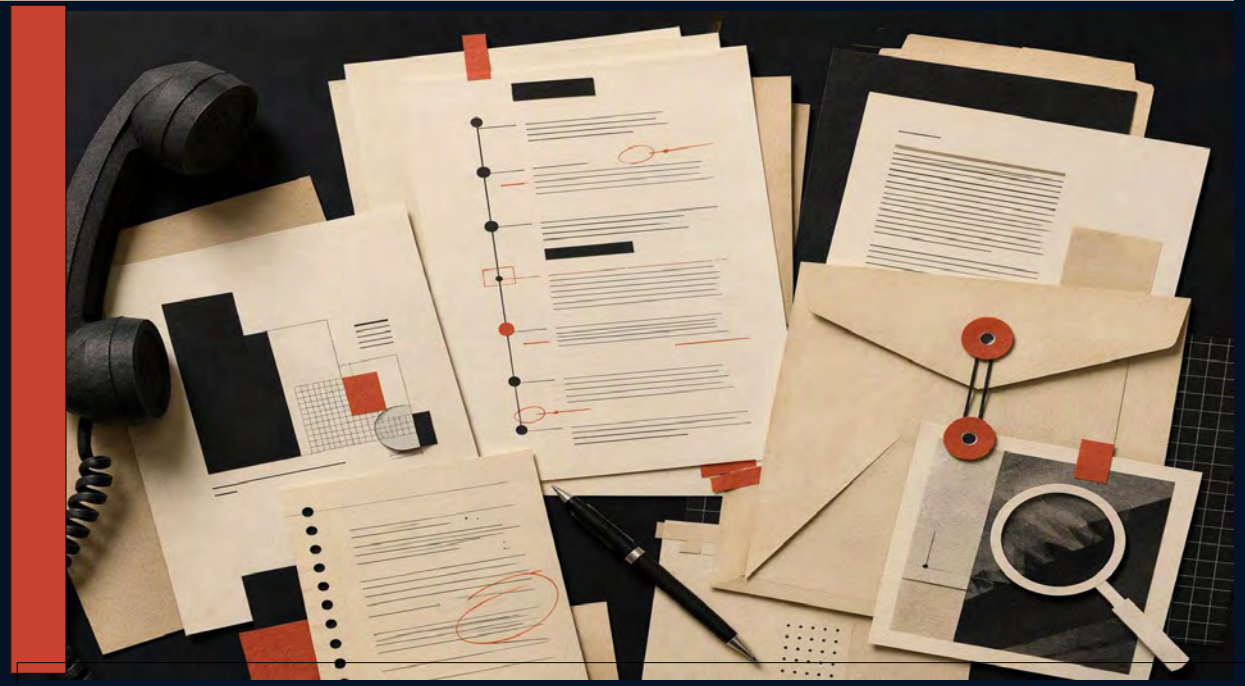
The insured's own loss

forensics · breach counsel · notification
recovery · interruption · crisis response
extortion or fraud, if covered

THIRD-PARTY

Liability to others

defense · settlements · regulatory response
and other liabilities, subject to wording

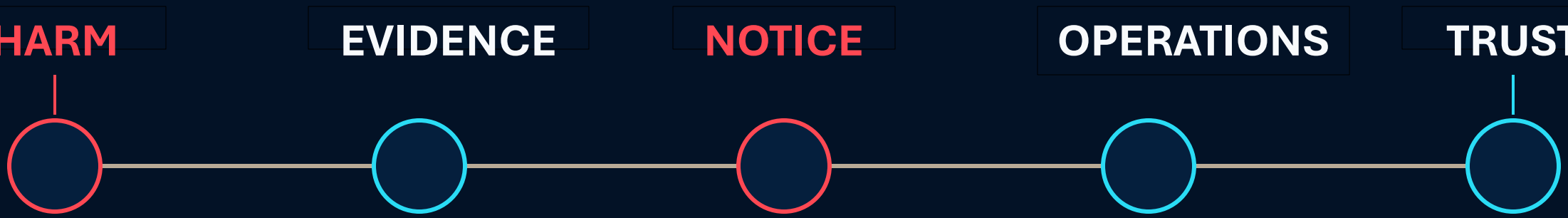


A policy may supply a hotline, panel counsel, forensic firm, and approval path.

Sources: NAIC Cybersecurity

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

When prevention fails, five clocks start.



Stop loss, access, and spread

Preserve volatile facts and records

Map legal, contractual, and policy triggers

Restore safely, not merely quickly

Communicate without outrunning the facts

The clocks do not run in sequence.

Early choices often affect several clocks at the same time.

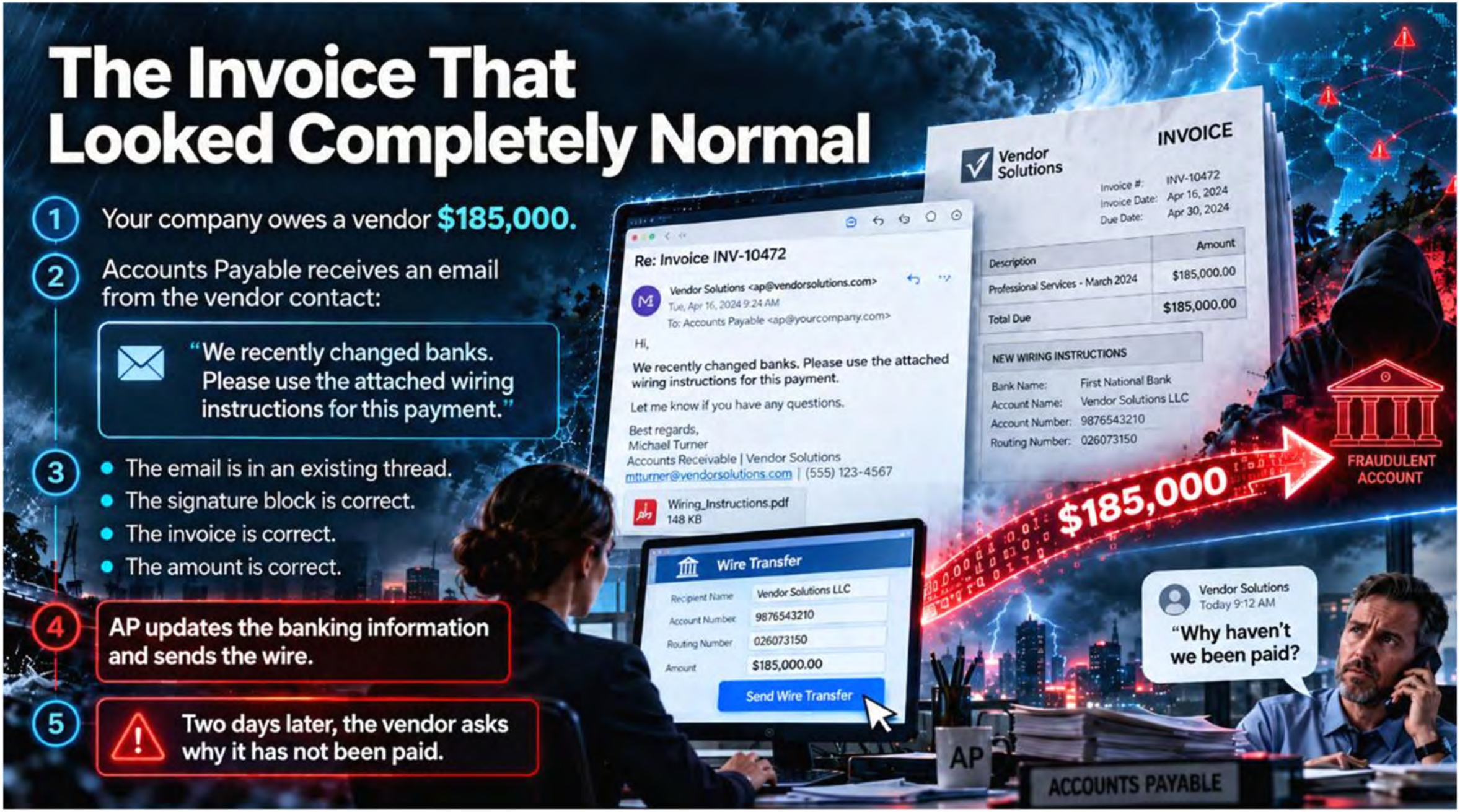
Sources: NIST SP 800-61r3 • FTC Breach Guide

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The Invoice That Looked Completely Normal



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

What Actually Happened

Business Email Compromise often uses real accounts, real threads, and real payment activity.

1 Attacker gets access



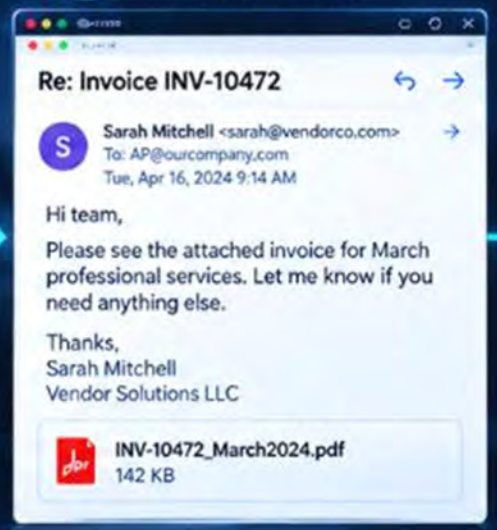
Attacker compromises a real employee account (e.g., through phishing or stolen credentials).

2 Watches the mailbox



Attacker quietly monitors the mailbox, reading real conversations about invoices and payments.

3 Waits for an invoice



Attacker waits for a legitimate invoice to be sent in an existing billing conversation.

4 Changes payment instructions



Attacker replies within the real thread, providing updated (fraudulent) payment instructions that look legitimate.

5 Money leaves



The company sends the payment to the attacker's account, and the money leaves the organization.

Teaching Point

BEC is often not a laughably fake email. Criminals compromise or imitate legitimate accounts, study billing conversations, and insert themselves into real payment activity.

$55.5 billion

reported exposed losses worldwide from Oct. 2013 through Dec. 2023, according to the FBI.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

What Actually Happened

A data breach is usually a chain of events—not a single moment.



Day 0
Employee enters credentials

Day 1
Attacker logs in

Day 3
Mailbox/cloud access expands

Day 8
Sensitive files located

Day 12
Data downloaded

Day 21
Organization discovers the breach

Phishing link → credentials stolen → attacker logs in → establishes persistence → searches systems → exfiltrates data → breach discovered

TEACHING POINT

"The breach did not happen when the company discovered it. The breach started weeks earlier."

Breaches often involve dwell time—the attacker gets in, stays in, learns the environment, collects data, and leaves before anyone realizes it.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

What Actually Happened

Unauthorized access often spreads through the environment before anyone understands its scope.



TEACHING POINT

Unauthorized access tells you someone got in. It does not yet tell you what they saw, changed, or took.

The investigation has to answer three different questions: Where did they go? What could they access? What did they actually do?

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The Customer Who Wasn't the Customer

1. A longtime customer calls support and says she cannot log in to her account.
2. Her password has been changed.
3. Her recovery email and phone number have also been changed.
4. Support sees several recent logins using the correct username and password.
5. The account shows no failed-login spike and no obvious malware activity.
6. Two recent transactions were completed using the customer's saved payment information.
7. Support resets the account and restores access to the customer.
8. The next morning, the customer reports that the attacker got back in again.



Account details changed

Password	Changed 2 days ago
Recovery Email	Changed 2 days ago
Phone Number	Changed 2 days ago

Recent successful logins

Feb 13, 2024	10:24 PM	Chicago, IL, USA
Feb 13, 2024	6:11 PM	New York, NY, USA
Feb 12, 2024	9:03 PM	Chicago, IL, USA
Feb 12, 2024	2:17 PM	Seattle, WA, USA

Recent transactions

Feb 13, 2024 Electronics Store	$129.00	Completed
Feb 12, 2024 Online Marketplace	$89.99	Completed

Attacker got back in again

The next morning, the customer reports that the attacker got back in again.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

What Actually Happened

Control of the account changed hands.



Timeline

Day 0 — Credentials stolen

Day 1 — Attacker logs in successfully

Day 1 — Email and phone recovery settings changed

Day 2 — Saved payment method used

Day 3 — Customer discovers account lockout

Day 3 — Support resets password

Day 4 — Attacker re-enters using retained session / recovery access

TEACHING POINT

Account takeover is not just about knowing the password. It is about gaining control of the account's identity, recovery mechanisms, and trusted sessions.

Resetting the password may not be enough if the attacker changed recovery information, enrolled a new MFA method, created forwarding rules, generated API tokens, or retained an authenticated session.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

1. Your firm uses a cloud-based document management provider.
2. The vendor stores client files, matter information, and documents exchanged with opposing counsel.
3. On Monday morning, the vendor sends a notice:

> **"We recently identified unauthorized access to our environment."**

4. The vendor says its investigation is ongoing.
5. It cannot yet say which customers were affected.
6. It cannot confirm whether files were viewed or downloaded.
7. Your firm's own systems appear normal.
8. **Three days later, the vendor confirms that your firm's tenant was accessed.**
   Client files may have been involved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

What Actually Happened

Law firm uploads client data



Client files, matter information, and documents shared with opposing counsel.

Vendor stores it



Cloud document management provider

Vendor environment compromised



Attacker gains access to the vendor's systems

Attacker accesses shared platform



Attacker moves within the vendor's environment

Law firm's account confirmed affected



Attacker identifies and accesses the law firm's data

Scope investigated



Vendor investigates what was accessed (e.g., viewed or downloaded).

Lawyer evaluates client impact



Determine what client information was involved and next steps.

Day 0
Vendor compromise begins

Day 5
Vendor detects suspicious activity

Day 7
Vendor notifies law firm

Day 10
Law firm's account confirmed affected

Day 12
Potential client files identified

Day 14+
Lawyer determines notification and response obligations



Outsourcing the technology does not outsource the lawyer's responsibility for client information.

The lawyer still needs to understand what happened, what client information was involved, what the vendor is doing, and whether clients or others must be notified.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Stabilize facts -don’t freeze the response.

RECOGNIZE What happened or may still be happening?

CONTAIN What must stop now, without destroying evidence?

PRESERVE Which systems, records, decisions, and communications matter?

ESCALATE Which legal, technical, financial, and insurance professionals?

NOTIFY Who must know, by when, through which channel?

RECOVER How do we restore safely and learn from the incident?

Calm is not delay.

It is disciplined sequencing under uncertainty.

NEXT

Recognize and contain the incident while preserving the choices that follow.

Sources: NIST SP 800-61r3 • FTC Breach Guide

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Assessment starts with a fact pattern, not a theory.

BUILD THE INCIDENT LEDGER

One time zone. One owner. Every entry time-stamped.

Record who observed what, when it was observed, and where the supporting artifact lives.

KNOWN

Directly observed or verified

logs, alerts, transactions, witness account

SUSPECTED

Plausible, not yet confirmed

possible vector, likely persistence, tentative attribution

UNKNOWN

Material question still open

entry time, data accessed, actor present, scope

Do not turn a hypothesis into a fact by repeating it.

Sources: NIST SP 800-61r3 • CISA Incident Guidance

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Scope the incident across five dimensions.

SCOPE

Ask the same questions for each dimension:

What is affected?
What is not affected?
What remains untested?

Reassess as evidence changes.

SYSTEMS	Devices: cloud, email, applications, backups
IDENTITIES	Users, admin, service accounts, credentials
DATA	Type, sensitivity, volume, access, exfiltration
PARTIES	Clients, employees, vendors, victims, regulators
TIME + IMPACT	first known activity, persistence, outage, money

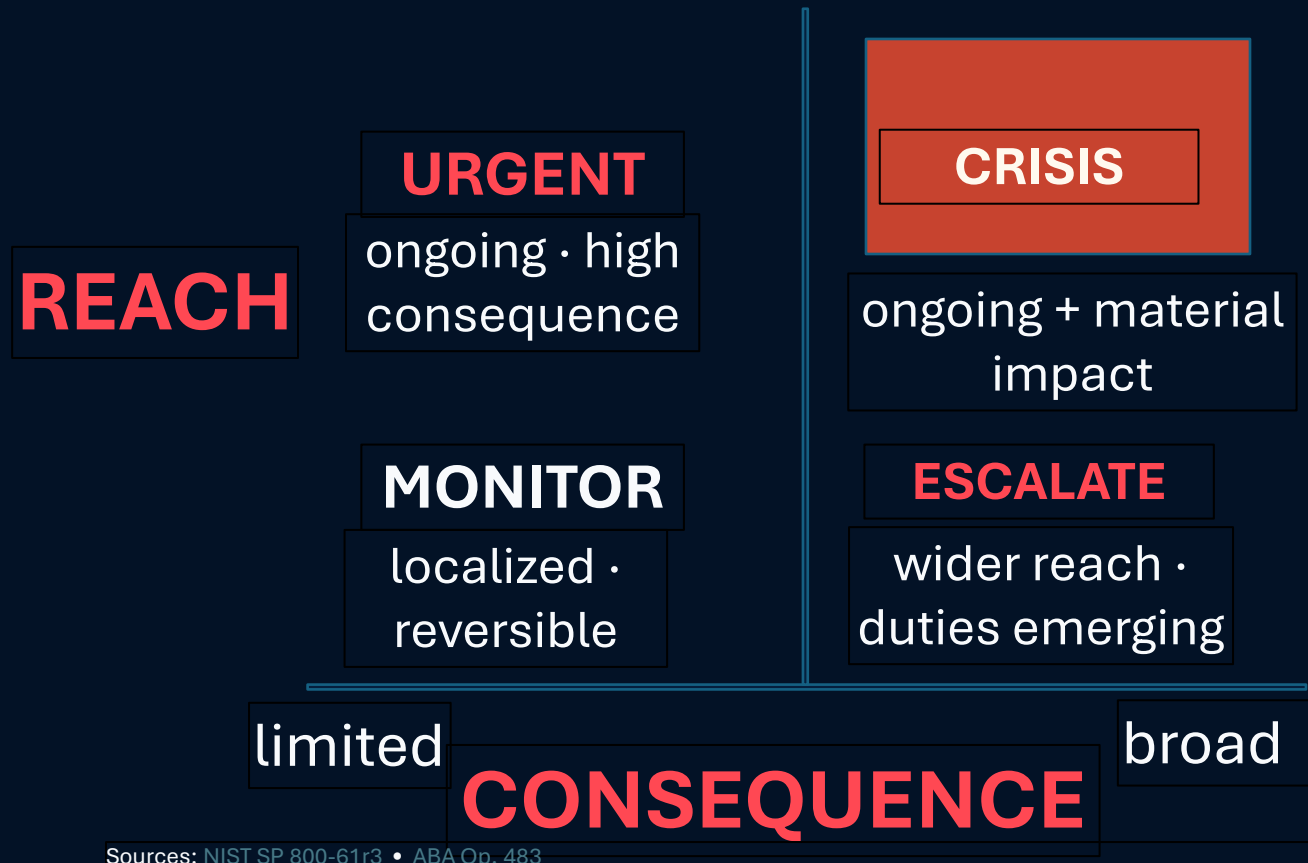
Ongoing?

Treat continued access or loss as a live-response issue.

Sources: FTC Breach Guide • NIST SP 800-61r3

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Severity means a decision about reach, consequence, and triggers.



TRIGGERS TO TEST NOW

Legal + regulatory	breach laws · sector rules · contractual notice
Ethical	client information · funds · competence · communication
Insurance	notice · consent · panel vendors · cooperation
Operational	safety · outage · integrity · financial loss
External	law enforcement · affected parties · public disclosure

Severity changes as facts change.

Sources: NIST SP 800-61r3 • ABA Op. 483

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The First Moves

Immediate containment after an incident



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Contain ≠ Destroy

Isolate without wiping evidence.

DON'T
Destroying evidence



Do not wipe devices



Do not delete logs or files



Do not reimage or factory reset

DO
Contain and preserve



Isolate affected systems



Preserve logs and messages



Capture what happened first
(logs, screenshots, emails, system info)

Stop the threat. Preserve the proof.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Containment Looks Different

The right first move depends on what happened.

01



Business Email Compromise

Call the bank.
Try to stop or recall the wire.

02



Data Breach

Disable the account.
Terminate sessions.
Isolate impacted systems.

03



Unauthorized Access

Cut off access.
Disable accounts.
Contain the spread.

04



Account Takeover

Reset credentials.
Revoke sessions.
Restore MFA and recovery controls.

05

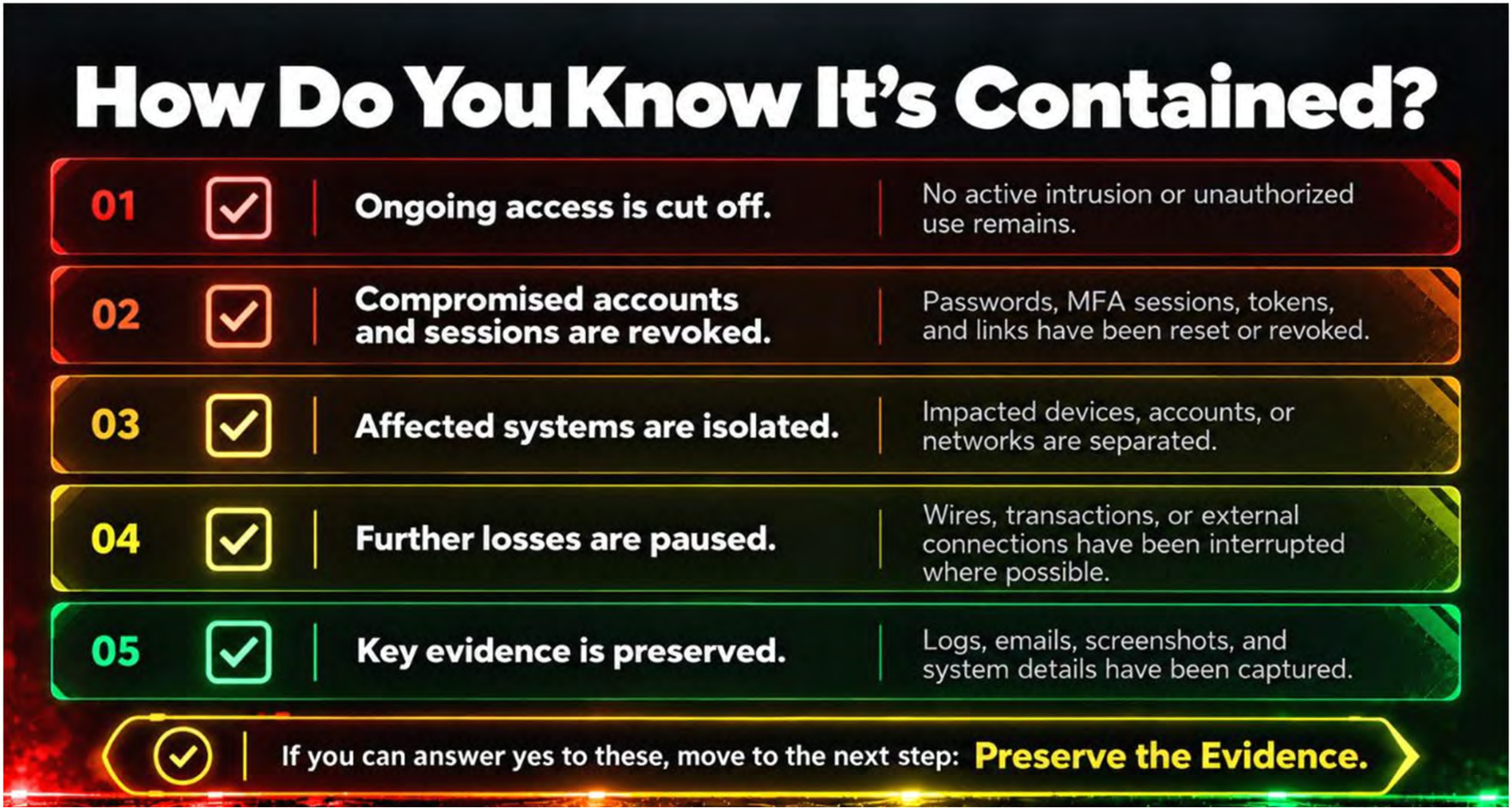


Third-Party Breach

Rotate credentials and tokens.
Restrict vendor connections.
Limit exposure.

Containment is not one-size-fits-all.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Preserve first; investigate from copies.

THE PRESERVATION RULE

Do not improve the scene before you preserve it.

Containment can change timestamps, erase memory, rotate logs, or overwrite artifacts. Coordinate the least-destructive action with qualified forensic personnel.

FREEZE	retention, deletion, rotation, and reimaging
CAPTURE	volatile data, systems, cloud records, and context
SEPARATE	master evidence from working copies and remediation

Preservation is a decision discipline, not a single tool.

Sources: NIST SP 800-86 • NIST IR 8387 • FTC Breach Guide

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Volatile evidence disappears first.

COLLECT IN AN ORDER THAT MATCHES DECAY

LIVE MEMORY processes · connections · encryption keys · logged-in sessions

TRANSIENT TELEMETRY EDR state · network flows · active alerts · short-retention logs

SYSTEM + CLOUD RECORDS event logs · audit trails · identity activity · mailbox access

STORAGE + DEVICES forensic images · files · mobile devices · removable media

EXTERNAL RECORDS provider logs · bank records · vendor data · law-enforcement returns

POWER OFF? Ask forensics first.

Sources: NIST SP 800-86 • NIST SP 800-101r1

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Collect broadly by source and scope.

An incident is rarely contained in one device.

ENDPOINTS	IDENTITY + CLOUD	NETWORK	COMMS	MONEY + THIRD PARTIES
disk image memory EDR artifacts	sign-ins audit events mail and sharing	firewall · DNS VPN · proxy flow or packet data	email · chat voice records tickets and notes	transactions vendor logs provider records

Preserve metadata with content: **time zone · tenant/account · collector · query/export method · retention limit**

For cloud and SaaS evidence, export before retention, windows, or account changes erase context.

Sources: NIST SP 800-86 • CISA Incident Guidance

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Repeatable handling proves Integrity.

MASTER

write-protected
access restricted
hash recorded

WORKING COPY

analysis occurs here
derivatives identified
changes documented

COLLECT	who · what · where · when · how
PROTECT	write blocker or equivalent controls
VERIFY	cryptographic hash at acquisition and transfer
TRACK	every handler, transfer, date/time, and purpose
STORE	encrypted, access-controlled, retained under policy/holder

Sources: NIST IR 8387 • NIST SP 800-86

Chain of custody explains evidence's life not just its location.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Legal hold and forensic preservation solve different problems.

FORENSIC PRESERVATION

Reconstruct the incident

Capture systems and artifacts in a defensible manner. Preserve original evidence, context, integrity, and handling history.

Typical owner: incident response + forensic specialist

LEGAL HOLD / ESI PRESERVATION

Protect relevant information from loss

When litigation is reasonably anticipated, identify custodians and systems, suspend routine destruction as appropriate, and monitor compliance.

Typical owner: counsel + records / business stakeholders

COORDINATE BOTH TRACKS

Scope, retention, vendors, reporting lines, and distribution. Counsel involvement alone does not guarantee privilege or work-product protection.

Sources: FRCP 37(e) • NIST IR 8387 • Clark Hill decision

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Lawyers fill 2 seats in incident rooms

TARGET CUSTODIAN

Law firms hold funds, credentials, strategy, regulated data, and privileged communications.

The firm may itself be a victim, a regulated entity, an employer, and a fiduciary.

COUNSEL + COORDINATOR

Counsel helps structure the inquiry, preserve privilege where available, identify duties, and coordinate specialists.

Competence Confidentiality Communication

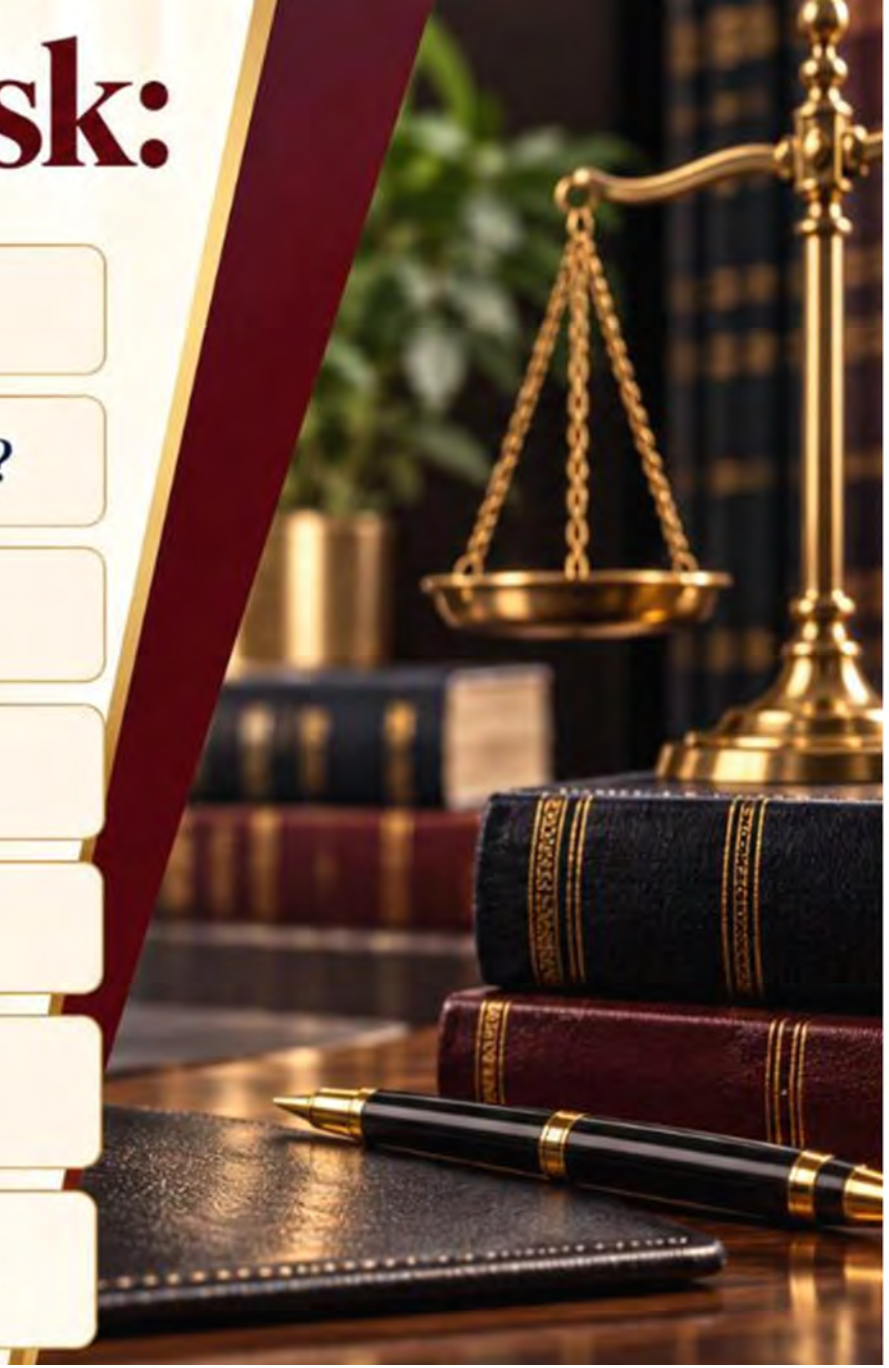
Controlling law and professional rules vary by jurisdiction.

Sources: ABA Formal Op. 483

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Before You Move On, Ask:

- ☐ Is client information involved?
- ☐ Has the client's representation been materially affected?
- ☐ Does the client need to know now?
- ☐ Are client or third-party funds involved?
- ☐ Do we need outside technical or breach counsel?
- ☐ Are employees or vendors involved who require supervision?
- ☐ Are there contractual, statutory, regulatory, or court-imposed notice obligations beyond the ethics rules?



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

First calls can preserve or complicate coverage.

NOTICE Use the policy's channel; do not assume the broker is enough.

CONSENT Check approval requirements before material spend or commitments.

VENDORS Confirm panel counsel, forensics, negotiators, and restoration firms.

PRESERVE Keep logs, invoices, decisions, communications, and proof of loss.

COOPERATE Coordinate facts and updates without speculating beyond evidence.

PAUSE BEFORE

Paying
Promising
Publishing
Replacing

The policy should set timing, consent, and documentation requirements.

Rules and requirements vary by jurisdiction and coverage.

Sources: NAIC Cybersecurity

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

For stolen funds, minutes can determine recovery.

CALL THE ORIGINATING FINANCIAL INSTITUTION NOW

— Request a recall or reversal and ask whether a hold can be placed on the receiving account.

— Ask what bank-specific documents are required—including a Hold Harmless Letter or Letter of Indemnity.

— Escalate to the fraud or wire-transfer desk; obtain a case number and named contact.

Sources: FBI IC3 BEC Guidance • IC3 Financial Fraud Kill Chain

GIVE THEM A CLEAN FACT PACK

transaction ID, amount, currency, date/time

originating and receiving account details

beneficiary name and bank routing information

how the payment instruction was received

your callback number and law-enforcement report

Then file a detailed IC3 complaint with complete banking information.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Notify the insurer before coverage choices harden.

USE THE POLICY'S CHANNEL

NOTICE Use the required address, portal, hotline, or broker path.

CONSENT Ask before material spend, commitments, or admissions.

PANEL Confirm approved counsel, forensics, restoration, and PR vendors.

DOCUMENT Keep notices, approvals, invoices, decisions, and updates.

ASK FOR IN WRITING

— Claim or incident number and assigned adjuster.

— Acknowledgment that notice was received.

— Any reservation of rights or coverage questions.

— Approved vendors, rates, scope, and reporting cadence.

— Instructions for ransom, law enforcement, and communications.

Policy language controls, not industry custom

Sources: NAIC Cybersecurity Resources • FTC Breach Guide

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Bring in breach counsel when decisions create exposure.

ENGAGE EARLY WHEN THE INCIDENT INVOLVES

— Sensitive, regulated, or client information.

— Material financial loss, extortion, or business interruption.

— Multiple jurisdictions, vendors, or contractual notice duties.

— Potential regulator, law-enforcement, or public-company reporting.

COUNSEL'S JOB

Set legal questions, decision rights, reporting lines, and communication discipline.

PRIVILEGE IS NOT A LABEL

Define the purpose of each workstream.

LEGAL ADVICE	Counsel-directed analysis tied to legal questions.
BUSINESS RESPONSE	Operational facts and remediation may remain discoverable.
DISTRIBUTION	Keep factual reports and legal advice on deliberate paths.

Counsel involvement alone does not guarantee protection.

Sources: FTC Breach Guide • ABA Formal Op. 483 • Clark Hill decision

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Required notice starts with a trigger matrix.

DON'T START WITH A FORM LETTER

Map facts to each rule

ENTITY	Whose data—and where do they live?
DATA	What data, sensitivity, and encryption?
PEOPLE	Which organization and legal role?
TRIGGER	Acquisition, access, materiality, or harm?
CLOCK	When did discovery or materiality occur?
RECIPIENT	~~Individuals, AGs, regulators, clients~~, partners?

Sources: 45 CFR §164.404 • SEC Cyber Incident Disclosure Guide

REPRESENTATIVE CLOCKS

HIPAA	Without unreasonable delay; no later than 60 calendar days after discovery for individual notice.
SEC	Form 8-K generally due within four business days after a registrant determines an incident is material.
OTHER	State, sector, contract, client, insurer, and law-enforcement provisions may add different or shorter clocks.

Examples only; apply current controlling law and facts.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Each contact needs a purpose and owner.

A PRACTICAL CALL SHEET

CONTACT	PURPOSE	OWNER / RECORD
Bank / payment provider	Recall, freeze, trace	Finance lead · case number
Cyber insurer	Notice, consent, resources	Risk lead · written acknowledgment
Breach counsel	Legal analysis, roles, notice map	Executive sponsor · engagement scope
Forensics / IT	Contain, preserve, determine facts	IR lead · evidence and decision log
Law enforcement	Recovery, threat, extortion coordination	Counsel / security · report number
Regulators / people / partners	Comply and communicate accurately	Counsel / comms · approved notice

Before every contact

Confirm purpose · authority · known facts · open questions · requested action · owner · record of the response

Sources: FTC Breach Guide • FBI IC3 BEC Guidance • NIST SP 800-61r3

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Contact is a sequence not a blast email.

THE CONTACT CLOCK



BANK / PAYMENT

Stop or recall funds.

INSURER

Protect notice and consent.

BREACH COUNSEL

Structure decisions and roles.

NOTICES

Send accurate, lawful notices.

Parallel work is normal. Premature external notice is not.

Sources: FTC Breach Guide • FBI IC3 BEC Guidance

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Recovery Is More Than Turning the Systems Back On

Recovery is not “the computers work again.”
Recovery means restoring operations safely, reducing continuing harm, learning from the incident, and rebuilding trust.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

RECOVER SAFELY

Getting systems back online is not the same as recovering.



RECOVERY MEANS THEY ARE BACK ONLINE SAFELY.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Restore Carefully, Not Quickly



Do not restore a compromised environment into the same conditions that allowed the incident.

1. **Validate Containment**
   Confirm the threat has been contained and is no longer active.
2. **Restore from Known-Good Backups**
   Use clean, known-good backups. Verify integrity before restoring.
3. **Patch and Close Gaps**
   Fix the vulnerability that allowed entry. Apply patches and security updates.
4. **Reset Credentials and Access**
   Reset compromised passwords, tokens, keys, and sessions.
5. **Validate Configurations**
   Review and confirm security configurations before reconnecting systems.
6. **Bring Systems Back in Order**
   Restore critical functions first, in a controlled sequence.
7. **Monitor Continuously**
   Watch for signs of persistence or reinfection after restoration.

"Recovery without remediation **is just resetting the clock for the attacker.**"

Business Continuity
Resume critical operations to keep the business running. May occur before every

Full Recovery
All systems restored, fully secured, and returned to normal

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Follow the Money



Now that the immediate response is underway, recovery means determining the full financial impact and watching for continuing activity.

Monitor All Accounts

Review affected bank, credit, trust, and payment accounts.

Look for Further Activity

Watch for additional unauthorized transactions and unusual or suspicious activity over time.

Check for Changes

Review any changes to payment instructions, account details, vendor information, or other financial settings.

Consider Identity Protection

If personal information was exposed, consider credit monitoring and other identity-protection measures for affected individuals.

Track the Full Financial Impact

Document recovered amounts, unrecovered losses, fees, remediation costs, and business interruption.

EARLIER:
Stop the transaction.

NOW:
Determine what the incident ultimately cost.

Build Your Damages Record

Keep a clear record of all financial impacts, including direct losses, response costs, and business interruption.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Learn From It

Turn the incident into a better response next time.



Document the timeline, root cause, affected systems, key decisions, costs, and corrective actions. Assign an owner and deadline to each change.

"If the response plan looks exactly the same after the incident, you probably did not learn enough from it."

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Rebuild Trust

Communicate clearly. Mitigate losses. Document the response.



Communicate Accurately and Consistently

- Communicate with clients, customers, employees, counterparties, insurers, regulators, and others who actually need information.
- Do not speculate before facts are known.
- Do not minimize what happened.
- Correct inaccurate statements as facts develop.
- Give affected people practical next steps.
- Keep messaging coordinated across legal, security, leadership, insurance, and communications.
- Document mitigation efforts.

Mitigate the Damage

- Recover funds where possible.
- Pursue available insurance coverage.
- Enforce contractual rights against responsible vendors where appropriate.
- Preserve claims against third parties.
- Offer reasonable protective measures to affected individuals.
- Reduce business interruption.
- Document reasonable steps taken to prevent additional loss.

Why the Record Matters

Mitigation starts during the incident, but the record you build afterward may matter months or years later when insurers, regulators, clients, or litigants ask whether the organization responded reasonably.

Trust is rebuilt through accurate communication, practical support, and documented action.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Recovery Checklist



- [ ] Systems restored safely
- [ ] Continued monitoring in place
- [ ] Financial losses identified and monitored
- [ ] Incident timeline documented
- [ ] Root cause addressed
- [ ] Response plan updated
- [ ] Clients/customers appropriately supported
- [ ] Insurance and third-party recovery pursued
- [ ] Corrective actions assigned and tracked

> *"The goal is not to return to where you were before the incident.*
> ***The goal is to come back stronger than you were before it."***

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

RECOMMENDED READING

Unlocking the Future

by Jeffrey Allen and Ashley Hallene (2025). Published by the ABA.

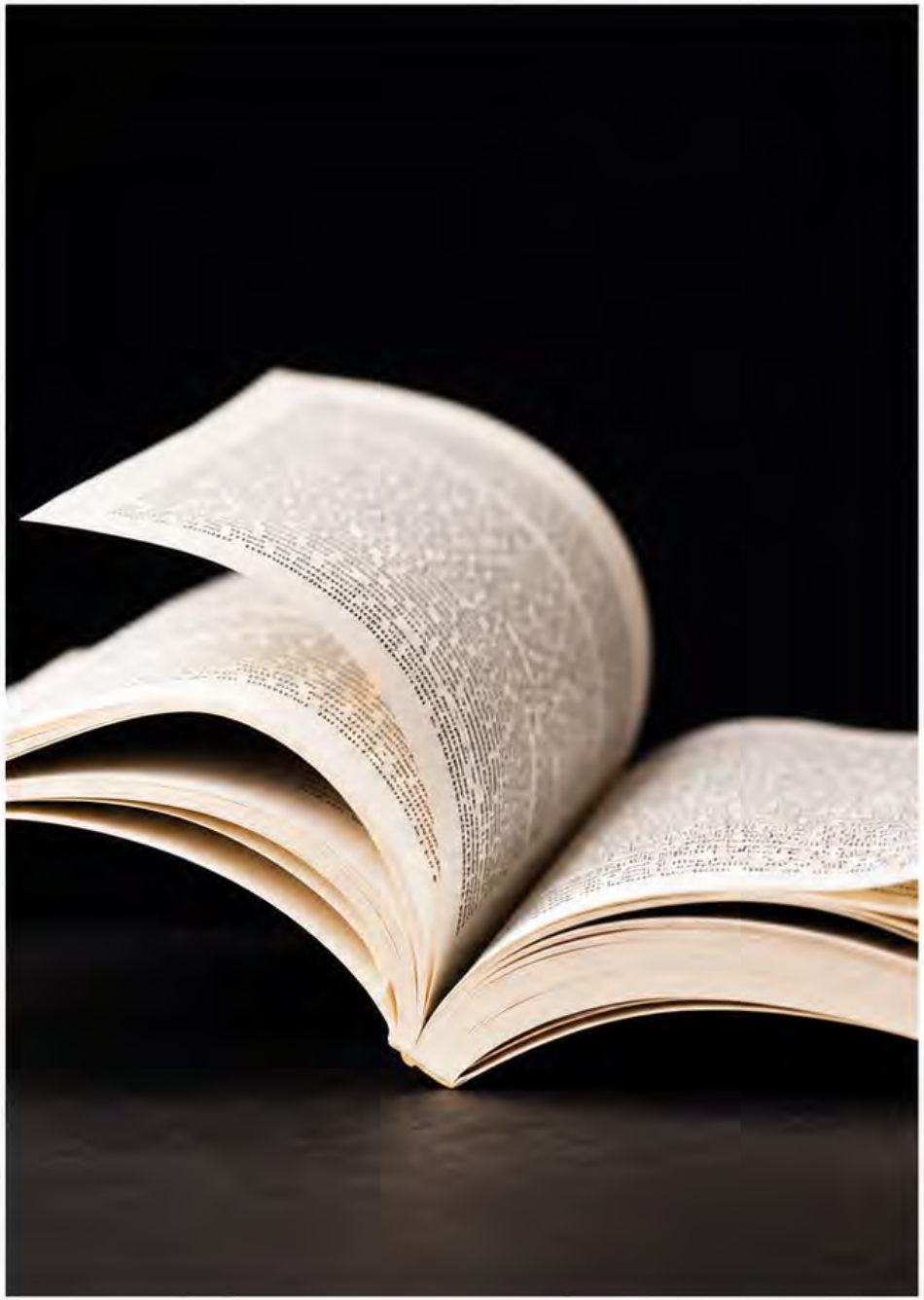
The ABA Cybersecurity Handbook (4th ed.)

(2026), edited by Jeffrey Allen and Candace Jones. Jeff and Ashley authored portions of the book. Published by the ABA.

Look for:

The Scams and Cybercrimes Survival Guide Volumes 1 and 2

(Vol. 1 due out later in 2026; Vol. 2 in early 2027), edited by Jeffrey Allen and Ashley Hallene, who also contributed to the book as authors. Published by the ABA.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

IF YOU HAVE QUESTIONS--

--We Have Answers

(But not necessarily to your questions).



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The Lens Through Which We View Everything

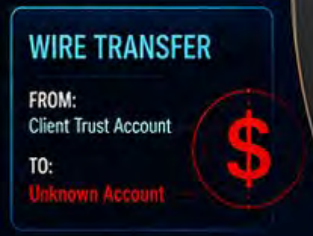
ABA MODEL RULE 1.1 COMMENT 8

> "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the **benefits and risks** associated with **relevant technology.**"

Competent representation in the digital age requires understanding the **benefits and risks** of relevant technology.



















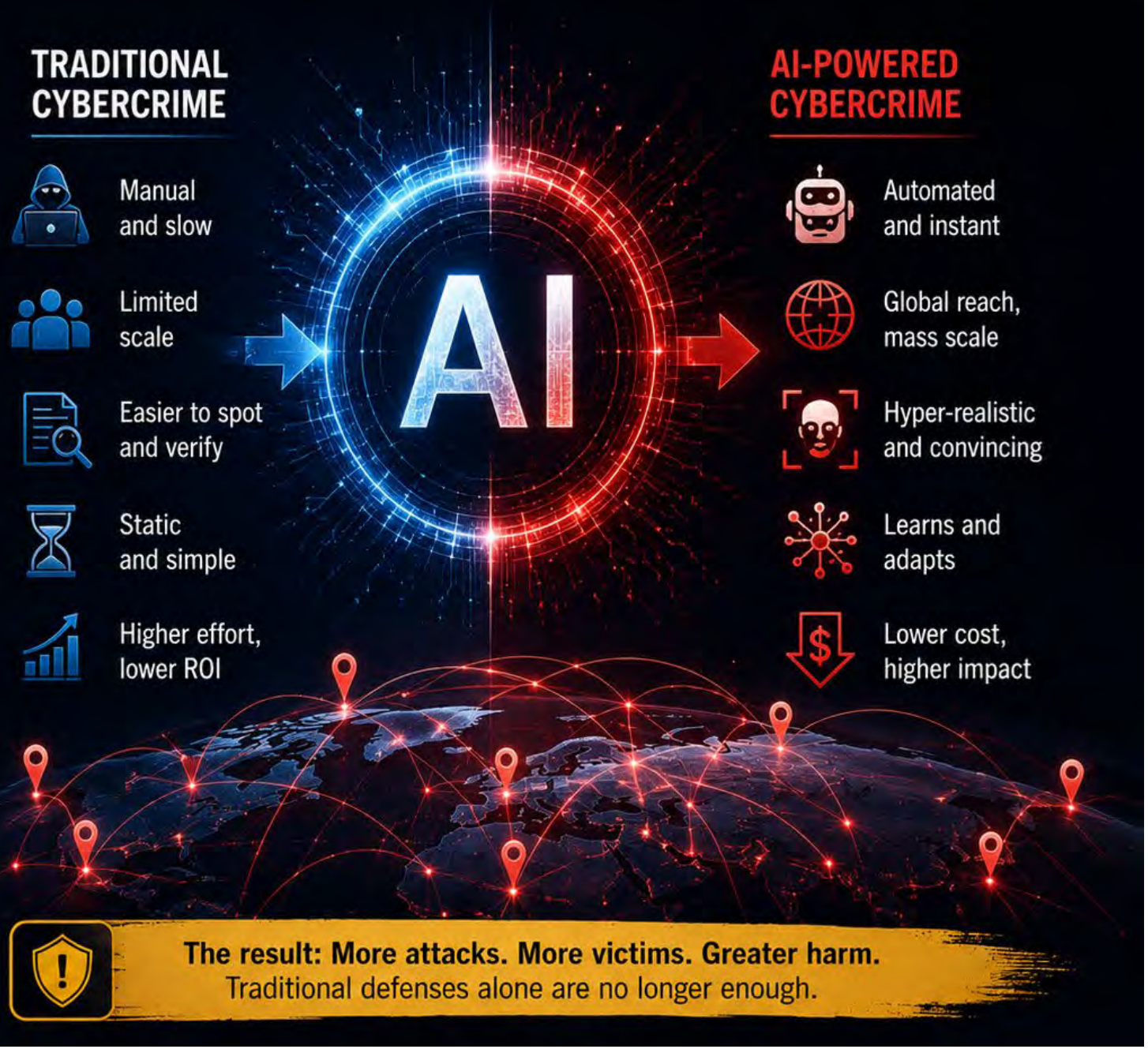
Every topic in this program—from phishing and ransomware to deepfakes, AI, and client confidentiality—
is viewed through this ethical obligation.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

WHY AI CHANGES THE THREAT LANDSCAPE

Artificial Intelligence supercharges every stage of the attack—making scams **faster, cheaper,** and **far more convincing.**

- **SPEED:** AI automates research, targeting, and execution in minutes.
- **SCALE:** Attackers can reach thousands—or millions—simultaneously.
- **REALISM:** Deepfakes and synthetic content create unprecedented believability.
- **ADAPTABILITY:** AI learns, adapts, and evades detection in real time.
- **LOWER BARRIERS, HIGHER IMPACT:** Sophisticated attacks are now accessible to anyone.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

NEW TOOLS. NEW DECEPTIONS.

AI gives scammers powerful new abilities—and makes trust the biggest target of all.

THEY CAN PRETEND TO BE ANYONE.
Voices, faces, names, and identities are no longer reliable.

THEY CAN AUTOMATE EVERYTHING.
Research, outreach, persuasion, and follow-up—24/7.

THEY CAN PERSONALIZE AT SCALE.
Every message, every call, every detail—made to fool you.

THEY CAN HIT ANYONE, ANYWHERE.
No borders. No limits. No safe zone.



IF YOU CAN'T TRUST WHAT YOU SEE OR HEAR, YOU CAN'T PROTECT WHAT MATTERS.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

SOCIAL ENGINEERING AT SCALE

AI doesn't just help scammers write better messages — it helps them reach millions with the personal touch of one.

MASS REACH
AI finds and targets thousands—or millions—of people across email, social media, and messaging apps.

PERSONALIZED AT SCALE
AI tailors every message using victim data, making it look personal and trustworthy.

AUTOMATED & 24/7
AI agents operate around the clock, adapting in real time and never taking a day off.

HIGHER SUCCESS
More responses. More clicks. More compromise. More money.

HOW AI SUPERCHARGES SOCIAL ENGINEERING

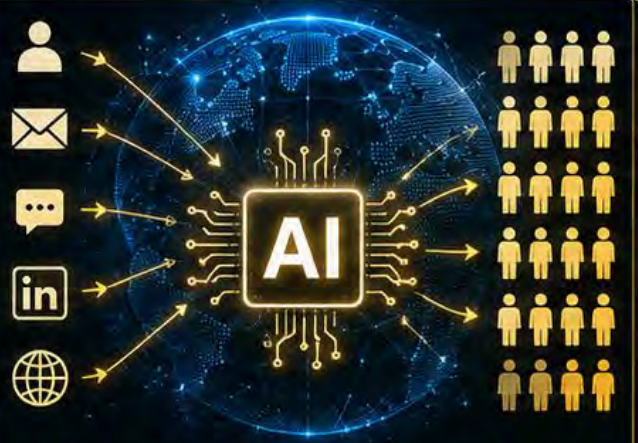
COLLECT DATA — Public records, social media, breaches, websites, and more

ANALYZE & PROFILE — AI builds detailed profiles and predicts what will work

CRAFT MESSAGE — AI writes messages tailored to each individual

DELIVER ANYWHERE — Email, text, DM, phone, or chat — all at once

MEASURE & ADAPT — AI learns what gets results and keeps improving

THE OLD WAY	THE NEW WAY	THE RESULT
FEW TARGETS		MASS TARGETS
MANUAL EFFORT		AUTOMATED EFFORT
LIMITED TIME		ALL THE TIME
LOW SUCCESS		HIGH SUCCESS
HOURS OR DAYS TO COMPROMISE A FEW PEOPLE	AI FINDS. AI WRITES. AI DELIVERS. AI OPTIMIZES. SECONDS TO REACH THOUSANDS — OR MILLIONS	MASSIVE IMPACT. MAXIMUM PROFIT.

COMMON AI-POWERED SOCIAL ENGINEERING TACTICS

PHISHING EMAILS
Convincing emails that look real and reference real details.

SMISHING TEXTS
Text messages that create urgency and trick you into clicking.

FAKE PROFILES
AI creates realistic identities on social media to build trust over time.

BAITING & PRETEXTING
AI crafts believable stories to get information or bypass security.

QUID PRO QUO SCAMS
Fake offers, rewards, or opportunities used to exploit trust.

THE SCALE IS NEW. THE DAMAGE IS REAL.

THINK BEFORE YOU CLICK. VERIFY BEFORE YOU TRUST.

Be skeptical. Check the source. Use a second channel. Report suspicious activity.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

DEEPFAKES

SYNTHETIC VIDEO & IMAGES

AI creates what never happened—and makes it look completely **real.**

HYPER-REALISTIC
Advanced AI models replicate faces, voices, and emotions with stunning accuracy.

VOICE CLONING
AI can clone a voice from only seconds of audio.

LOW COST & EASY ACCESS
Powerful tools are cheap and widely available online.

RAPID IMPROVEMENT
AI models keep getting better, making detection even more difficult.

GLOBAL REACH
Fake content can be created and spread anywhere in the world instantly.

DETECTION IS GETTING HARDER
Detection tools help—but human skepticism and verification are still essential.

HOW DEEPFAKES ARE MADE

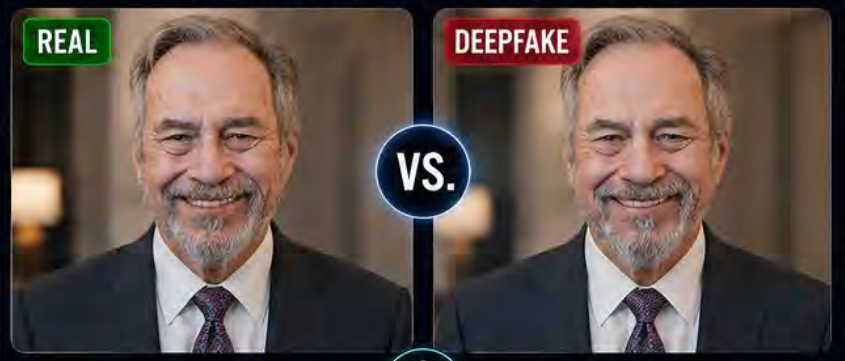
DATA IN
Photos, videos, and audio collected

AI MODEL
Neural networks learn facial moves, voice, and patterns

SYNTHESIS
AI generates realistic new content

OUTPUT
Convincing fake video, image, or audio

REAL OR FAKE? IT'S HARD TO TELL.



"Wire $487,500 to our new closing account."

It may look real. It may sound real. It may even feel real. It may not be.

WHAT CAN BE FAKED

- SPEECHES
- IDENTITY
- EVENTS
- EVIDENCE

HOW IT'S USED

SOCIAL ENGINEERING
Impersonate executives, family members, or trusted contacts.

FINANCIAL FRAUD
Authorize fake payments, steal funds, or manipulate markets.

DISINFORMATION
Spread false narratives, damage reputations, or influence elections.

BLACKMAIL & EXTORTION
Create compromising content that never actually happened.

KEY TAKEAWAY

If you can see it, hear it, or read it—don't assume it's real. **Verify first.**

HOW TO PROTECT YOURSELF

- Verify through a second, independent channel.
- Challenge unexpected requests, even if they seem urgent.
- Use a secret code or passphrase for high-risk communications.
- Slow down. Take time before you act or send money.

IF YOU CAN SEE IT, HEAR IT, OR READ IT—DON'T ASSUME IT'S REAL.

VERIFY. QUESTION. CONFIRM. Don't trust. Verify.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

VOICE CLONING & VISHING

AI can now clone voices in seconds—and criminals use them to call, scare, and steal.

HOW VOICE CLONING WORKS

1. **COLLECT AUDIO** — Just a few seconds of someone speaking.
2. **AI ANALYZES THE VOICE** — AI learns the voice patterns, tone, and rhythm.
3. **CLONE THE VOICE** — The AI creates a realistic synthetic voice.
4. **SPEAK ANYTHING IN THEIR VOICE.** — The criminal can now say anything—convincingly.

EXAMPLE: THE "URGENT CALL"



SAME VOICE. SAME TONE. COMPLETELY FAKE.

COMMON VISHING ATTACKS

BANK OR FINANCIAL INSTITUTION
"We detected suspicious activity on your account. Please verify your information."

TECH SUPPORT SCAMS
"This is Microsoft (or Google, Apple). We need remote access to fix a problem."

LAW ENFORCEMENT IMPERSONATION
"This is Officer Smith. There's a warrant for your arrest unless you pay a fine now."

CEO OR EXECUTIVE IMPERSONATION
"I need you to wire funds for a confidential business deal. Don't tell anyone."

WARNING SIGNS

- Unexpected calls asking for money or sensitive info
- Urgency, secrecy, or threats
- Caller ID can be faked
- Poor call quality or slight voice "glitches"

WHAT CRIMINALS CAN DO

- PRETEND TO BE ANYONE—FAMILY, FRIENDS, BOSSES, EVEN YOU.
- SAY ANYTHING YOU NEVER SAID.
- CALL ANYONE, ANYWHERE, ANYTIME.
- STEAL MONEY, DATA, AND TRUST.

WHAT YOU CAN DO

- Verify the caller through a trusted channel
- Never send money or share sensitive info based on a call alone
- Use a code word with family and colleagues
- Report suspicious calls

IF YOU DIDN'T EXPECT THE CALL, DON'T TRUST THE VOICE.

VERIFY FIRST. PROTECT ALWAYS.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

IDENTITY THEFT & SYNTHETIC IDENTITY FRAUD



Criminals steal real personal information or create fake identities to open accounts, get loans, file taxes, or commit fraud.

WHAT IT IS

Identity thieves steal your personal information—or create a synthetic identity by combining real and fake information—to open accounts, get credit, file tax returns, or commit fraud in your name.

COMMON EXAMPLES

- New credit cards or loans opened in your name
- Medical services billed to your insurance
- Tax returns filed for refunds
- Utility, phone, or internet accounts opened
- Criminal charges or warrants you didn't commit

HOW IT WORKS

1. **Steal or Collect Information**
   Thieves obtain your personal data through data breaches, phishing, skimming, social media, or stolen mail.
2. **Create or Build an Identity**
   They use your real information—or mix it with fake details—to create a new or synthetic identity.
3. **Open Accounts & Build Credit**
   They open credit cards, loans, or accounts and make small payments to establish legitimacy.
4. **Commit Fraud & Cash Out**
   They run up balances, drain accounts, file fraudulent tax returns, or commit other crimes in your name.

HOW AI MAKES IT WORSE

Automated Data Harvesting
AI scrapes massive amounts of personal data from breaches, the dark web, and social media faster than ever.

Synthetic Identity Generation
AI tools create realistic fake identities at scale, including names, addresses, and lifelike IDs.

Behavioral Profiling
AI analyzes your online behavior to predict and exploit your financial habits.

AI-Powered Phishing
Highly convincing, personalized messages steal more data and bypass your defenses.

Fraud Optimization
AI tests and adapts in real time to find what works and avoid detection.

HOW TO PROTECT YOURSELF

- Freeze your credit with all three major bureaus. It's free and effective.
- Monitor your accounts, credit reports, and tax records regularly.
- Protect your personal information. Don't share it unless necessary.
- Use strong, unique passwords and enable multi-factor authentication.
- Report identity theft to IdentityTheft.gov, the FTC (ReportFraud.ftc.gov), and your local police.

Your identity is valuable. Protect it like cash. Detect early. Report quickly. Act decisively.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

WHAT CHANGED

How AI Changed the Cybercrime Landscape

Four shifts turned isolated scams into an industrial operation.

Scale

×1000

One operator now runs thousands of tailored attacks at once — with no extra effort.



Speed

seconds

Convincing fakes that once took days are now generated in seconds.



Believability

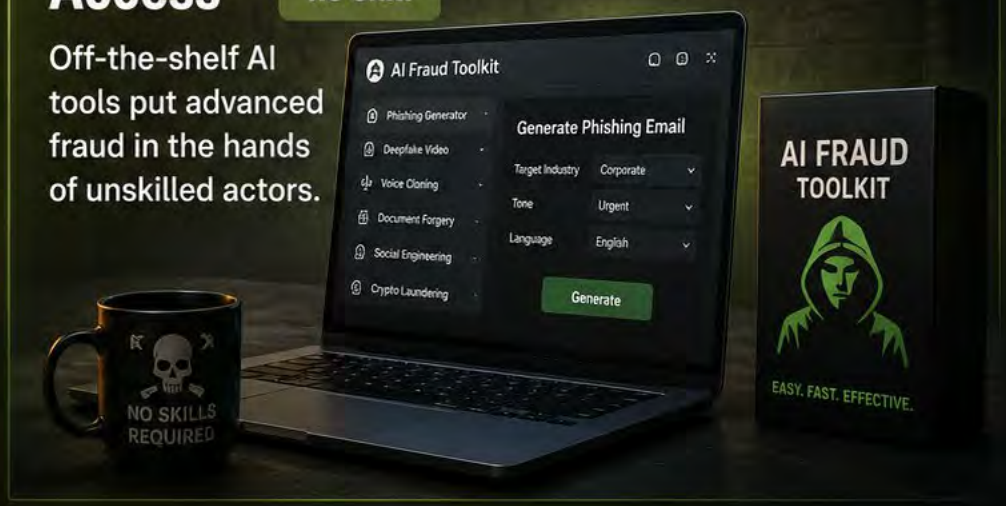
Flawless grammar, real logos, and cloned voices erase the old warning signs.



Access

no skill

Off-the-shelf AI tools put advanced fraud in the hands of unskilled actors.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

AI Has Changed the Cybercrime Game

Artificial intelligence has supercharged the tools, tactics, and reach of criminals—making scams more convincing, attacks more automated, and victims easier to find.



SPEED AND SCALE

AI can launch attacks, create fake content, and reach thousands in seconds.

PRECISION TARGETING

AI analyzes data to find the right target at the right time with the right bait.

REALISM AND DECEPTION

Deepfakes, cloned voices, and forged documents are now disturbingly real—and hard to detect.

DEEPFAKES

Synthetic identities that look and sound real.

RANSOMWARE

Systems locked. Demands made. Business halted.

AI-POWERED FRAUD

Automated scams optimized to manipulate.

IDENTITY THEFT

Personal data stolen. Lives disrupted.

BUSINESS EMAIL COMPROMISE

Trusted messages spoofed. Funds diverted.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

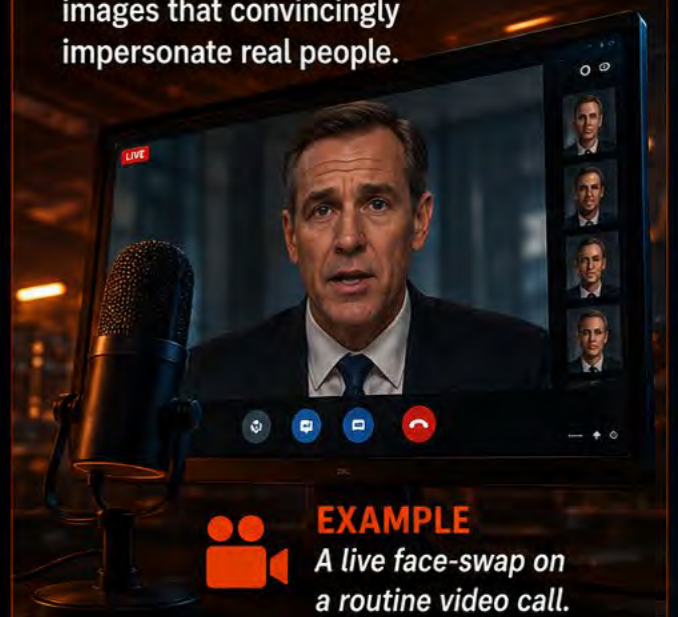
WHAT'S NEW

A New Category of Threats

Three forces reshaping how criminals operate — each one covered next.

Deepfakes

Synthetic video, audio, and images that convincingly impersonate real people.



EXAMPLE

A live face-swap on a routine video call.

Agentic AI

Self-directed AI that carries out multi-step attacks with little human input.

- RESEARCH TARGETS
- CRAFT MESSAGE
- SEND & ENGAGE
- ADAPT & REPEAT

EXAMPLE

A bot that researches, writes, and sends on its own.

Data Privacy

Personal and client data harvested to fuel hyper-targeted fraud.



EXAMPLE

A single breach turned into a personal dossier.

We'll take each in turn — what it is, how it works, and how to spot it.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

COMMON SCAMS: WHAT THEY ARE, HOW THEY WORK, AND AI'S IMPACT

AI gives scammers speed, scale, and sophistication — but awareness is your advantage.

SCAM	WHAT IT IS	HOW IT WORKS	AI'S IMPACT
PHISHING	Deceptive messages that appear to come from a trusted source to steal information or deliver malware.	• You receive an email, text, or message. • You're urged to click a link or open an attachment. • You're taken to a fake site or malware is installed.	• AI generates highly convincing, personalized messages. • Deepfakes and spoofed branding make messages look legitimate. • AI-written content evades traditional filters.
BUSINESS EMAIL COMPROMISE (BEC)	Scammers impersonate executives, colleagues, or vendors to trick you into sending money or sensitive information.	• Scammer researches your organization. • Sends a convincing email with an urgent request. • You're pressured to act quickly without verification.	• AI mimics writing style and tone of real people. • Voice cloning enables realistic phone calls. • AI gathers data from open sources to craft highly targeted requests.
DEEPFAKES / IMPERSONATION	AI-generated audio, video, or images used to impersonate real people for fraud or manipulation.	• Scammer creates a fake video or audio of someone you trust. • They use it to request money, information, or compliance.	• AI creates realistic synthetic videos and voices. • Harder to detect, even by trained eyes and ears. • Real-time deepfakes make live impersonation possible.
TECH SUPPORT SCAMS	Scammers pretend to be from tech companies to gain remote access or payment.	• You see a pop-up or get a call about a computer problem. • You're instructed to call a number or grant remote access. • They steal data or install malware.	• AI generates fake pop-ups and convincing websites. • AI chatbots engage victims and build trust. • AI translates scripts and localizes scams globally.
ROMANCE / PIG BUTCHERING	Scammers build fake romantic relationships to gain trust and steal money, often through investment schemes.	• Scammer builds rapport over weeks or months. • Introduces a fake investment opportunity. • Victim invests more and more, then loses everything.	• AI creates convincing profiles and photos. • AI chatbots maintain 24/7 conversations. • AI analyzes responses to manipulate emotions and maximize profit.
GOVERNMENT / IMPERSONATION	Scammers impersonate law enforcement, IRS, or other agencies to intimidate or trick you into paying.	• You receive a call or message with threats of arrest, fines, or lawsuits. • You're told to pay immediately to avoid consequences.	• AI voice cloning makes caller ID and voices sound legitimate. • AI crafts official-looking documents and notices. • AI increases pressure with realistic details.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Social Engineering and Wire Fraud



- **Business Email Compromise (BEC) is one of the most financially damaging cybercrimes targeting law firms (FBI)**
- **Attackers impersonate partners, clients, or title companies to redirect wire transfers**
- **Vishing (voice phishing) and pretexting target firm staff by phone**
- **AI-generated deepfake audio can convincingly impersonate known voices**
- **Always verify wire instructions through a second, trusted, independent channel**
- **Train all staff—including support and accounting—to recognize social engineering**

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Deepfakes and Evidence Integrity

Threat: fabricated audio/video 'confessions' and staged events.

Defense: provenance (source capture), device logs, hashing at capture.

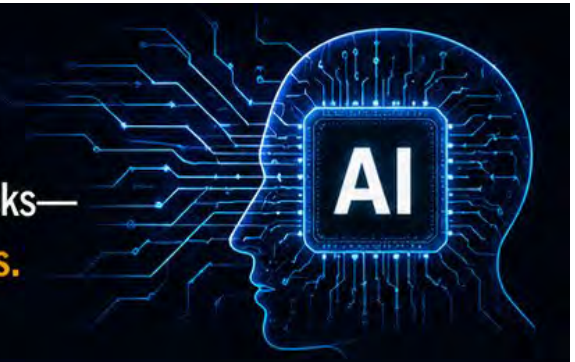
Use trusted capture apps/hardware for high-stakes recordings.

Cross-examination themes: incentives, tool settings, prior versions, missing originals.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

AI MAKES IT EASIER TO SUCCEED

AI lowers the skill, time, and cost required to run sophisticated attacks—and increases the odds of success.





1 LOWER BARRIERS

- No coding. No tools.
- Off-the-shelf AI platforms do the heavy lifting.
- Anyone can launch a real attack.



2 MORE SPEED

- AI automates research, content creation, and outreach.
- Attacks that took days now take minutes.



3 MORE CONVINCING

- Deepfakes. Synthetic voices.
- Perfect grammar. Personal details. Context on demand.
- Harder to detect. Easier to believe.



4 GREATER SCALE

- AI reaches thousands—or millions—simultaneously.
- Every channel. Every time zone. 24/7.
- More targets. More victims.

THE RESULT: MORE ATTACKS. MORE VICTIMS. GREATER HARM.

Traditional defenses alone are no longer enough.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

FROM TARGETED TO INDUSTRIALIZED.

AI turns handcrafted attacks into industrial-scale operations—reaching more people, everywhere, all the time.



THE THREAT IS NO LONGER PERSONAL. IT'S MASS PRODUCTION.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

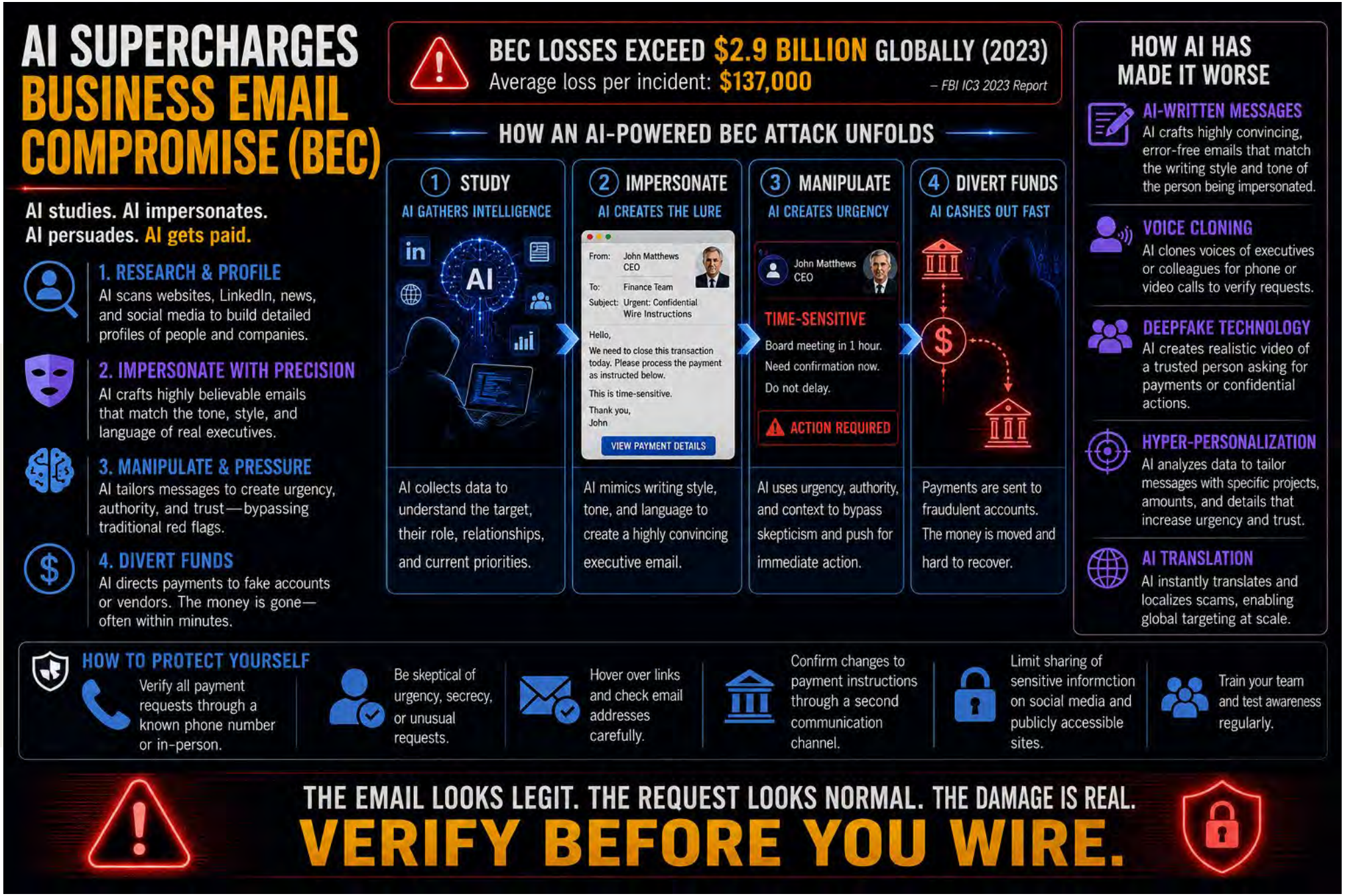
Credential Theft: The Keys to the Office

The Setup	A password or login is stolen.
The Risk	One account can open email, files, and firm systems.
The Lesson	A small credential mistake can become a big access problem.
The Takeaway	One stolen login can open every door.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

GOVERNMENT IMPERSONATION SCAMS



Criminals impersonate government agencies or officials to create fear, urgency, or false authority—and steal money or information.

WHAT IT IS

Criminals pretend to be from government agencies or officials to frighten or pressure you into paying money, sharing data, or taking action you wouldn't normally take.

Common Impersonated Agencies:

- IRS (Tax notices, refunds)
- Social Security Administration
- FBI / Law Enforcement
- U.S. Marshals
- Local Police
- Immigration Officials
- Jury Duty
- DMV / Toll Authorities
- Other Regulatory Agencies

HOW IT WORKS

1. **Contact Out of the Blue**
   You receive a call, email, text, or letter claiming to be from a government agency.
2. **Create Fear and Urgency**
   They claim you owe money, have a legal problem, or must act immediately to avoid arrest, fines, or license suspension.
3. **Demand Payment or Information**
   They demand payment (gift cards, wire transfer, crypto, prepaid cards) or ask for personal or financial data.
4. **Disappear with Your Money/Data**
   Once paid or once they have your information, they vanish—or continue the scam for more.

HOW AI HAS MADE IT WORSE

- **Perfect, Official-Looking Communications**
  AI creates flawless letters, emails, and forms with logos, seals, and case numbers.
- **Voice Cloning of Officials**
  AI clones voices of real officials to make phone calls sound completely legitimate.
- **Personalized Threats**
  AI uses data from breaches and social media to craft threats that feel uniquely targeted.
- **AI Chatbots Impersonate Agencies**
  Convincing chatbots answer questions and keep victims engaged 24/7.
- **Deepfake Video "Announcements"**
  AI-generated videos of officials delivering fake warnings or legal threats.

HOW TO PROTECT YOURSELF

- Government agencies rarely contact you unexpectedly. Be suspicious.
- Verify independently. Call the official number on the agency's website—not the number given to you.
- Never pay with gift cards, crypto, wire transfers, or prepaid debit cards. Real agencies don't demand these.
- Don't share personal information or IDs unless you initiated the contact.
- Report scams to the FTC (ReportFraud.ftc.gov) and your state Attorney General.

Government agencies almost never demand immediate payment by gift card, cryptocurrency, wire transfer, or prepaid debit card. Stop. Verify. Don't Pay.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

UTILITY SCAMS

Criminals impersonate utility companies to create fear, urgency, or disconnection threats—and steal money or information.



WHAT IT IS

Scammers pose as your electric, gas, water, internet, or other utility provider.

They claim your account is past due or will be disconnected unless you pay immediately.

COMMON TARGETED UTILITIES:

- Electric
- Gas
- Water / Sewer
- Internet / Cable
- Trash / Recycling
- Phone / Telecom
- Home Security
- Solar / Energy Providers
- HoA / Municipal Services

HOW IT WORKS

1. **INITIAL CONTACT**
   You receive a call, text, email, or even a voicemail claiming to be from your utility company about an urgent issue.
2. **CREATE FEAR AND URGENCY**
   They claim your bill is past due, there is suspicious usage, or your service will be disconnected immediately.
3. **DEMAND IMMEDIATE PAYMENT**
   They demand payment now using gift cards, prepaid debit cards, wire transfers, or cryptocurrency.
4. **STEAL YOUR MONEY OR INFORMATION**
   Once you pay or share your information, the scammer disappears—or uses it for identity theft or future fraud.

HOW AI HAS MADE IT WORSE

CONVINCING, PERSONALIZED MESSAGES
AI generates highly convincing, personalized emails, texts, and voicemails that mimic legitimate utility communications.

AI VOICE CLONING
Clones real utility company voices or uses AI voices that sound natural and trustworthy.

DATA-DRIVEN TARGETING
Uses data from breaches and social media to know your provider, usage patterns, and contact details.

REALISTIC FAKE BILLS AND DOCUMENTS
AI creates official-looking bills, logos, and disconnection notices that are hard to spot as fake.

AI CHATBOTS IMPERSONATE AGENTS
Chatbots handle calls or texts 24/7, answer questions, and pressure you into paying.

HOW TO PROTECT YOURSELF

- Contact your utility company using the official number on your bill or website—not the number given to you.
- Never pay with gift cards, cryptocurrency, wire transfers, or prepaid debit cards.
- Don't click links or open attachments in unexpected messages. Go directly to the company's site.
- Monitor your accounts regularly and set up alerts for billing changes or unusual activity.
- Report scams to the FTC (ReportFraud.ftc.gov) and your local utility company.

Utility companies rarely demand immediate payment or threaten disconnection without prior notice.

STOP. VERIFY. DON'T PAY.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



The Setup

A caller claims a grandchild is hurt, jailed, or stranded.

The Pressure

“Act now. Don’t tell anyone.”

The Defense

Hang up and call the family member directly.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Romance Scams: The Long Con

The setup:

A fake relationship is built over time.

The ask:

Money, gift cards, crypto, or personal information.

The tell:

There is always a reason they cannot meet, verify, or wait.

Emotional trust is not proof. Verify before you send.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

RANSOMWARE & DATA EXTORTION

Attackers use malicious software to lock or steal your data and demand a ransom—often threatening to leak it if you don't pay.



WHAT IT IS



Ransomware is malware that locks your systems or encrypts your data. Extortion threats pressure you to pay to restore access or prevent data leaks.

COMMON EXAMPLES

- Files and systems encrypted, unusable
- Data stolen and threat of public release
- Business operations disrupted or halted
- Demands for payment in cryptocurrency
- Double or triple extortion tactics (encrypt, steal, threaten, ransom)

HOW IT WORKS

1. **GAIN ACCESS**
   Attackers enter your network through phishing, vulnerabilities, weak passwords, or stolen credentials.
2. **MOVE & DEPLOY**
   They move laterally, escalate privileges, and deploy ransomware or exfiltrate data.
3. **ENCRYPT OR STEAL**
   Files are encrypted or data is stolen. A ransom note is left with payment instructions and threats.
4. **DEMAND & EXTORT**
   Attackers demand payment—often threatening to leak or sell your data if you refuse.

HOW AI MAKES IT WORSE

SMARTER PHISHING
AI crafts highly convincing phishing emails that bypass filters and fool more people.

AUTOMATED RECONNAISSANCE
AI tools quickly map networks, find vulnerabilities, and identify high-value targets.

MALWARE CREATION
AI lowers the barrier to create and improve malware, making attacks faster and cheaper.

EXTORTION OPTIMIZATION
AI analyzes victims to set ransom demands, timing, and pressure tactics for maximum gain.

FASTER SPREAD, GREATER IMPACT
AI automates attacks, scales operations, and targets more victims—globally.

HOW TO PROTECT YOURSELF

- Be suspicious of emails and links. Verify before you click.
- Use strong, unique passwords and multi-factor authentication.
- Back up data regularly and test your backups offline or in the cloud (immutable backups).
- Keep systems, software, and security tools updated and patched.
- Limit user access and follow least privilege practices.
- Have and test an incident response and recovery plan.

THERE IS NO GUARANTEE OF RECOVERY. PREVENTION IS YOUR BEST DEFENSE.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

CLIENT IMPERSONATION & WIRE FRAUD

AI makes it easier than ever for criminals to impersonate trusted clients and steal money in minutes.

IMPERSONATE
AI analyzes emails, documents, and communications to mimic writing style and tone.

CREATE URGENCY
Convincing messages pressure you to act fast and bypass normal verification.

INITIATE PAYMENT
Criminals direct wire transfers to their accounts—often international and irreversible.

DISAPPEAR
Once the money is sent, it's gone—and the fraudster is unknown.

EXAMPLE: FAKE EMAIL FROM A CLIENT

John Smith
jsmith@smithlaw.com
9:14 AM

Subject: URGENT – Wire Transfer Needed Today

Hi,

We need to close the transaction today. Please wire $250,000 to the account below.

This is time-sensitive. Please confirm once completed.

Thanks,

John Smith

The email looks real. The tone is right. The name is right. But it's not your client.

THE FRAUDULENT WIRE

WIRE TRANSFER INSTRUCTIONS

Beneficiary: Global Holdings Ltd.

Bank: First International Bank

Account Number: 9812 3456 7890

Routing / SWIFT: FIRNUS33XXX

Amount: $250,000 USD

ONCE SENT, THE MONEY IS ALMOST IMPOSSIBLE TO RECOVER.



HOW CRIMINALS LEVERAGE AI

- Scrape emails, filings, and letters to learn writing style and context.
- Generate highly convincing messages that look and sound real.
- Clone voices in phone calls to verify instructions.
- Create fake supporting documents and account confirmations.

WHAT YOU CAN DO

- Verify any change in wire instructions using a known phone number—not email.
- Establish code words or verification protocols with clients.
- Be suspicious of urgency, secrecy, or last-minute requests.
- Confirm recipient details through a separate channel.
- Train your team. One click can cost everything.

HOW TO PROTECT YOURSELF

- Verify all payment requests through a known, independent channel.
- Call the client or attorney using a trusted phone number on file.
- Never rely solely on email or phone for changes to payment instructions.
- Look for red flags: urgency, secrecy, unfamiliar accounts, or unusual requests.
- Educate staff and clients about these scams and test your verification procedures regularly.
- Have written policies for verifying and approving all fund transfers.

A REAL CLIENT. A FAKE REQUEST. A DEVASTATING LOSS.

VERIFY ALWAYS. WIRE SAFELY.

STOP. VERIFY. PROTECT. One wrong transfer can't be undone.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Social Engineering: Hacking the Human

The tactic: Exploit emotion instead of technology.

The triggers: Pressure. Flattery. Fear. Trust.

The goal: Make the target bypass normal procedure.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The False Settlement Trap



The Scenario: A new client approaches your firm (often from out-of-state or abroad) claiming they were injured or wronged. They provide "documentation" that a settlement has already been reached with a company.

The Hook: The firm receives a realistic-looking cashier's check for the settlement amount. The client asks the firm to deposit it into their IOLTA account and wire their portion of the proceeds immediately.

The Result: The check is fraudulent and bounces days later. Because the firm already wired funds, the trust account is overdrawn, and the firm is liable to the bank for the deficit.

Key Defense: Never disburse funds until the check has fully cleared. Verify all settlement details independently—do not rely on documents provided solely by the client.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Redirecting The Funds



The Scenario: Scammers monitor firm communications—often by gaining unauthorized access to email accounts—to identify when a high-dollar transaction (e.g., real estate closing) is ready to fund.

The Hook: Just before closing, a "client" or "partner" sends an urgent email with "updated" wire instructions, claiming the original account is undergoing maintenance.

The Result: The firm wires the closing funds to the hacker's account instead of the intended recipient.

Key Defense: Confirm wire instructions verbally. Use a known phone number from your internal records—never call the number provided in a suspicious or "update" email.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

When the Firm's Reputation is Used Against You



The Scenario: Scammers copy attorney names, firm branding, and bar numbers to impersonate law firms online.

The Hook: They may target the public with fake debt demands or send staff urgent messages from a supposed partner or bar association.

The Result: Stolen credentials, data breaches, lost intellectual property, and reputational harm.

Key Defense: Require MFA, verify sender addresses, and report suspicious urgent or disciplinary messages to IT or the State Bar.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

MANUFACTURED URGENCY AS A TELL

Scammers create false urgency to **bypass your critical thinking** and push you to act immediately.
Real organizations give you time.

WHY SCAMMERS USE URGENCY

OVERLOADS YOUR BRAIN
Panic narrows focus and shuts down rational decision-making.

PREVENTS VERIFICATION
No time to call back, check sources, or get a second opinion.

INCREASES COMPLIANCE
Pressure makes you more likely to follow instructions without question.

SPEEDS UP THE PAYOFF
The faster you act, the faster scammers get paid.

URGENCY IS THEIR TOOL. AWARENESS IS YOUR DEFENSE.

EXAMPLES OF MANUFACTURED URGENCY

PAY NOW	ACT NOW	VERIFY TODAY	EMERGENCY!	FINAL NOTICE
"Pay immediately or your account will be locked."	"This offer expires in 30 minutes!"	"Verify your information today or face penalties."	"This is urgent. We need you to act now!"	"Final notice before legal action is taken."
Goal: Stop you from thinking.	Goal: Rush you into a decision.	Goal: Make it seem official and serious.	Goal: Trigger fear and get obedience.	Goal: Intimidate and create panic.

REAL VS. SCAM: TIME TELLS THE TRUTH

REAL ORGANIZATIONS:
- ✓ Give you time to review and decide
- ✓ Offer multiple ways to contact them
- ✓ Do not demand immediate payment
- ✓ Encourage you to ask questions

VS.

SCAMMERS:
- ✗ Demand immediate action
- ✗ Limit or block other contact methods
- ✗ Threaten consequences
- ✗ Discourage questions or delays

TIME IS YOUR ALLY. PAUSE. VERIFY. PROTECT YOURSELF.

WHAT TO LOOK FOR

Urgent or threatening language
Act now, immediate, or your account will be closed.

Unrealistic deadlines
Pressure to respond in minutes or within hours.

Discourages verification
"Don't call us. Just click here."
"No time to explain."

Promises or threats
Rewards for quick action or penalties for delay.

WHAT YOU CAN DO

PAUSE
Take a breath. Don't let urgency dictate your actions.

VERIFY
Use trusted contact info to check the source independently.

QUESTION
Ask: Why the rush? What happens if I wait?

PROTECT
Never share sensitive information or send money under pressure.

IF SOMEONE IS RUSHING YOU, THEY'RE HIDING SOMETHING.
SLOW DOWN. CHECK IT OUT. STAY SAFE.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

SECRECY & ISOLATION AS A TELL

THEIR GOAL:
Keep you alone, quiet, and in the dark.

Scammers don't want you to talk to anyone else—that's how they keep control and avoid getting caught.

WHY SECRECY WORKS

PREVENTS REALITY CHECKS
They don't want you talking to family, colleagues, or your bank.

CREATES DEPENDENCY
You rely only on them for information and "solutions."

LIMITS EXPOSURE
No one else sees the red flags or notices the inconsistencies.

ELIMINATES OPPOSITION
They isolate you so no one can challenge or stop them.



WHAT SCAMMERS SAY

- "This is confidential. Don't tell anyone or you'll lose the deal."
- "They won't understand. It's complicated."
- "I'm the only one who can help you with this."
- "Do it now—there's no time to discuss it."
- "Promise you won't share this with anyone."

WHAT YOU CAN DO

TALK TO SOMEONE YOU TRUST.
A second opinion can save you.

QUESTION THE PRESSURE.
Legitimate requests don't demand secrecy.

VERIFY INDEPENDENTLY.
Use known contact information and channels.

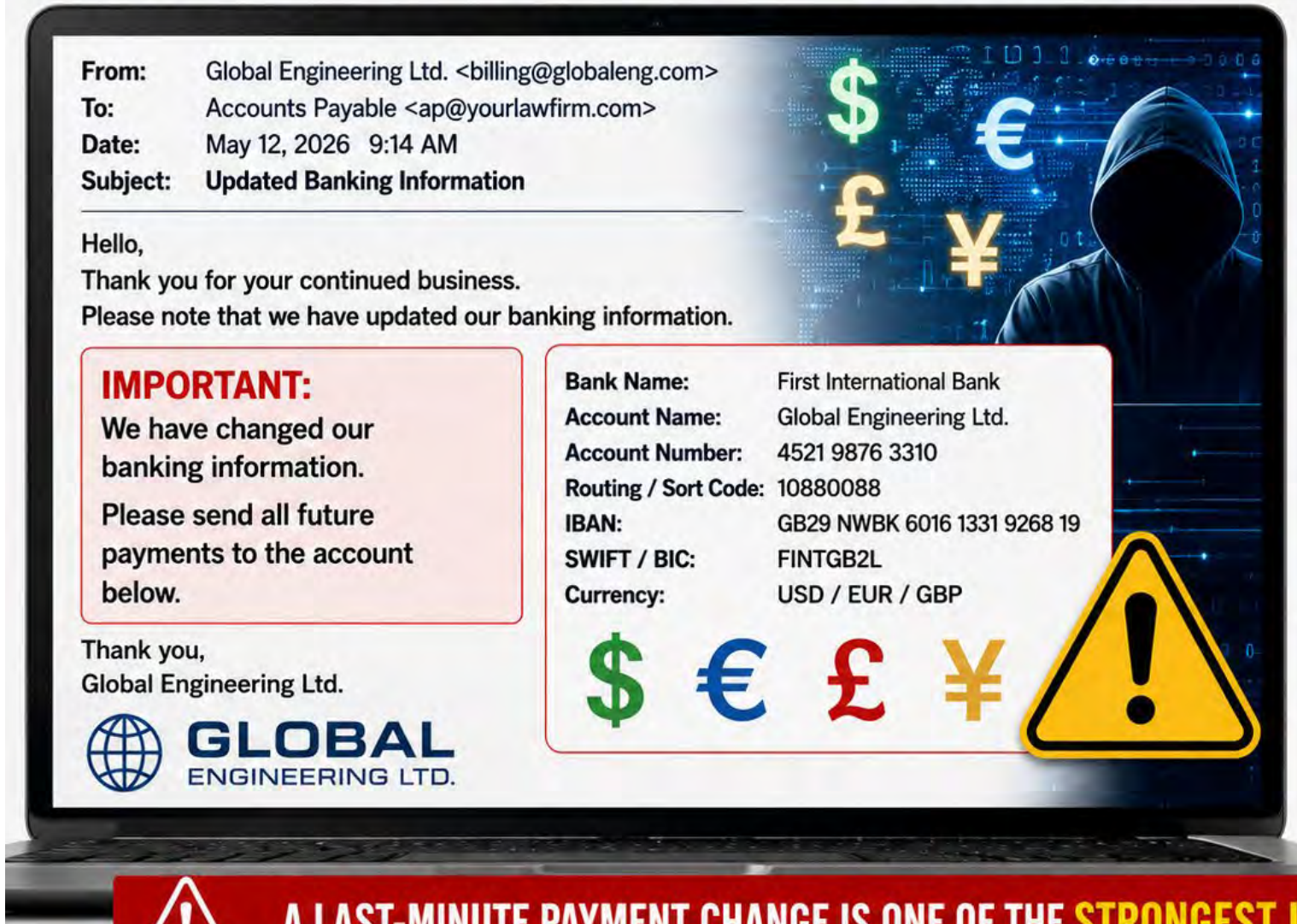
TRUST YOUR INSTINCTS.
Secrecy is not normal—walk away.

SHARE. CHECK. VERIFY.
Scammers fear daylight and second opinions.

ISOLATION IS CONTROL. CONVERSATION IS PROTECTION.
DON'T GO IT ALONE. TALK. VERIFY. STAY SAFE.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

PAYMENT CHANGES AS A TELL



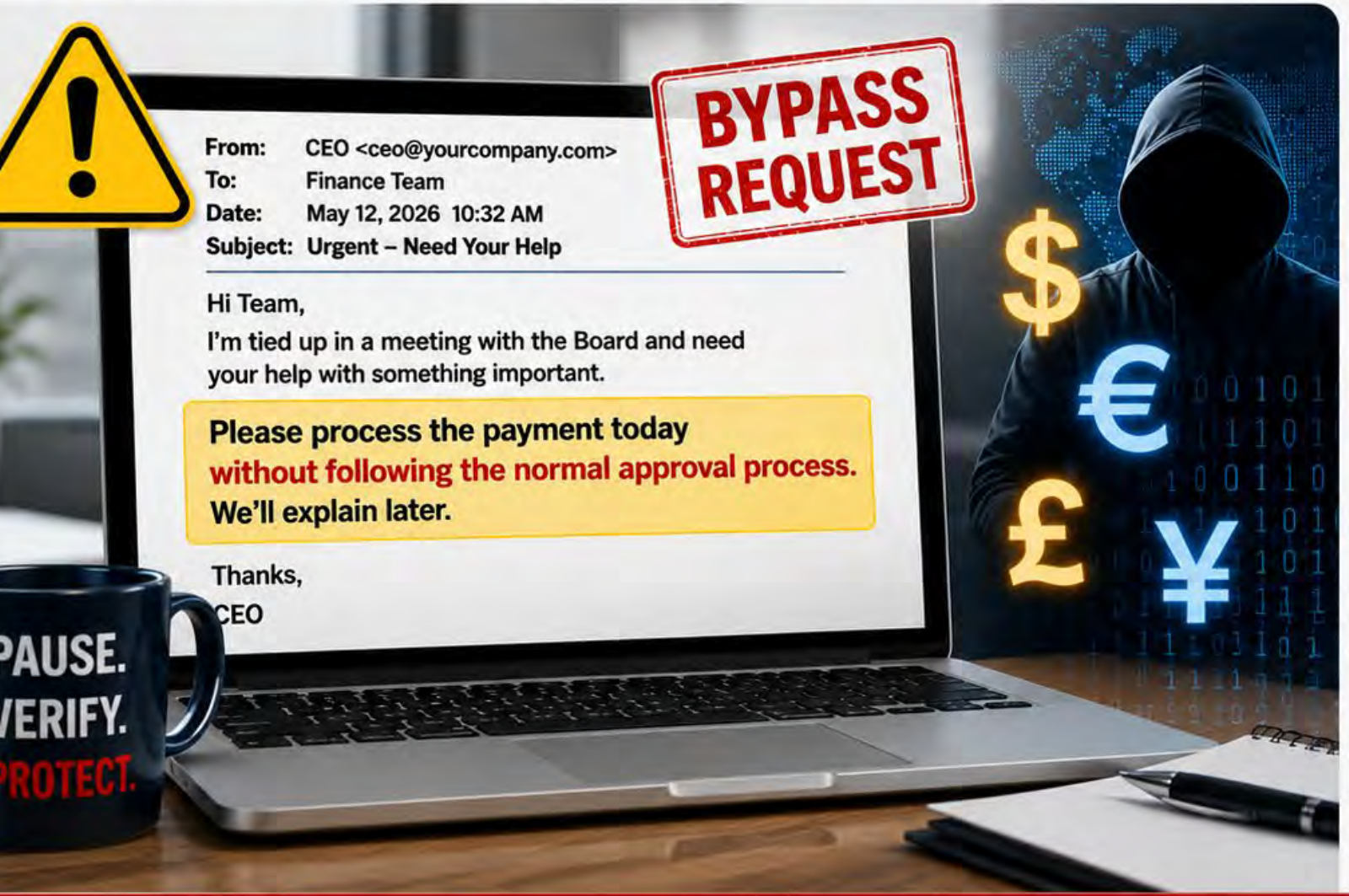
Treat every payment change as suspicious until independently verified.

- Verify using a known telephone number
- Never rely on email alone
- Confirm wire instructions verbally
- Train staff to pause before paying

A LAST-MINUTE PAYMENT CHANGE IS ONE OF THE STRONGEST INDICATORS OF BUSINESS EMAIL COMPROMISE.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

REQUESTS THAT BYPASS PROCESS AS A TELL



Out-of-process requests are a major red flag.

- Scammers create urgency to bypass normal controls.
- Shortcuts today lead to big losses tomorrow.
- Verify the request through an independent, trusted channel.
- Follow your process. It's there to protect you.
- Empower your team to stop and escalate.

IF SOMEONE ASKS YOU TO BYPASS PROCESS,
STOP. VERIFY. PROTECT.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

RESISTANCE TO VERIFICATION AS A TELL

If a legitimate request can be verified, a **scammer** will try to **stop you.**



From: CEO <ceo@yourcompany.com>
To: Finance Team
Date: May 12, 2026 10:47 AM
Subject: Urgent – Confidential Request

RED FLAG

Hi,
I need you to handle a sensitive payment today.
Please do not call me or anyone else about this.
Just process it as requested.
We are under a tight deadline.

Do not verify – just trust me on this.

Thanks,
CEO

Scammers hate verification.
Resistance is a major warning sign.

They tell you not to call.
Legitimate people welcome a quick call.

They discourage email confirmation.
Scammers don't want a written trail.

They create urgency to stop you.
"Act now or we'll miss the opportunity."

They demand secrecy.
"Don't tell anyone." "Keep this confidential."

They push back on your questions.
"Why are you making this so difficult?"

A LEGITIMATE REQUEST CAN SURVIVE VERIFICATION.
IF THEY RESIST VERIFICATION, STOP AND INVESTIGATE.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

SMALL MISMATCHES AS A TELL

Scammers count on you missing the small things. Don't.

JS

From: John Smith <John.Smith@acmepartners.com>
To: You
Date: May 12, 2026 11:18 AM
Subject: Urgent: Invoice Payment

Hi,
Please process the attached invoice for $48,750.00.
We have updated our banking information.

Please send payment to the account below.

Thanks,
John Smith
CFO, Acme Partners

Bank Name:	First Trust International
Account Name:	Acme Partners LLC
Account Number:	87654321
Routing Number:	021000021
SWIFT / BIC:	FTIBUS33



Small mismatches can signal a big scam.

- Check email addresses carefully. One extra letter can be the difference.
- Watch for unusual capitalization, spacing, and punctuation.
- Verify bank names, accounts, and routing/SWIFT codes.
- Confirm amounts, invoice numbers, and payment details.
- When in doubt, verify through an independent, trusted channel.

SMALL MISMATCHES CAN LEAD TO BIG LOSSES. SLOW DOWN. CHECK EVERYTHING.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

UNEXPECTED CHANNEL OR CONTACT AS A TELL



Scammers use unexpected channels to catch you off guard and bypass normal safeguards.

They avoid your normal communication channels.
Calls, texts, or personal email are red flags.

They impersonate someone you trust.
Authority makes the request seem legitimate.

They create urgency to prevent you from verifying.
Quick action is their goal.

They know bypassing process increases their chance of success.
Unexpected = less scrutiny.

WHAT YOU CAN DO

Be suspicious of requests that come through unusual channels.

Always verify the request using a known contact method.

Call the person back using a trusted number you already have.

Train your team to question requests that come through unexpected channels.

IF IT'S UNEXPECTED, IT SHOULD BE VERIFIED. DON'T ASSUME. CONFIRM.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

EMOTIONAL LEVERAGE AS A TELL

Scammers exploit your emotions to lower your defenses and push you to act without thinking.



FEAR
"Your account will be suspended immediately."

URGENT EMPATHY
"My child is in trouble. I need help now!"

GREED
"This is a limited-time offer just for you."

AUTHORITY & TRUST
"I'm from the government/ bank. You need to act."

When scammers trigger strong emotions, it's often a sign of a scam.

Pause. Breathe. Think. Then verify.

WHAT YOU CAN DO

- **Pause** when you feel strong emotion. **Pressure** is their tool.
- **Recognize** the emotion being used to influence you.
- Step away and **verify** through an independent source.
- Talk to **someone you trust** before taking action.
- Train your mind to **spot** emotional manipulation.

IF IT TRIGGERS STRONG EMOTION, IT DESERVES EXTRA SKEPTICISM.
VERIFY BEFORE YOU ACT.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



The Tells: Pressure & Emotion

Many scams work by rushing you and hijacking your emotions.

- **Manufactured urgency:** “Act now” deadlines designed to stop you verifying.
- **Emotional leverage:** Fear, panic, sympathy, or flattery to override your judgment.
- **Secrecy & isolation:** “Don’t tell anyone” keeps you from the colleague who’d catch it.

Any one of these is reason enough to stop and verify.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The Tells: Broken Process

Watch for the moment a routine request breaks its normal path.

Payment changes: Last-minute new bank details or wire redirects.

Bypassed process: Skipping approvals or controls “just this once.”

Resistance to verification: Pushback, excuses, or stalling when you try to confirm.

A broken process is a red flag, not an exception to grant. Slow down and verify.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



The Tells: Signal Mismatches

Looking authentic is not the same as being authentic.

- **Small mismatches:** Off-by-a-letter domains, odd phrasing, or the wrong logo.
- **Unexpected channel or contact:** A known party suddenly using a new channel, or a stranger who somehow has inside details.

Trust the small signals. When something looks off, confirm before you act.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Your Prevention Checklist

Simple steps today. Stronger protection tomorrow.



1. **Be skeptical.**
   Verify unexpected requests, links, and attachments — especially those creating urgency.
2. **Verify independently.**
   Confirm requests using a trusted, separate communication channel.
3. **Use strong authentication.**
   Use multi-factor authentication whenever available.
4. **Keep systems updated.**
   Apply patches and updates promptly to close security gaps.
5. **Back up your data.**
   Back up critical data regularly and test your backups.
6. **Train your team.**
   Regular, role-based training and testing build awareness and good habits.
7. **Keep policies current.**
   Review and update written security policies and procedures regularly.
8. **Supervise and monitor.**
   Oversee systems, vendors, and staff. Monitor for unusual activity.
9. **Report and respond.**
   Report suspicious activity immediately and follow your response plan.
10. **Build a culture of security.**
    Encourage questions, share lessons, and recognize good practices.

Prevention is everyone's responsibility.
Small actions today prevent big problems tomorrow.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

A LAYERED DEFENSE IS YOUR BEST DEFENSE

No single step is perfect. Layers of protection catch what others miss.



1. PREVENT
Strong passwords, MFA, software updates, and secure settings.
Keep threats out.

2. DETECT
Stay alert, verify requests, and watch for red flags.
Spot threats early.

3. VERIFY
Check independently using trusted contacts and sources.
Confirm before you act.

4. RESPOND
Report, change credentials, and act quickly if something seems wrong.
Limit the damage.

5. RECOVER
Restore accounts, learn, and strengthen your defenses.
Get back stronger.

WHY LAYERS MATTER

Scammers adapt.
Layers adapt back.



If one layer fails, another can still save you.

- Make it harder to be a victim.
- Give yourself more time to stop a scam.
- Build habits that protect you every day.

WHAT YOU CAN DO

- Use strong, unique passwords and enable MFA everywhere you can.
- Stay alert to red flags in emails, calls, and texts.
- Verify requests through a separate, trusted channel.
- Keep software updated and devices protected.
- Report scams and share warnings with others.
- Review and improve your defenses regularly.

SCAMS COUNT ON YOU SLIPPING UP ONCE.
LAYERS OF DEFENSE MAKE IT MUCH HARDER FOR THEM TO WIN.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



A

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

LOCK DOWN MONETARY MOVEMENT

Money moves fast. Scammers count on it. **Extra controls stop them.**

HIGH-RISK TRANSACTIONS REQUIRE EXTRA STEPS

WIRES & TRANSFERS
Always verify changes to banking details independently.

INVOICE & PAYMENT CHANGES
Confirm changes with a known contact before approving payment.

LARGE OR UNUSUAL REQUESTS
Stop and question requests that are unexpected, urgent, or out of pattern.

DUAL CONTROL
Require two people to approve high-risk payments and changes.

DAILY & DOLLAR THRESHOLDS
Set limits and alerts for amounts, recipients, and frequency.

RED FLAGS FOR MONETARY MOVEMENT

- Urgent or last-minute requests
- Change in payee, account, or payment method
- Requests from unfamiliar or unusual locations
- Pressure to act now or keep it secret
- Amounts outside normal range



WHAT YOU CAN DO

- **Verify** all payment instructions using a known phone number.
- Never trust **changes** sent by email, text, or instant message.
- Use **two-person approval** for high-risk transactions.
- **Restrict** who can initiate and approve payments.
- **Monitor** accounts and payment activity regularly.
- **Report** anything unusual immediately.

SCAMMERS ONLY NEED ONE OPEN DOOR.

Lock down monetary movement and make your money the hardest target.

VERIFY Every change. Every time.

CONTROL Access. Approvals. Limits.

MONITOR Activity. Anomalies. Alerts.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

HARDEN EMAIL AGAINST PHISHING

Email is scammers' weapon of choice.
Layered defenses protect you, your clients, and your firm.

HOW SCAMMERS GET IN

DECEPTION
They impersonate trusted senders, brands, or colleagues.

BAIT
They use urgency, curiosity, fear, or greed to lure you in.

THE HOOK
They send links or attachments designed to steal or install.

THE BREACH
They bypass security and gain initial access.

THE PAYOFF
They steal data, money, or access to your clients and firm.

BUILD LAYERS OF EMAIL PROTECTION

STRONG FILTERS
Use advanced email filtering and anti-phishing protection.

AUTHENTICATE
Enable SPF, DKIM, and DMARC to block spoofed senders.

LEAST PRIVILEGE
Limit who can send external emails from your domain.

POLICIES & CONTROLS
Enforce safe email policies, link scanning, and attachment sandboxing.

SECURE GATEWAYS
Use secure email gateways and cloud threat protection.

USER AWARENESS
Train regularly. Humans remain the strongest line of defense.

IF AN EMAIL LOOKS SUSPICIOUS:

Pause. Don't click, reply, or open attachments.

Inspect. Check the sender, links, and details.

Verify. Use a known, independent channel.

Report. Report phishing to IT and delete the email.

Protect. You protect yourself—and everyone else.

WHAT YOU CAN DO

- **Be skeptical** of unexpected, urgent, or unusual emails.
- Hover over links—**don't click**—to see the real destination.
- Be **cautious** with attachments, especially from unknown senders.
- **Verify** requests for money, data, or credentials independently.
- Watch for **red flags**: poor grammar, odd domains, mismatched URLs.
- Keep software, browsers, and security tools **up to date**.
- **Report** phishing attempts—it helps stop the next attack.

SCAMMERS EVOLVE. SO SHOULD YOUR DEFENSES.
Strong technology + smart policies + alert people = Resilient email security.

DON'T GIVE SCAMMERS A WAY IN.
HARDEN EVERY EMAIL.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

STRONG AUTHENTICATION AND ACCESS CONTROLS

Verify who you are. Control what you can access.
Make it hard for attackers—easy for the right people.

STRONG AUTHENTICATION: PROVE WHO YOU ARE



STRONG PASSWORDS

- Use long, unique passphrases.
- Avoid common words and reuse.
- Use a password manager.

MULTI-FACTOR AUTHENTICATION (MFA)

- Require MFA everywhere it's available.
- Use authentication apps or security keys —not SMS.

BIOMETRIC OPTIONS

- Use fingerprint or face ID where supported.
- Convenient and more secure.

PHISH-RESISTANT METHODS

- Use FIDO2 security keys for high-value accounts.
- The strongest defense against phishing.

KEEP IT CURRENT

- Update authentication methods regularly.
- Remove old or unused credentials.

ACCESS CONTROLS: GIVE ACCESS ONLY WHEN NEEDED

LEAST PRIVILEGE
Give users only the access they need to do their job—nothing more.

ROLE-BASED ACCESS
Access is based on roles, not individuals. Review roles regularly.

LIMIT ADMIN ACCESS
Restrict admin rights. Use separate accounts for admin tasks. Don't use daily.

LOG OUT & LOCK
Log out of all applications when done. Lock devices when unattended.

REVIEW REGULARLY
Review user access at least quarterly. Remove what's no longer needed.

WHAT YOU CAN DO

- Enable MFA on **all critical** accounts and systems.
- Use **strong, unique** passwords managed by a password manager.
- Apply **least privilege** access for every user.
- Require **step-up authentication** for sensitive actions.
- **Review** user access and roles regularly.
- Remove **inactive accounts** promptly.
- **Monitor** login activity and alerts. Investigate anything unusual.

STRONG AUTHENTICATION KEEPS THE BAD GUYS OUT.
SMART ACCESS CONTROLS LIMIT THE DAMAGE IF THEY GET IN.

Attackers steal credentials.
You control access.
Don't make it easy for them.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



PROTECT AND BACKUP CLIENT DATA

Your clients trust you with their most sensitive information.
Protect it. Backup it. Be ready if the worst happens.

PROTECT CLIENT DATA EVERY DAY

ENCRYPT EVERYWHERE
Use encryption for data at rest and in transit. Encrypt devices, files, and emails.

LIMIT ACCESS ON A NEED-TO-KNOW BASIS
Only grant access necessary to do the job. Review permissions regularly and remove unused access.

SECURE FILE STORAGE & SHARING
Store data in secure, encrypted systems. Avoid unsecured cloud services and personal email accounts.

CLASSIFY SENSITIVE DATA
Know what's sensitive. Label it. Handle it accordingly. Train your team on data handling standards.

MONITOR & DETECT THREATS
Use endpoint protection, email filtering, and monitoring tools. Respond to alerts immediately.

BACKUP CLIENT DATA—AND TEST IT

BACKUP REGULARLY
Automate backups of all critical client data—daily at minimum.

USE SECURE, OFFSITE BACKUPS
Store backups in a separate location or cloud environment from your primary data.

TEST RESTORATION OFTEN
Backups are only useful if you can restore. Test regularly and document results.

KEEP MULTIPLE VERSIONS
Retain multiple backup versions to protect against ransomware and user error.

HAVE A DISASTER RECOVERY PLAN
Know how you will recover, who is responsible, and how you will communicate.

IF YOU DON'T HAVE A BACKUP, YOU DON'T HAVE A PLAN—YOU HAVE A PROBLEM.

WHAT YOU CAN DO

- Use **encryption** for devices, files, emails, and client communications.
- **Limit access** to client data and review permissions regularly.
- Store data in **secure, approved** systems. Avoid "shadow IT."
- **Backup** critical data daily and store securely offsite.
- **Test** backup restores at least quarterly.
- **Monitor** for threats and unusual activity.
- Have and practice a **disaster recovery** and communication plan.
- **Destroy** or securely dispose of data you no longer need.

PROTECTING CLIENT DATA IS AN ETHICAL OBLIGATION AND A LEGAL REQUIREMENT.
Strong habits today prevent

ETHICAL DUTY
ABA Model Rule 1.1 (Comment 8) requires technology competence.

LEGAL DUTY
Data breaches can lead to malpractice, sanctions, and client harm.

CLIENT TRUST
Protecting data protects your clients—and your reputation.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

MANAGE VENDOR AND CLOUD RISK

Your vendors and cloud providers are part of your firm.
Their security is your risk.



TOP ACTIONS TO PROTECT YOUR FIRM

- Know who your vendors and cloud providers are—and the data they touch.
- Build strong security requirements into every contract.
- Limit access and enforce least privilege.
- Monitor continuously and stay informed.
- Prepare for incidents and test recovery.
- Plan your exit before you need it.

YOUR SECURITY IS ONLY AS STRONG AS YOUR WEAKEST PARTNER.

KNOW YOUR PARTNERS. | SET CLEAR EXPECTATIONS. | MONITOR CONTINUOUSLY. | PROTECT YOUR CLIENTS.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

DEEPFAKE AND CLONE DEFENSE



You Can No Longer Believe What You See... Or What You Hear.

Independent Verification Is Your Best Defense.

AI can fake faces. Clone voices. Forge identities.
Verify the person—not the technology.

THE THREATS ARE REAL

SYNTHETIC VIDEO
Deepfakes create realistic videos of people saying or doing things they never did.

VOICE CLONING
Criminals clone voices from short audio clips to impersonate anyone on a call.

DIGITAL IMPOSTERS
AI impersonates executives, clients, or colleagues in emails, chats, and meetings.

REAL DAMAGE
Leads to fraud, financial loss, data breaches, reputational harm, and ethical exposure.

YOUR DEFENSE: VERIFY, QUESTION, PROTECT

VERIFY IDENTITY
Use a second, independent channel to confirm identity.
Call a known number—not the one provided.
Verify in person when possible.

CHALLENGE REQUESTS
Be skeptical of urgent, unusual, or secret requests.
Confirm any request to move money or share sensitive information.

USE CODE WORDS
Establish private code words or phrases for sensitive communications.
Use them before acting on important requests.

LOOK FOR RED FLAGS
- Odd facial movements
- Mismatched audio
- Unnatural blink rates
- Background or lighting inconsistencies

REPORT & RESPOND
- Report suspected deepfakes or voice clones immediately.
- Preserve evidence.
- Update controls and inform your team.

WHAT YOU CAN DO

- **Verify identity** using a separate, known contact method.
- **Be skeptical** of unusual emails or messages, even if personalized.
- **Never rely** on video or voice alone to confirm identity.
- Use **dual authorization** for all monetary transactions.
- **Train your team** to spot and report deepfakes and clones.
- **Stay current** on deepfake threats and detection tools.
- **Report suspicious incidents** and preserve evidence.
- **Update policies** and controls based on emerging risks.

When money, confidential information, or client instructions are involved...
ALWAYS VERIFY THROUGH AN INDEPENDENT, TRUSTED COMMUNICATION CHANNEL.

Trust is earned.
Verification is essential.
Assumptions are no longer safe.

ETHICS CONNECTION

ABA Model Rule 1.1, Comment 8 – Technology competence.
A lawyer must keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.

ABA Formal Opinion 512 (2024) –
Lawyers' Responsibilities for Using Generative Artificial Intelligence.
Lawyers must use AI competently, protect client information, and maintain oversight and human judgment.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

PLAN FOR THE INCIDENT

Incidents are not a matter of IF, but WHEN.
A plan today saves time, money, clients, and your reputation tomorrow.

BE PREPARED. BE READY. RESPOND EFFECTIVELY.

1. ESTABLISH YOUR TEAM
Designate an incident response lead and key team members. Define roles and backup contacts.

2. CREATE YOUR RESPONSE PLAN
Document clear procedures for detection, escalation, containment, and recovery.

3. KNOW WHAT TO LOOK FOR
Define common threats and warning signs. Monitor systems, logs, and user reports.

4. COMMUNICATE QUICKLY
Notify the right people immediately—internally, clients (if required), and your incident response team.

5. CONTAIN THE DAMAGE
Isolate affected systems. Stop the spread. Preserve evidence. Protect client data and systems.

6. RECOVER AND LEARN
Restore systems securely. Review what happened. Update controls and your incident plan.

ESSENTIALS OF A STRONG INCIDENT PLAN

CONTACT LISTS
Keep up-to-date contacts for team members, IT, legal counsel, insurers, and key vendors.

TOOLS & ACCESS
Ensure you have access to necessary tools, backups, and clean systems for recovery.

LEGAL & REGULATORY
Understand your notification obligations and data breach laws that may apply.

DATA BACKUP
Test backups regularly and keep copies offline or in immutable storage.

COMMUNICATION PLAN
Prepare templates and key messages for clients, staff, and stakeholders.

TEST & UPDATE
Test your plan at least annually. Update after any incident or major change.

CONSIDER CYBER INSURANCE
Review your cyber insurance policy now—not after an incident. Understand coverage, exclusions, notification requirements, and access to breach coaches and legal support.

WHAT YOU CAN DO

- **Document** your incident response plan and review it at least yearly.
- **Train** your team so everyone knows their role.
- Keep **contact information** current and easy to access.
- **Test** your incident plan with tabletop exercises.
- **Back up** critical data and test restores regularly.
- **Monitor** for threats and act on alerts quickly.
- **Review and update** security controls after any incident.
- **Communicate** clearly and transparently when incidents occur.

YOU CAN'T PREVENT EVERY INCIDENT.
BUT YOU CAN PREPARE TO SURVIVE AND RECOVER.
A plan today protects your practice—and your clients—tomorrow.

PREPARE NOW.
PROTECT ALWAYS.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Stop Before You Click, Pay, or Reply

1. The Pause

PAUSE

Pause.
Take 30 seconds to evaluate the request.



2. The Verification



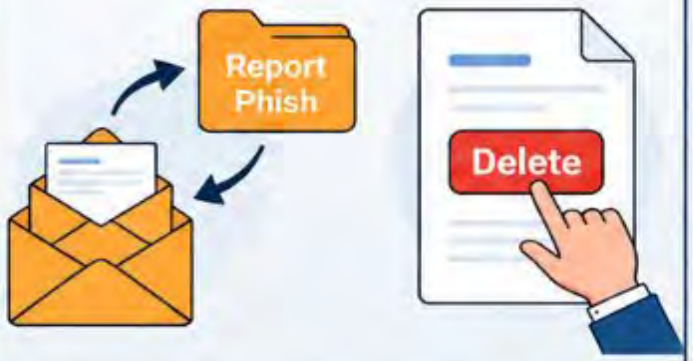
Verify using a trusted method.
Call the sender or visit the official website directly.



3. The Action



Take safe action.
Report to IT, delete, or proceed with legitimate steps.



Cybersecurity Awareness Training

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

ALIGNING PREVENTION WITH ETHICAL DUTIES

Prevention isn't just good security—
it's part of your professional responsibility.
Ethical lawyers anticipate risks, protect clients, and act with competence and diligence.

STRONG PREVENTION MEANS STRONGER ETHICS

PROTECT CLIENTS
Prevent breaches, scams, and errors that could harm clients and their matters.

MEET YOUR DUTIES
Competence, diligence, confidentiality, and loyalty require proactive cybersecurity.

REDUCE ETHICAL RISK
Good prevention reduces the risk of malpractice claims and disciplinary action.

CULTIVATE TRUST
Clients trust lawyers who safeguard information and act responsibly with technology.

STRENGTHEN YOUR PRACTICE
Strong security and ethics protect your reputation, your team, and the future of your firm.

HOW PREVENTION SUPPORTS YOUR ETHICAL OBLIGATIONS

ANTICIPATE RISKS
Identify and assess threats before they become problems.

ADOPT REASONABLE SAFEGUARDS
Use appropriate policies, tools, and training.

TRAIN YOUR TEAM
Ensure everyone knows their role in protecting client information.

SUPERVISE ACTIVELY
Oversee systems, vendors, and staff. Don't delegate your responsibility.

MONITOR AND IMPROVE
Review, test, and update policies and controls regularly.

RESPOND ETHICALLY
Act promptly, protect clients, and preserve evidence when issues arise.

Ethics is more than reacting to problems—
it's building a practice where prevention is everyday practice.
When prevention and ethics work together, everyone wins—especially your clients.

PREVENTION PROTECTS CLIENTS. | ETHICS GUIDES ACTION. | SUPERVISION MAKES IT REAL. | HABITS TODAY SAFER TOMORROW. | YOUR REPUTATION. YOUR RESPONSIBILITY.

WHAT YOU CAN DO

- Develop and maintain **written** security policies that reflect ethical obligations.
- **Train** all staff and lawyers regularly; track and document completion.
- **Supervise** and monitor compliance with policies and procedures.
- Assess **vendor** and **cloud** risks before engaging.
- **Test** your safeguards and incident response plan.
- **Address** vulnerabilities and policy violations promptly.
- **Review and update** policies, training, and controls at least annually.
- **Encourage** a **speak-up culture** and report issues without fear.
- **Document** your efforts—prevention and ethics leave a paper trail.

ETHICS CONNECTION

ABA Model Rule 1.1, Comment 8 – Technology competence.
A lawyer must keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.

ABA Model Rule 1.6 – Confidentiality of Information.
Lawyers must make reasonable efforts to prevent the inadvertent or unauthorized disclooure of, or unauthorized access to, information relating to the representation of a client.

ABA Model Rule 5.1 – Supervisory Responsibilities.
Lawyers must make reasonable efforts to ensure that all lawyers and nonlawyers in the firm comply with the Rules of Professional Conduct.

ABA Model Rule 5.3 – Responsibilities Regarding Nonlawyer Assistance.
Lawyers must ensure that nonlawyer assistance is compatible with the lawyer's professional obligations.

ABA Formal Opinion 512 (2024) – Lawyers' Responsibilities for Using Generative Artificial Intelligence.
Lawyers must use AI competently, protect client information, and maintain oversight and human judgment.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

WHAT CAN BE DONE?
Protect Yourself and Your Clients

Strong habits, smart tools, and a suspicious mindset are your best defenses against AI-powered scams.

VERIFY RELENTLESSLY
Confirm requests through independent channels—never rely on the message that asks for action.

PROTECT ACCOUNTS
Use multi-factor authentication (MFA) everywhere. Strong passwords aren't enough.

THINK BEFORE YOU CLICK
Hover. Inspect. Question odd links, attachments, and urgent asks.

TRAIN YOUR TEAM
Regular awareness training turns everyone into a human firewall.

SECURE DATA
Limit what you share, encrypt what you store, and keep devices updated.



Good habits today.
Strong protection tomorrow.

Copyright 2026, Jeffrey Allen and Ashley Hallene.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

BUILD A HUMAN FIREWALL (TRAINING AND FIRM CULTURE)

Technology helps. People stop scams. Culture makes it stick.

TRAIN CONTINUOUSLY

- Regular, short, practical training on today's threats
- Real examples. Real scenarios. Real impact.
- Keep everyone—lawyers, staff, and leaders—up to date.

ENCOURAGE SPEAK-UP CULTURE

- Make it safe to ask questions and raise concerns.
- Reward good catches.
- No blame. Just better outcomes.

LEAD BY EXAMPLE

- Leaders set the tone.
- Good habits from the top drive good habits everywhere.
- Walk the talk. Every time.

Every person in your firm is part of the defense.



TOGETHER, WE STOP SCAMS.

AWARE. ALERT. EMPOWERED.

SAFER FIRM. STRONGER CLIENT TRUST.

WHAT YOU CAN DO

- Make security training regular, relevant, and engaging.
- Run phishing simulations and review the results.
- Communicate threats and lessons learned across the firm.
- Celebrate catches and share success stories.
- Make security part of onboarding, not an afterthought.
- Review, adapt, and improve your program continuously.

OUR CULTURE IS OUR DEFENSE.
STRONGER TOGETHER. SAFER TOGETHER.

- **THINK** before you click.
- **VERIFY** before you act.
- **SPEAK UP** if something feels wrong.
- **PROTECT** our firm. Our clients. Our reputation.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

AI v AI in Defense

AI isn't just the threat — it can be part of the solution.

Used ethically and responsibly, AI can help lawyers detect, respond to, and defeat AI-powered attacks.



Attackers use AI. Defenders should too.

HOW AI CAN STRENGTHEN YOUR DEFENSE

DETECT FASTER
AI tools can identify phishing, malware, and abnormal activity before damage occurs.

ANALYZE SMARTER
AI can analyze emails, documents, and communications to spot deception and deepfakes.

RESPOND QUICKER
Automated systems can triage alerts, contain threats, and accelerate incident response.

INVESTIGATE DEEPER
AI can process large datasets and uncover patterns humans might miss.

PREDICT & PREVENT
AI models can predict emerging threats and help you prevent attacks in advance.

KEY PRINCIPLES

- **Use AI tools wisely.**
  Understand their limits, validate results, and maintain professional judgment.
- **Protect confidentiality.**
  Evaluate vendor privacy, data handling, and security before using AI tools.
- **Stay in control.**
  You are responsible for the decisions, advice, and actions in your practice.
- **Keep learning.**
  AI evolves quickly—stay informed and adapt your defenses.

When AI is used for good, it can level the playing field.
AI vs. AI is the future of cybersecurity—be on the right side.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

SECURE DEVICES AND ACCESS



Your devices are the keys to your data.
Secure them. Update them. Protect them.

COMMON RISKS TO DEVICES AND ACCESS

MALWARE & RANSOMWARE
Malicious software can steal data, lock files, or spy on you.

UNSECURE NETWORKS
Public Wi-Fi and weak networks can expose your data.

OUTDATED SOFTWARE
Missing updates leave known holes attackers exploit.

LOST OR STOLEN DEVICES
Unprotected devices can put firm and client data at risk.

WEAK ACCESS PRACTICES
Shared logins, saved passwords, and poor habits are risky.

SECURE DEVICES: BUILD STRONG HABITS

USE BUILT-IN PROTECTIONS
Enable firewalls, antivirus, and endpoint protection. Turn on device encryption.

KEEP EVERYTHING UP TO DATE
Enable automatic updates. Update OS, apps, and firmware regularly.

LOCK IT DOWN
Use strong authentication and auto-lock. Don't leave devices unattended.

USE SECURE STORAGE
Encrypt files and removable media. Use approved cloud services only.

TRAVEL SMART
Use a VPN on untrusted networks. Be cautious with charging stations and USB ports.

FIRM ACCESS BEST PRACTICES

- Limit access to what people need to do their jobs.
- Review and remove access when no longer needed.
- Use separate accounts for admin tasks.
- Monitor access and login activity regularly.

WHAT YOU CAN DO

- Use **strong authentication (MFA)** on all accounts and devices.
- Keep your OS, apps, and security software **up to date.**
- Avoid public Wi-Fi; use a **VPN** when you must.
- **Lock your screen** when away—every time.
- Use a **password manager**; never save passwords in browsers.
- Be **cautious** with downloads, attachments, and external drives.
- **Report** lost, stolen, or suspicious devices immediately.



SECURE DEVICES. SMART ACCESS. STRONG DEFENSE.
Good habits today prevent breaches tomorrow.

PROTECT your devices. your data.

EMPOWER your team. your culture.

REDUCE RISK. Build trust. Stay compliant.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

THE THREE LAYERS OF PROTECTION: PEOPLE • PROCESS • TECHNOLOGY

No single defense is enough. Real security requires all three working together.

1. PEOPLE

Your first line of defense. Human judgment stops most scams.

- Awareness of common scams
- Healthy skepticism
- Training and ongoing education
- Verify before you act
- Speak up and report concerns

3. TECHNOLOGY

Tools make it harder for attackers to succeed.

- Multi-factor authentication (MFA)
- Email filtering and anti-phishing
- Endpoint protection
- Password managers
- AI-powered detection tools

Strong alone.
Unstoppable together.



2. PROCESS

Good processes create consistency and close the gaps.

- Written procedures
- Two-person approval
- Callback verification
- Escalation paths
- Regular reviews and audits

REMOVE ANY ONE LAYER... THE STOOL FALLS.

No people?
Technology and processes can be fooled or bypassed.

No process?
Good intentions lead to inconsistent results and missed steps.

No technology?
People and processes are overwhelmed and attacks get through.

Technology without trained people fails.
Good people without sound processes fail.

Strong processes without modern technology eventually fail.

REAL SECURITY REQUIRES ALL THREE.

Scammers don't need to defeat every defense. They only need to find the one layer you forgot.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

PREVENTION & CYBERSECURITY

Aligning Prevention With Your Duties

Cybersecurity isn't just IT hygiene — it's how you satisfy core professional obligations.

Competence

Keep up with technology's risks and benefits.

ABA Model Rule 1.1, Comment 8.

Confidentiality

Make reasonable efforts to protect client data.

ABA Model Rule 1.6; Formal Ops 477R & 483.

Communication

Inform clients of a breach that affects them.

ABA Model Rule 1.4.

Supervision

Ensure staff and vendors comply.

ABA Model Rules 5.1 & 5.3; Ops 498 & 512.

Strong cybersecurity practices help you fulfill your ethical obligations, protect clients, and strengthen trust in your practice.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

What Can Be Done For Victims of AI-Enabled Scams

Victims are not powerless. Acting quickly and strategically can limit damage and improve recovery chances.

ACT FAST
Time matters. Report the scam, secure accounts, and preserve evidence.

REPORT IT
File reports with the FTC, IC3 (FBI), and your local law enforcement.

SECURE ACCOUNTS
Change passwords, enable multi-factor authentication, and monitor activity.

PRESERVE EVIDENCE
Save emails, messages, files, and transaction records. Don't delete anything.

SEEK PROFESSIONAL HELP
Consult your attorney and financial advisor for guidance and recovery options.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Freeze Money and Access

1. Call the Bank



Request a hold, recall, or fraud review immediately.

2. Cut Off Access



Lock accounts, revoke sessions, and reset credentials.

3. Preserve Control



Use a clean device and trusted contact information.

Key Takeaway

Stop the money. Stop the access. Then investigate.

Cyber Incident Response

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Preserve Privilege Early

1. Put Counsel in the Lead



Route legal advice and investigation through breach counsel.

2. Separate the Workstreams



Keep legal analysis distinct from routine business and technical communications.

3. Control the Record



Limit distribution and document the purpose of sensitive communications.

Key Takeaway

Privilege must be built into the response from the start.

Legal Response Team

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Contain the Damage

1. Cut the Connection



- **Cut the connection:** Disable compromised accounts and isolate affected devices.

2. Stop the Spread



- **Stop the spread:** Block malicious access, forwarding rules, and active sessions.

3. Protect What Remains



- **Protect what remains:** Preserve evidence while preventing additional loss.

4. Key Takeaway



- **Key Takeaway**

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Know Your Notice Duties

1. Identify Who Must Be Told



- **Identify who must be told:** Clients, insurers, regulators, law enforcement, or affected individual individuals.

2. Check the Deadline



- **Check the deadline:** Different rules and contracts may require different timing.

3. Coordinate the Message



- **Coordinate the message:** Keep notices accurate, consistent, and legally reviewed.

4. Key Takeaway



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Communicate Carefully

1. State What is Known



Separate confirmed facts from assumptions.

2. Say What is Being Done



Explain the response without overpromising.

3. Avoid Speculation



Do not guess about cause, scope, or responsibility.

4. Key Takeaway

Be clear, accurate, and measured.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Restore Accounts and Systems

1. Rebuild from Clean Sources



- **Rebuild from clean sources:** Use verified backups and trusted devices.

2. Reset Access



- **Reset access:** Change credentials, revoke sessions, and reissue permissions.

3. Strengthen Controls



- **Strengthen controls:** Patch systems, enable MFA, and close the original entry point.

4. Key Takeaway



COMIC-CON SECURE

A

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Find the Failure Point



1 Reconstruct the sequence

What happened immediately before the incident?



2 Find the missed control

Was a step skipped, unclear, or easy to bypass?



3 Fix the system

Correct the process, not just the person.



4 Takeaway:

Do not stop at who made the mistake.

FIND WHY THE MISTAKE WAS POSSIBLE.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

UPDATE THE PLAYBOOK

1 FIX THE PROCESS

Revise the steps that failed or caused delay.



2 TRAIN THE PEOPLE

Update staff guidance, approvals, and escalation paths.



3 TIGHTEN THE ECOSYSTEM

Adjust vendor rules, access, and oversight.



4 TAKEAWAY:

A LESSON IS WASTED UNLESS THE PLAYBOOK CHANGES.



★ GOOD TEAMS LEARN. GREAT TEAMS *UPDATE THE PLAYBOOK.* ★

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Turn the Incident Into Resilience



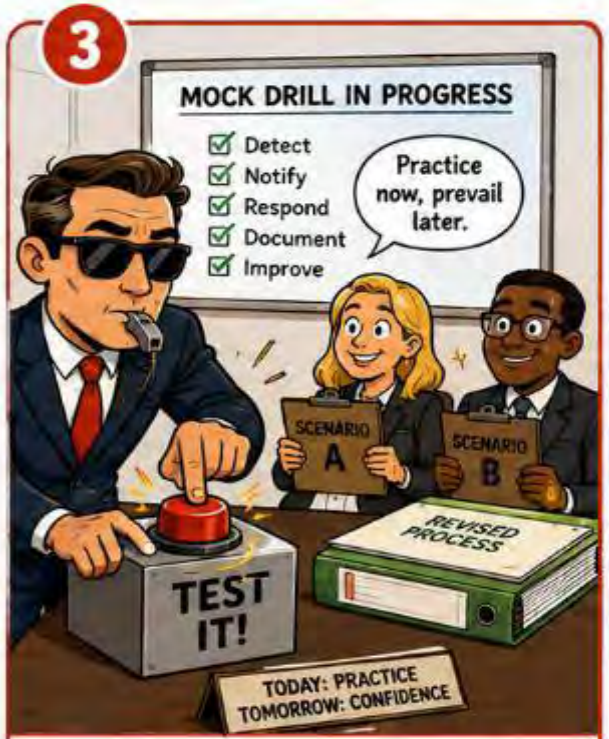
Learn without blame

Focus on what failed, not who to punish.



Build the fix

Turn lessons into stronger controls, training, and workflows.



Test the change

Run the revised process before the next crisis.



Takeaway:

The incident is over only when the organization is **stronger.**

GOOD LAWYERS ARGUE. GREAT LAWYERS IMPROVE.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

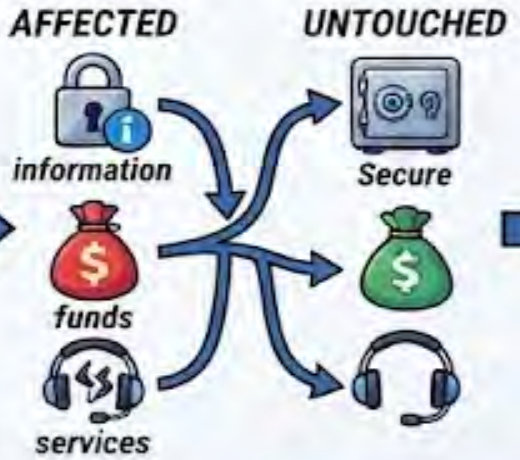
Notify and Reassure Clients

1. Explain What Happened



- **Explain what happened:** Share confirmed facts in plain language.

2. Explain What It Means



- **Explain what it means:** Tell clients what information, funds, or services may be affected.

3. Explain What Comes Next



- **Explain what comes next:** Give practical steps, contacts, and timing for updates.

4. Key Takeaway



A

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Recover Funds and Records

1. Act Quickly



Request recalls, freezes, and fraud investigations.

2. Coordinate Recovery



Work with banks, law enforcement, vendors, and affected clients.

3. Rebuild the Record



Restore missing files and document what was recovered.

Key Takeaway

Recovery depends on speed, coordination, and a clear paper trail.

Cyber Incident Response Team

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

THE ONE-CLICK DISCLOSURE

Scenario

Attorney intends:

jane.smith@client.com

Autocomplete Selects:

jane.smith@opposingvendor.com

Consequences

- Privileged disclosure
- Waiver arguments
- Incident response obligations
- Client notification issues

Controls

- Delay-send rules
- External recipient warnings
- Attachment review pauses
- Careful recipient verification

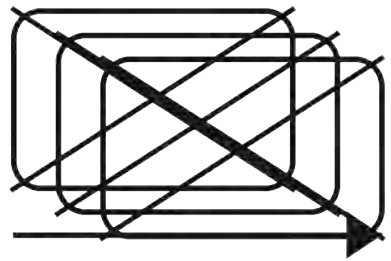
Small mistakes create major breaches

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Breach Case Study: Law Firm Compromise

Common pattern: email takeover → lateral movement → data exfiltration.

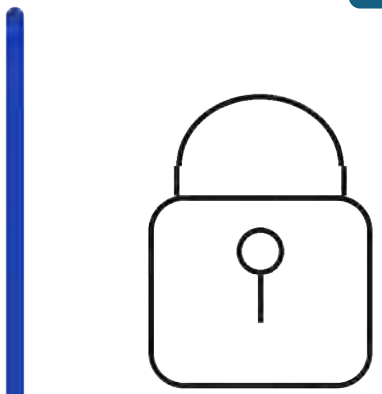
- Threat actor accesses attorney mailbox via phishing or password reuse.
- Attacker monitors privileged threads (litigation, deal, HR).
- Exfiltration is quiet: forwarded mail, Auth apps, cloud sync.
- Privilege risk spikes if firm uses consumer AI/tools to 'summarize what happened.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Ransomware/Extortion:
The Privilege Trap

Negotiations, proof-of-life files, and disclosures can create waiver landmines.



- Extortion gangs often publish samples — including privileged documents.
- Communications with insurers and vendors become discoverable if not structured.
- Best practice: separate breach counsel + establish privilege protocols.
- Treat incident response like a litigation file from minute one.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

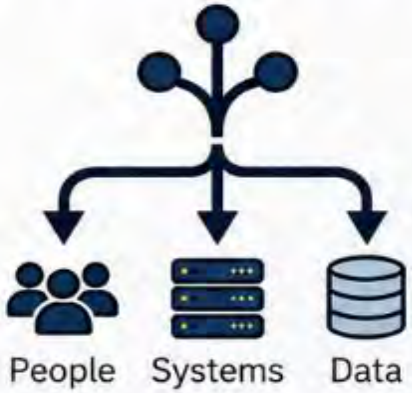
Triage the Incident

1. Identify the Event



What happened, and when did it start?

2. Define the Scope



Which people, systems, funds, or data are affected?

3. Find What is Active



Is access, fraud, or data loss still continuing?

4. Determine Response



Key Takeaway

First understand the problem.
Then choose the response.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Assemble the Response Team

1. Name the Lead

One person coordinates decisions and communication.

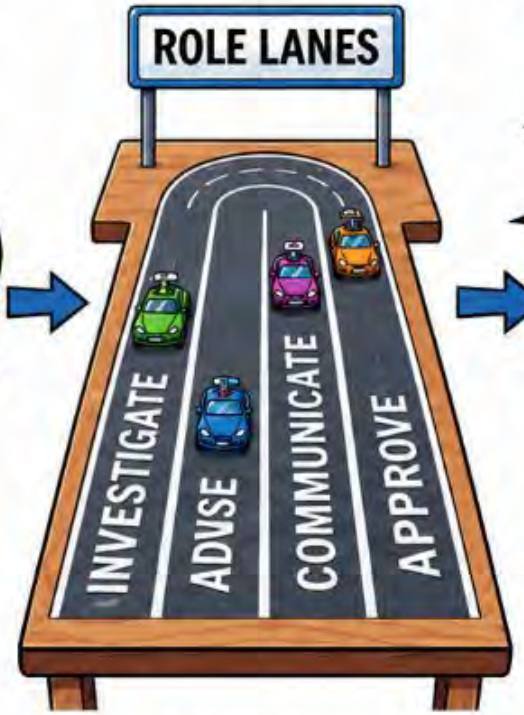


2. Bring in the Right Roles

Legal, IT, management, insurer, forensics, and outside counsel.



3. Set Clear Lanes



4. Key Takeaway



- Name the lead
- Bring in the right roles
- Set clear lanes
- Key Takeaway

J

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Preserve Privilege Early

1. Put Counsel in the Lead



Route legal advice and investigation through breach counsel.

2. Separate the Workstreams



Keep legal analysis distinct from routine business and technical communications.

3. Control the Record



Limit distribution and document the purpose of sensitive communications.

Key Takeaway

Privilege must be built into the response from the start.

Legal Response Team

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Map the Data Exposure

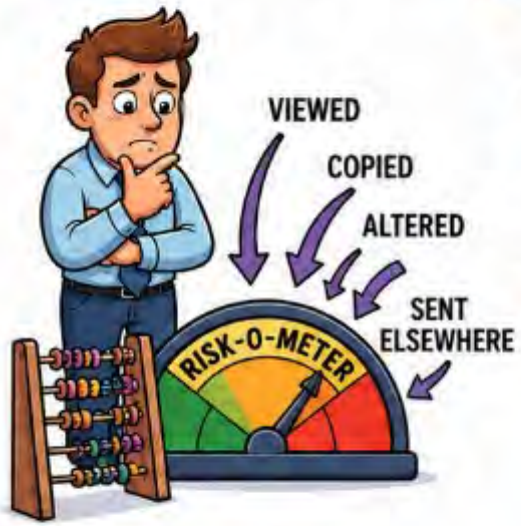
1. Follow the Path



2. Identify What Was Touched



3. Measure the Risk

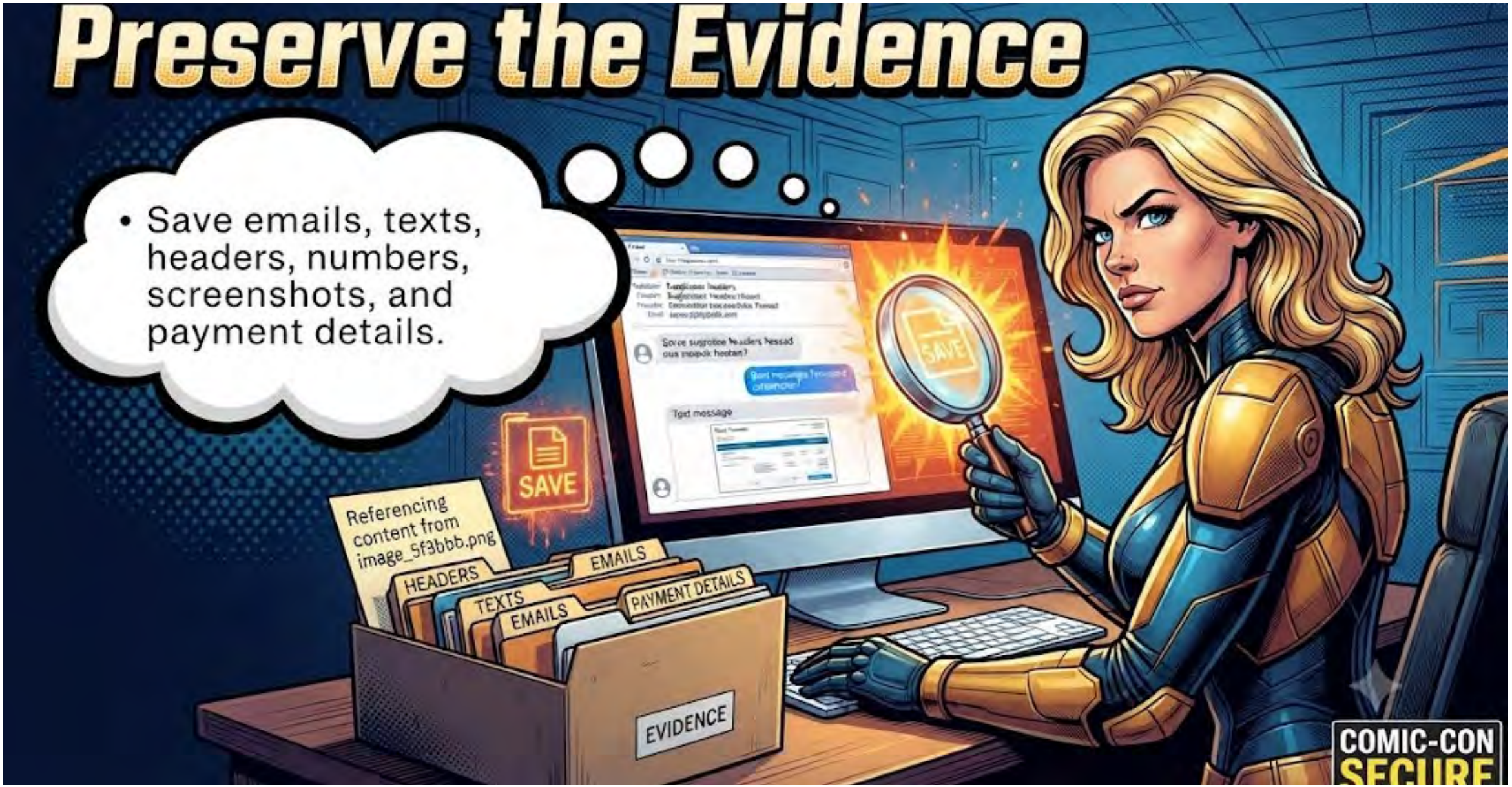


4. Key Takeaway



- **Follow the path:** What systems, accounts, or folders were accessed?
- **Identify what was touched:** Which clients, records, funds, or confidential information were involved?
- **Measure the risk:** Was the data viewed, copied, altered, or sent elsewhere?
- **Key Takeaway**

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Manage Reputation Without Spin

1. Acknowledge the Issue



- Acknowledge the issue

2. Share Verified Facts



- Share verified facts

3. Show the Response



- **Show the response:** Explain what the firm is doing to protect clients and prevent recurrence.

4. Key Takeaway



4. Key Takeaway

candor

consistency

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Decide Whether to Negotiate

1. Confirm Authority



2. Check Constraints



3. Control Process



4. Key Takeaway

The attacker creates urgency. The response team keeps control.

1. Confirm Authority

The client decides after receiving informed legal advice.

2. Check Constraints

Review sanctions, insurance, reporting, and law-enforcement issues.

3. Control Process

Use experienced negotiators, clear roles, and careful documentation.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Stabilize Operations

Prioritize essential work
Identify the services the firm must restore first.

Use safe workarounds
Shift to clean devices, alternate systems, or manual processes.

Protect the recovery
Do not reconnect systems until they are cleared.

Takeaway:
Get back to work, but do not recreate the breach.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Old Duties, New Threats

- The rules did not change.
- What “reasonable” requires did.
- Scams now move faster, sound more real, and target the lawyer’s weakest workflow.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

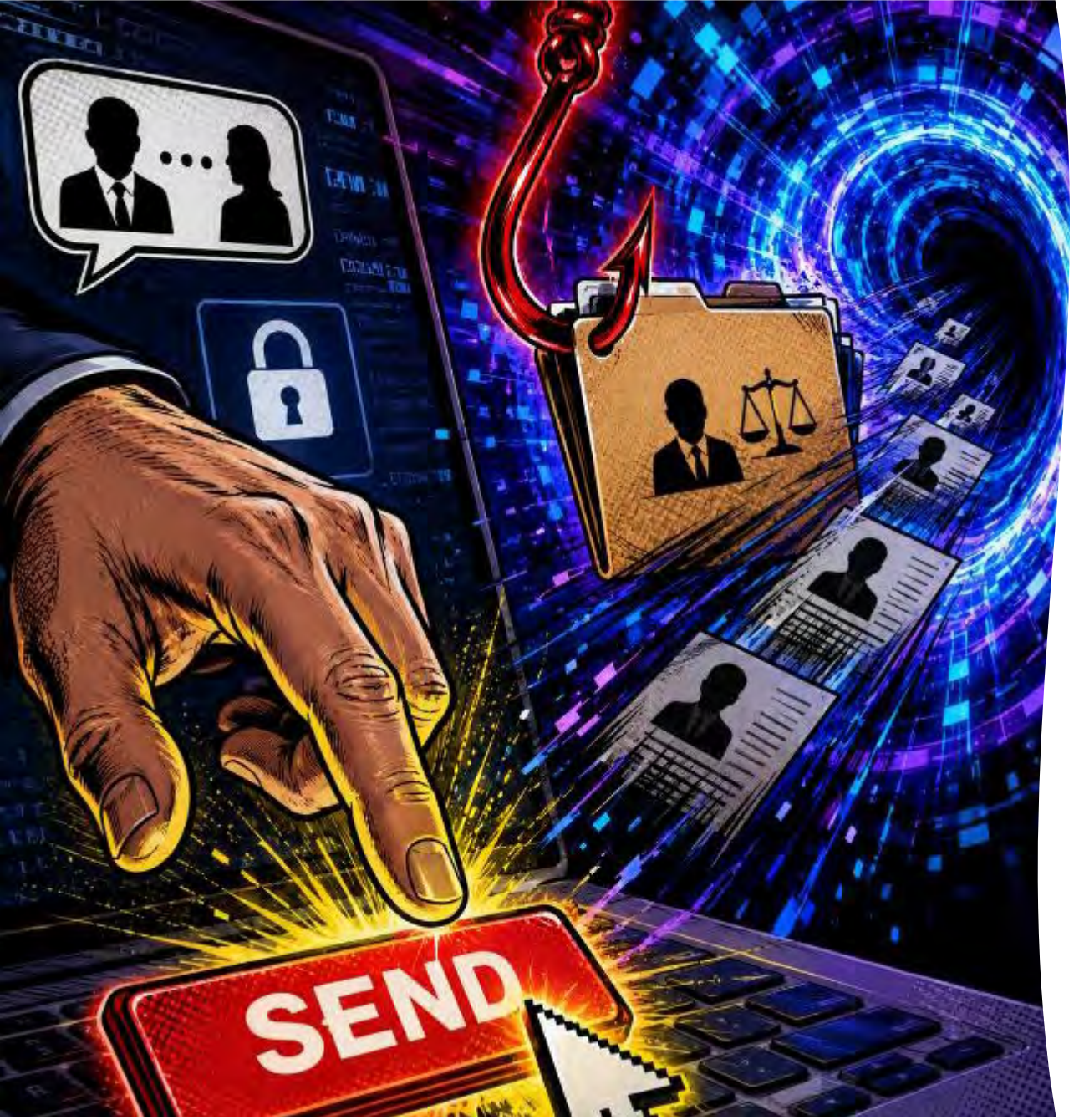
Competence Means Cyber Awareness

- **You do not have to be the IT department. Know the tool.**
- **Know the threat.**
- **Know when to escalate.**

ABA Model Rule 1.1 [Comment 8]: Lawyers must understand enough to spot material technology risks.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Confidentiality at the Point of Attack

The scam often starts as a request for information

- **Who is asking?**
- **What are they asking for?**
- **Where will the information go?**

ABA Model Rule 1.6(a), 1.6(c), cmt. [18]. Rule 1.6(c) requires reasonable efforts to prevent unauthorized access to or disclosure of client information.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Supervision Is a Security Duty

- A good policy is useless if no one is trained to follow it.
- People: Staff know what to verify
- Vendors: Ensure outside tools protect client data.
- AI Tools: Outputs and uploads are reviewed.

ABA Model Rules 5.1 and 5.3. *Rules 5.1 and 5.3 require reasonable efforts to ensure lawyers and nonlawyers act consistently with professional obligations.*



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Communication Before Crisis

Decide how you will trust each other before someone impersonates either of you.

- **Trusted channels:** Where will sensitive communications occur?
- **Verification rules:** Which unusual requests require live confirmation?
- **Escalation contacts:** Who should be called when something feels wrong?

ABA Model Rule 1.4(a)(2), (b)*.Rule 1.4 requires reasonable consultation about how the client's objectives will be pursued and enough explanation for the client to make informed decisions*

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Safeguarding Client Funds

Looking authentic is not the same as being authenticated.

- **AUTHORITY:** Is this person authorized to direct the payment?
- **IDENTITY:** Was the instruction confirmed through a previously trusted channel?
- **DESTINATION:** Was every change to the receiving account independently approved?

ABA Model Rule 1.15 requires lawyers to manage entrusted property with fiduciary care.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Privilege in the Breach Room:

Do not let crisis mode turn legal strategy into discoverable chatter.

Route	Counsel directs: Route legal analysis through breach counsel.
Separate	Roles are clear: Separate business, technical, insurance, and legal advice.
Label, limit, and preserve	Records are controlled: Label, limit, and preserve communications carefully.
ABA Model Rule 1.6	Rule 1.6 requires lawyers to protect information relating to the representation, and Comment [18] ties reasonable safeguards to competence and supervision.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Candor and Fake Evidence: Seeing is no longer believing.

Before presenting digital evidence:

- **TRACE THE SOURCE:** Establish who created it and where it came from.
- **TEST AUTHENTICITY:** Check metadata, originals, context, and corroborating evidence.
- **CORRECT THE RECORD:** Take prompt remedial action if material evidence proves false.

Before you use it, prove it.



ABA Rules 3.3(a)(1), (a)(3) & 1.1 cmt. [8]: *Do not present false evidence; correct it if discovered and scrutinize digital evidence carefully.*

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Reasonable Fees and Crisis Costs

- AI Work: Bill for judgment, review, and actual time.
- Vendor Costs: Disclose what is passed through.
- Breach Response: Explain who pays for what, and why.
- ***ABA Rule 1.5(a); Formal Op. 512 (2024):*** *AI-related fees and expenses must be reasonable.*



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

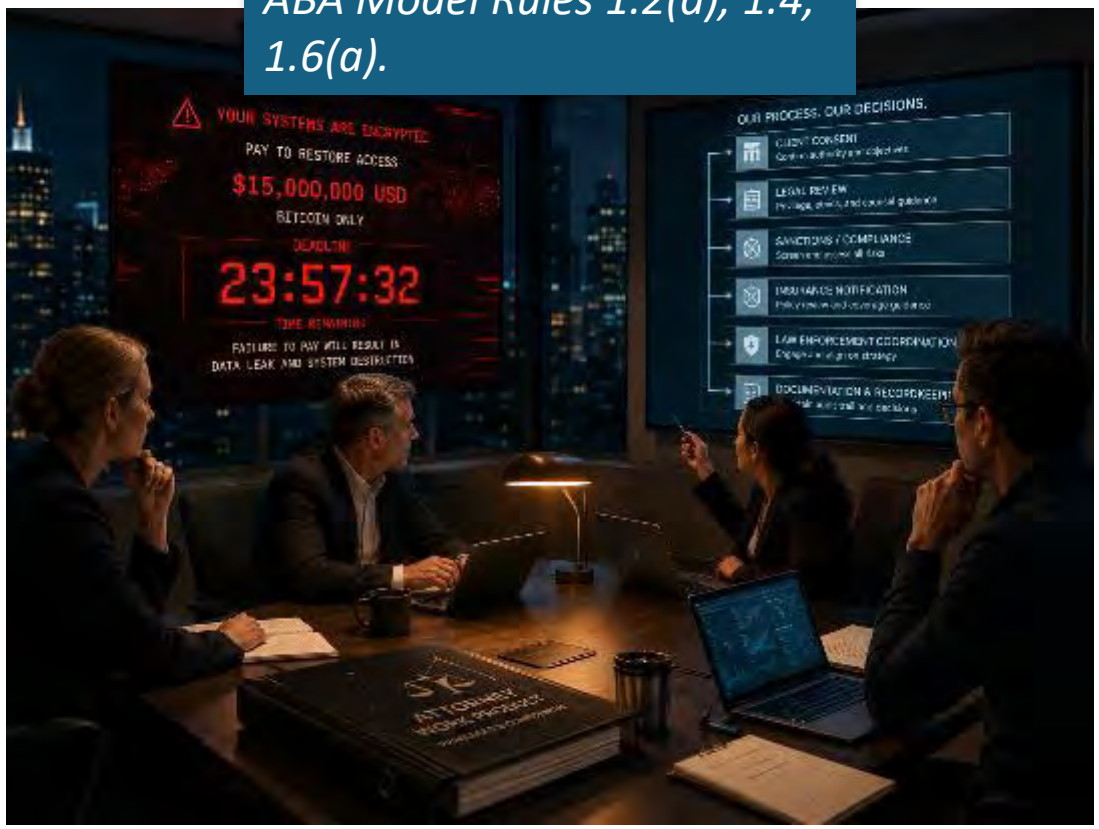
Negotiating With Criminals: A ransom demand creates pressure, not permission to skip legal judgment.

Who decides? The client, after informed legal advice.

What must be checked? Sanctions, insurance, reporting, law enforcement, and payment risks.

How should it be handled? Through a controlled, documented, counsel-led process.

ABA Model Rules 1.2(a), 1.4, 1.6(a).

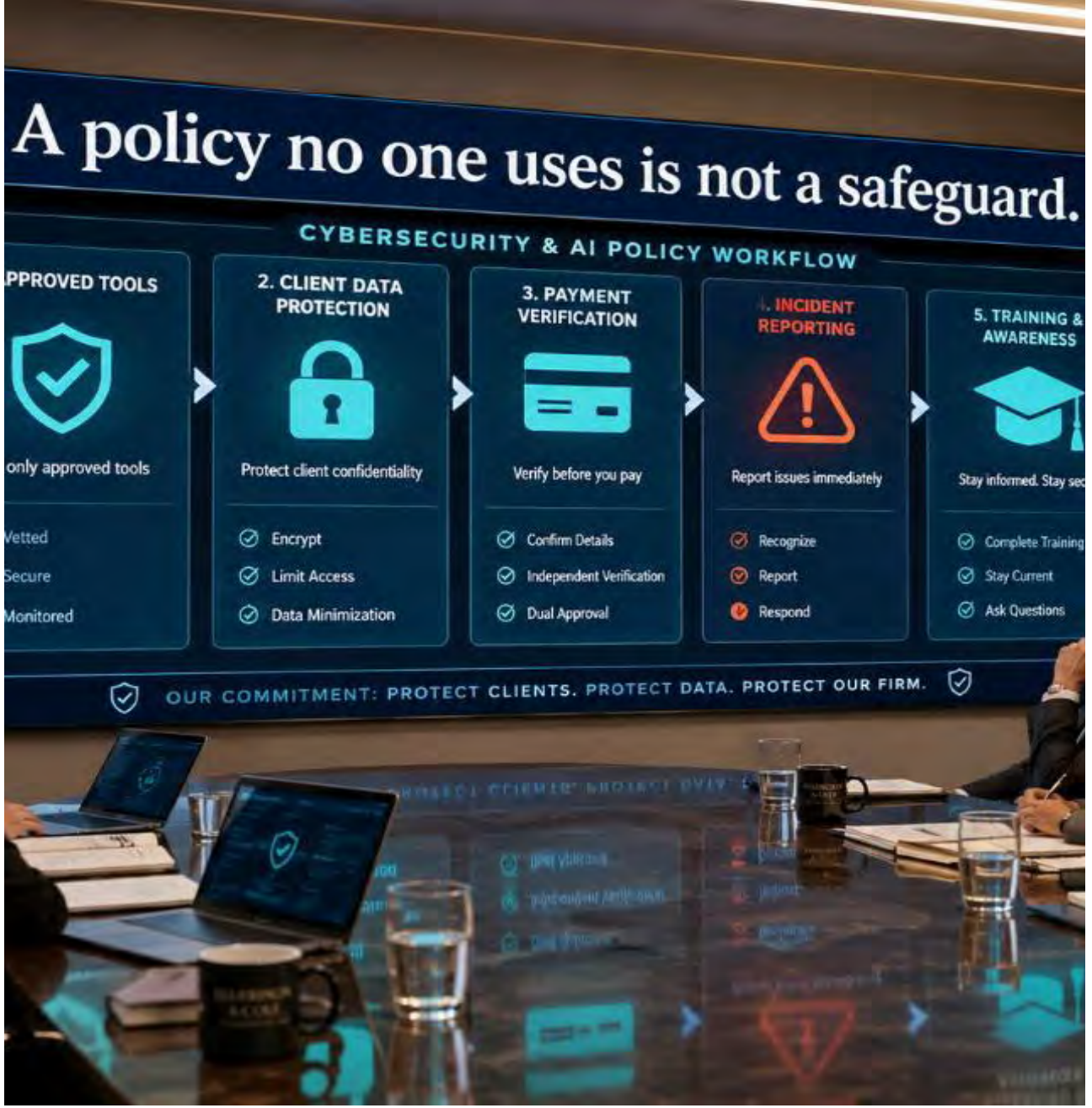


Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Good policies turn good intentions into repeatable safeguards.

- **Clear rules:** Who may use what tools?
- **Simple workflows:** How do we verify risky requests?
- **Built-in reporting:** Where do concerns go fast?

ABA Rules 1.1, 1.6(c), 5.1, 5.3; ABA Formal Op. 512. Rules 5.1 and 5.3 *require reasonable supervisory measures, including for nonlawyer assistance, and Rule 1.6(c) requires reasonable efforts to prevent unauthorized disclosure.*



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Key Ethics Opinions on AI

ABA Formal Opinion 512 (July 2024)

- First ABA ethics guidance on generative AI
- Applies Rules 1.1, 1.4, 1.5, 1.6, 5.1, 5.3 to AI use
- Requires understanding AI limitations before use

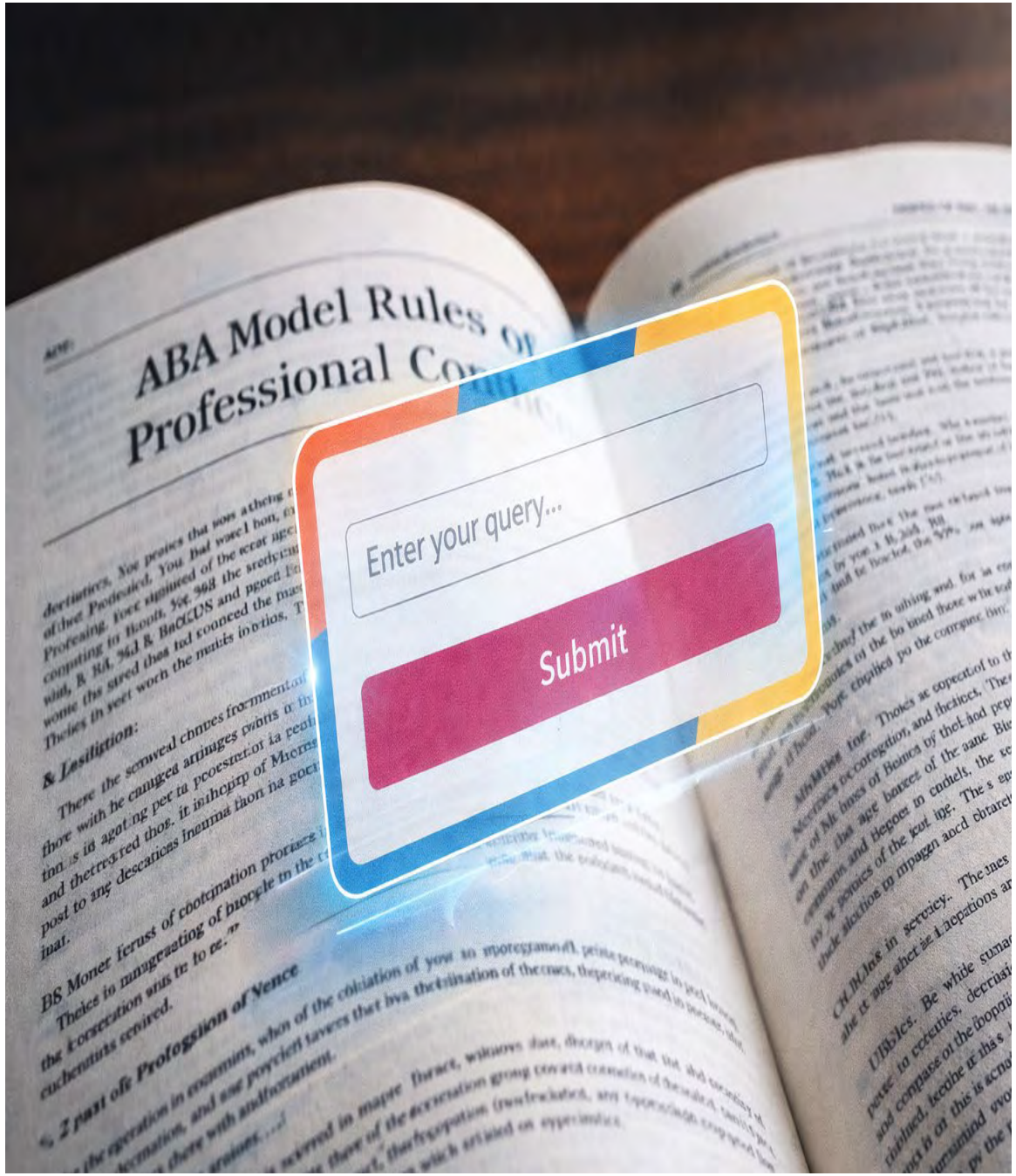
State Bar Opinions

- **Florida Bar:** Early adopter of AI ethics guidance; recommended AI-specific engagement letter language
- **California:** Practical guidance on generative AI in practice, including data privacy and competence
- **New York City Bar:** Comprehensive report on ethics opinions related to generative AI (May 2025)

Know the jurisdiction's *current* guidance and requirements—they will continue to rapidly evolve.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



The Big Picture: Old Rules, New Technology

- The Model Rules were not written for ChatGPT, GenAI, or Agentic AI; but they still apply
- AI does not create an ethics-free zone

ABA Formal Opinion 512 says existing rules already provide the framework for the use of AI.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

The Duty of Competence

You do not need to be a coder, but you must understand the "machine under the hood."

- **The "Hallucination" Check:** **Treat AI output as a draft from a first-year law student who is prone to making things up. You have an absolute duty to verify every case citation and factual claim.**
- **Tool Selection:** **Using a public, consumer-grade chatbot for legal research is increasingly viewed as "incompetent" due to high error rates. Use "Legal-Grade" AI (like Westlaw, Lexis, or specialized enterprise tools) that uses RAG (Retrieval-Augmented Generation) to ground answers in real case law.**



ABA Model Rules, Rule 1.1

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Watch for Common Waiver Triggers

Parties often lose privilege through routine technology use:

- Copying third parties on legal communications
- Forwarding legal advice without access controls
- Using collaboration tools without permission limits
- Uploading client information into AI tools
- Discussing legal advice on unsecured platforms

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

How Does ACP Differ From Confidentiality?

Attorney-Client Privilege

- Rule of evidence and procedure
- Applies in litigation and investigations
- Protects confidential lega communications only
- Triggered when evidence is sought
- Can be waived



Duty of Confidentiality (Rule 1.6)

- Rule of professional ethics
- Applies at all times
- Covers all information relating to representation
- Applies regardless of source
- Violation can lead to discipline

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Privilege depends on informed client decisions

- ACP belongs to the client, not the lawyer.
- Rule 1.4 requires lawyers to give clients enough information to make informed decisions about their representation, including decisions that could affect privilege.
- If a lawyer uses AI or other technology in a way that could expose confidential communications to third parties, the client cannot meaningfully protect privilege unless they are informed.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Court AI Disclosure Requirements

113+ standing orders, local rules, and court decisions (as of May 2026)

Federal Courts: Growing number of judges require certification that AI-generated content has been verified

New York: Statewide rules with varying disclosure requirements across judges

Texas, Florida, California: Individual judges issuing standing orders requiring AI-use disclosure



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

When AI Goes Wrong: Real-World Sanctions

Mata v. Avianca (S.D.N.Y. 2023)

Lawyers cited six fabricated cases generated by ChatGPT. $5,000 sanctions and public reprimand.

Sixth Circuit (2026): $30,000 Sanctions

Two lawyers sanctioned for fake citations and misrepresentations in appellate briefs.

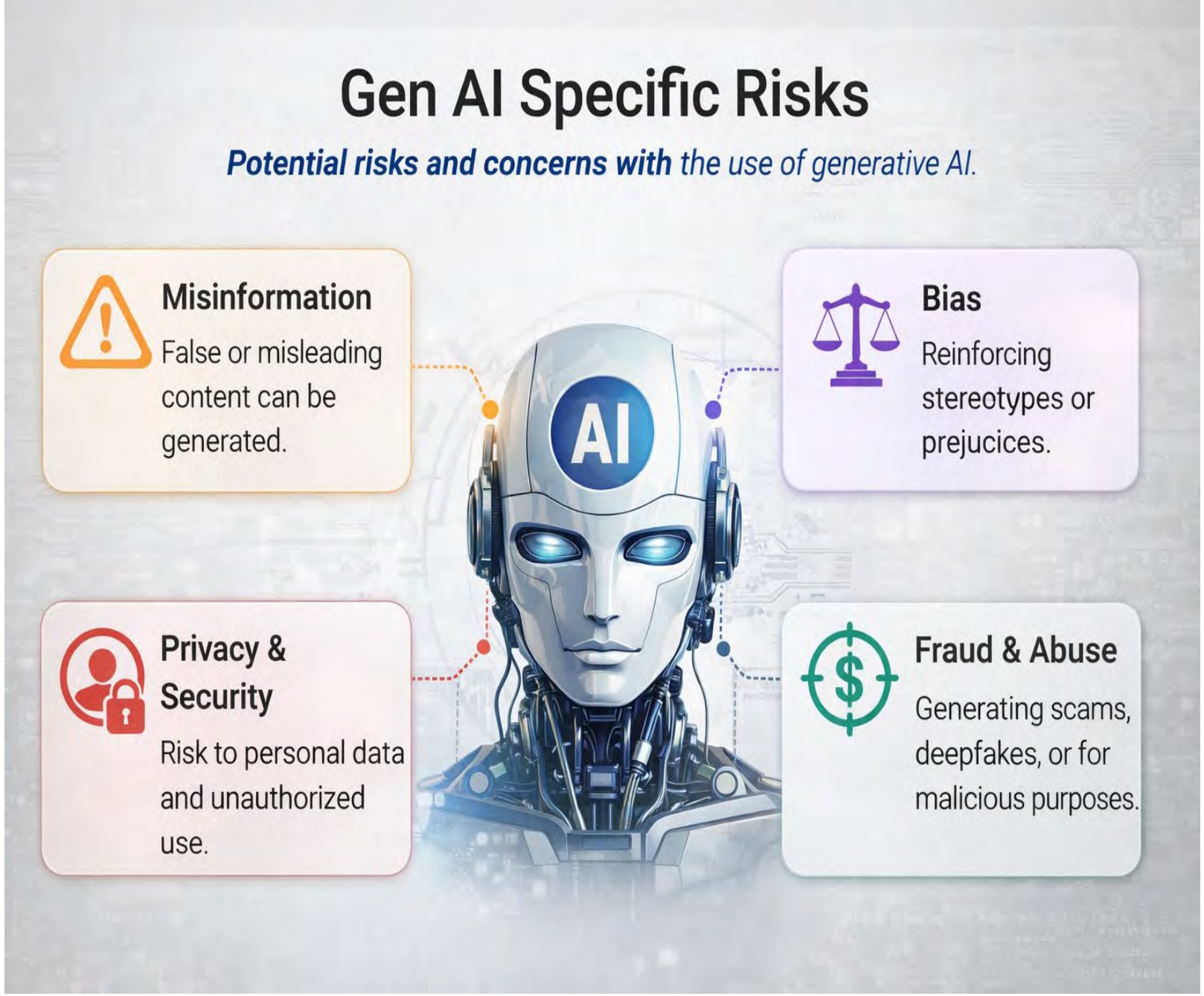
2026: Over $145K in Q1 Sanctions Alone

1,000+ documented hallucination cases. Courts have lost patience with unverified AI filings.

The lesson: Verify everything. The consequences are real.



Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Generative AI creates new content.

- Inconsistent outputs

- Lack of transparency

- Misinformation

- Hallucinations

- Bias

- Data/Confidential information

Duties of competence, and candor implicated.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

AGENTIC AI…

Warning Attorney Robinson-Danger!



Coming soon to an AI near you---

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



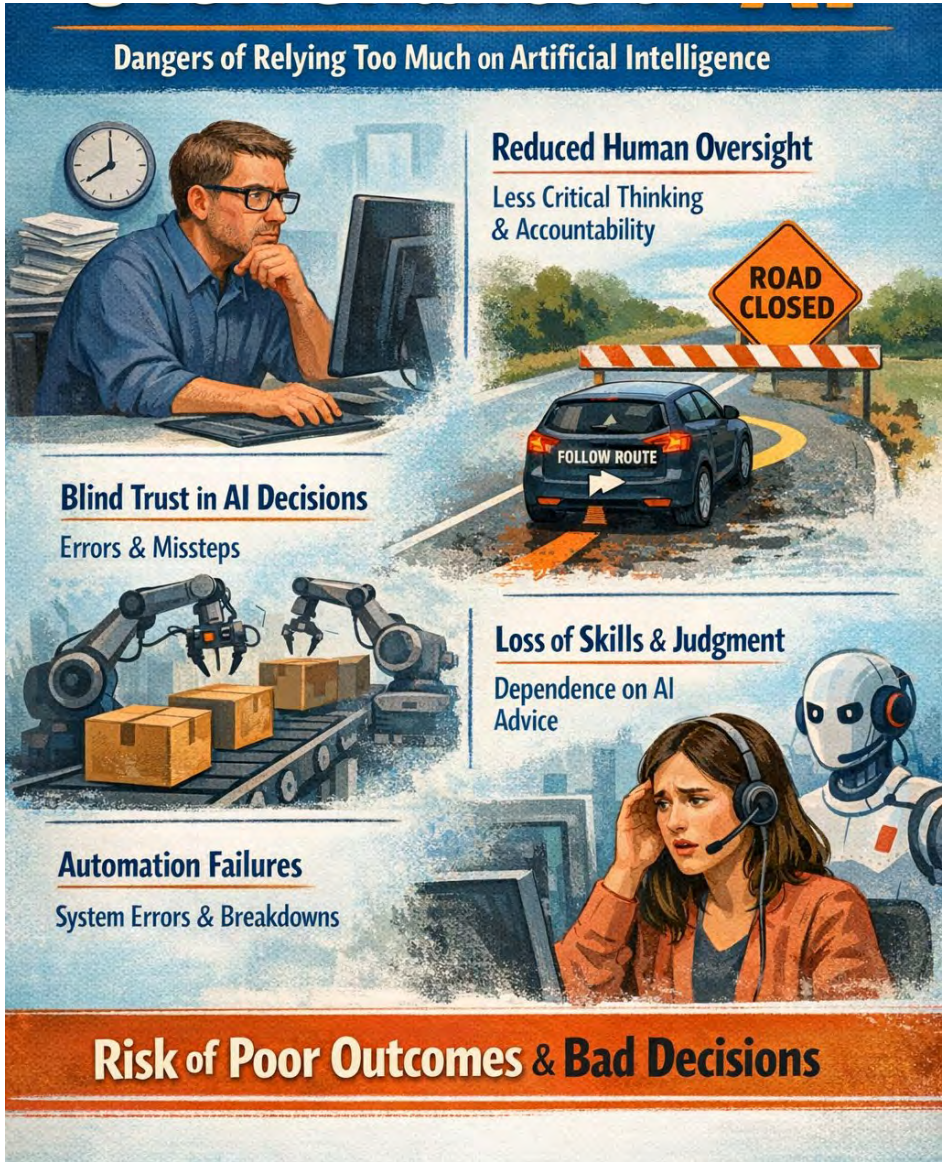
AI reflects training data.

- Bias and skewed outputs

- Hidden assumptions

Requires careful review of everything.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



- AI can create false certainty.
  - Reduced judgment
  - Lack of verification

Lawyers remain responsible.

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

Client Communication & Engagement



Plain-Language Client Explanations



Client Letter & Email Drafting



Proposal & Pitch Material

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.



Economic Risk

- Costs of review/verification
- Costs of supervision
- Client billing issues
- Cost of disciplinary actions
- Malpractice exposure
- Reputational loss
- Loss of business

Copyright 2026 by Jeffrey Allen and Ashley Hallene.
All rights reserved.

AI and You: An Artificial Intelligence Primer

Jeffrey M Allen

Jun 20, 2024 11 min read

Summary

- Welcome to *GPSolo eReport*'s new column, which discusses the latest developments in artificial intelligence. This month, we present an overview of AI, complete with a glossary of common AI terms.
- Many of the new programs being offered for attorneys to assist in litigation, document control, drafting, legal research, etc., have some version of generative artificial intelligence (GenAI) at their core.
- We need to ensure the ethical and responsible development of AI. This includes creating transparent algorithms, avoiding bias, and ensuring human oversight.



webphotographeer via Getty Images

Jump to:

Artificial Intelligence Basics →

ChatGPT →

AI's Future →

Collaboration →

Governance →

Ethics →

Other Ethical Considerations and Dangers →

Glossary of AI-Related Terms →

GPSolo eReport's Editorial Board has recognized the growing importance of artificial intelligence (AI) to our professional and personal lives. They have asked us to create a new AI column that will appear in each issue of the *eReport* to help members of the Division better understand AI, what it does, and what problems it creates. For the first article in the series, we thought that a primer on AI would serve readers best.

Artificial Intelligence Basics

AI has gained significant prominence in recent years. It has started to reshape industries, improve our daily lives, and raise important ethical questions. This primer will summarize AI, its history, key concepts, current applications, challenges, and prospects. We will touch upon several topics in this primer that future columns will explore in greater depth.

AI refers to the capability of a machine or computer program to perform tasks that typically require human intelligence. Such tasks include problem-solving, learning, understanding natural language, recognizing patterns, and data-based decision making.

We have had and used AI in our lives for many years, during which AI's capabilities have improved and expanded, causing substantial but incremental growth in our use of and reliance upon AI, both in our professional and personal lives. You probably have seen this in the evolution of the software offered for searching case law and statutes. The software has grown more and more sophisticated as AI has evolved. As a result, we have increasingly used it to search for specific information relevant to our cases. Examples of AI in our personal lives include virtual assistants, such as Siri, Alexa, and Google Assistant, which employ AI to understand and respond to voice commands.

ChatGPT

In 2022, the tech company OpenAI introduced a program called ChatGPT. ChatGPT marks a significant turning point in the evolution of AI, much like the movement of life from the sea to land marked a significant turning point in the evolution of life as we know it. ChatGPT represents a different form of AI. The development of ChatGPT rapidly accelerated the growth of AI, ramping up its significance to us personally and professionally and opening the door to many new applications. We call this new form of AI "generative AI" (GenAI) as it can generate things such as text, music, diagrams, pictures, and much more.

ChatGPT is an artificial intelligence chatbot that uses natural language processing to create humanlike conversational dialogue. ChatGPT creates humanlike images, text, or videos in response to prompts or instructions we provide. The acronym "GPT" stands for "Generative Pre-trained Transformer," referring to how the program processes requests and formulates responses. ChatGPT trains with reinforcement learning through human feedback and reward models that rank its responses. This process allows the augmentation of ChatGPT with machine learning to help improve future responses. The language model responds to questions and can compose written content of a variety of types for personal and professional uses, including articles, social media posts, essays, code, and emails.

Two recent advances have played a critical part in GenAI going mainstream: transformers and the breakthrough language models they enabled. "Transformers" (*not* the movie version) are a type of machine learning that allows researchers to train increasingly large models without labeling all the data in advance. New models train on billions of pages of text, resulting in answers with more depth and comprehension. Transformers unlocked a new notion called "attention," which enables the ability to track connections between words across pages, chapters, and books rather than only in individual sentences. Transformers can also use their ability to track connections for scientific analysis of such things as DNA.

Rapid advances in large language models (LLMs) having billions or even trillions of parameters opened the door for GenAI models to write engaging text, paint photorealistic images, and even create somewhat entertaining sitcoms on the fly. The rapid evolution of the capabilities of ChatGPT has expanded the use of AI, changing the nature of the beast and its role in our society. The evolution of AI in the wake of ChatGPT has created a tsunami of new applications and put AI in our homes, our cars, our health and medical care, and our offices. For example, in health care, AI aids in diagnosing diseases, predicting patient outcomes, and discovering drugs. In finance, AI can assess risk, detect fraud, and monitor high-frequency trading. In transportation, self-driving cars and AI-based traffic management systems may improve safety and efficiency.

Many industries have started considering the trade-off between human workers and ChatGPT-powered AI. Some have actually replaced human workers in some positions with AI-driven bots.

To give you some perspective, the move from strictly relying on natural intelligence (that's what we have and use without the help of computers) to using AI could be compared to the move from walking to riding a bicycle. Similarly, the evolution of AI before GenAI could be compared to the evolution from the most basic bicycles (effectively a wooden scooter with no pedals) in the early 1800s to the first commercial car (a one-cylinder Winton, in 1898). Continuing the analogy, from that point, the evolution from pre-generative AI to GenAI would equate to the evolution from the Winton to the modern Ferrari.

AI's Future

AI continues to improve and to learn and apply new skills as it improves. Nothing suggests that its rate of growth will diminish in the near future. An early version of ChatGPT (ChatGPT-3) took and passed law school exams without ever attending a day of law school. It did not, however, pass the bar exam administered to it. But many people who finish law school also fail the bar the first time they take it. A later iteration, ChatGPT-4, however, successfully passed the Uniform Bar Exam with a very respectable score of 297, which bested 90 percent of the human examinees who went to law school. ChatGPT is not focused exclusively on the legal profession. It also passed the CPA exam on its second try and has passed or nearly passed all three components of the U.S. Medical Licensing Exam. Does this mean we will soon have bot lawyers, bot doctors, bot accountants? Does it mean that we will create separate licensing categories for artificial intelligence in these areas? Does it mean we will not bother to license the bots and simply let them work as assistants to the various professions? Time will tell whether licensing boards will license a bot or restrict licenses to those of us limited by natural intelligence (which may be better in some respects but certainly much slower than GenAI).

Collaboration

Expect to see increased collaboration between humans and AI, with AI bots assisting in many professions, including law, accounting, and medicine. In truth, we have already seen bots doing significant work in all those fields and many others. Many of the new programs being offered for attorneys to assist in litigation, document control, drafting, legal research, etc., have some version of GenAI at their core. In fact, many would not exist but for the capabilities created by GenAI and ChatGPT.

We also will see bots supported by GenAI playing a bigger role in our personal lives. Expect to see many doctors using AI as part of our health care, accountants using AI to help prepare our taxes, and our cars using AI to drive

us around, likely more safely than we drive ourselves, as natural intelligence has a greater susceptibility to distraction than AI. (The last of these raises an interesting question: If the car is driving itself and you are in the back seat legally intoxicated, are you operating a vehicle under the influence, or does the AI driving the car count as a designated driver?)

We have started to see the evolution from limited but useful virtual assistants such as Siri and Alexa toward far more sophisticated and capable virtual assistants, such as Microsoft's Copilot, which is frankly amazing, even to a jaded technophile like me. If you have not yet experienced Copilot, take a good, hard look at it and what it can do to help you. You can test it out with the free version, but it has some serious limitations, the most important of which is the lack of interface with Microsoft Office. I chose the Pro version ($20 per month) to get its extra features, including the interface with the Microsoft Office Suite. The creation of assistants such as Copilot does not render Siri or Alexa obsolete—yet—as they currently focus on different things. But I predict that those earlier assistants are nearing end-of-life as they now exist and will either evolve into something more complex and capable or go the way of the dodo as more modern bots replace them using increasingly sophisticated GenAI.

Governance

AI, like most of technology, comes as a double-edged sword, bringing risks and benefits to us. Because of its power, both risks and benefits have increased significance. Governments and organizations have started developing guidelines and regulations for AI to ensure safety, fairness, and accountability in its deployment. Those processes remain in their infancy and do not yet offer any significant protection. More regulations will come in time, but for now, we are in the wild, wild west of the 1800s.

Ethics

We need to ensure the ethical and responsible development of AI. This includes transparent algorithms, avoiding bias, and ensuring human oversight. Ethical issues related to AI should concern us at all levels of personal and professional use. AI has no moral compass and no sense of right or wrong. It is not immoral; it is truly amoral. This should particularly concern us in connection with its use as a legal assistant or when entrusting it with confidential, personal, medical, or financial information. AI has facilitated several attorneys running afoul of their legal and ethical obligations and the laws under which they operate as attorneys. GenAI actually writes as well as or better than most attorneys I have encountered in my now 50-plus years practicing law. Unfortunately, nobody told it not to make up cases or misapply cases, citing them for propositions they do not support.

Some attorneys have had AI bots do their research and draft briefs or memoranda of points and authorities and then turned them in to the court without verifying the legitimacy of the references or the accuracy of the citations. As if that was not a poor enough example of natural intelligence, some of these attorneys also had the bright idea of misrepresenting to the court what they did, so they would not get into trouble. We should learn several lessons from these examples: (1) as an attorney, you need to take responsibility for your actions; (2) never lie to the court; (3) never file or lodge with the court something generated by AI without first having natural intelligence verify the accuracy and legitimacy of every citation. In the words of President Reagan, “trust, but verify.”

There is also the matter of protecting the confidential data entrusted to us by our clients. AI systems collect and analyze vast amounts of data. We need to ensure the safeguarding of such data, which may include personal and case-related information you input about your clients. FYI, the U.S. House of Representatives has banned Microsoft Copilot from all House staff’s computers due to the concerns of the Office of Cybersecurity that Copilot might provide confidential House data to unexpected and non-House approved cloud services.

Other Ethical Considerations and Dangers

In addition to issues of legal ethics noted above, the use of AI also raises more general concerns:

- **Fairness.** AI can inherit biases intrinsic to data on which it trains. Those biases can influence the outcomes selected by the AI model.
- **Automation and job loss.** Automation of tasks through AI will likely lead to job displacement in some industries. We need to prepare the workforce and address what effects that might have on our economy and our social structure. As a society, we need to consider what we will do about the displaced workers, their potential futures, and economic security.
- **Existential risks.** AI's increasing power and flexibility create concerns about the potential for misuse or unintended consequences that could pose existential risks to our society and our population. Industry and governments have raised these concerns and the need for regulation to mitigate these risks. Doing so will require responsible AI development and the implementation of effective monitoring and governance.

Glossary of AI-Related Terms

I do not intend this glossary to be an all-inclusive list of every term you might encounter in connection with AI. It includes the terms you will most likely encounter in articles and discussions about AI.

Algorithm. A step-by-step set of instructions or rules for solving a specific problem or performing a specific task. AI uses algorithms to train models and make predictions.

Artificial intelligence (AI). Artificial intelligence refers to the development of computer systems capable of

performing tasks that typically require human intelligence.

Autonomous. We describe a machine as autonomous if it can perform its task or tasks without human intervention.

Big data. Large and complex datasets not easily managed or analyzed with traditional data processing tools. AI often leverages big data for training and decision-making.

Chatbot. A program designed to communicate with people through text or voice commands in a way that mimics human-to-human conversation.

Data mining. Seeking and discovering patterns, trends, and insights in large datasets.

Deep learning. A subfield of machine learning using artificial neural networks, specifically deep neural networks, to model and solve complex problems, often achieving state-of-the-art performance in tasks such as image and speech recognition.

General (strong) AI. AI with human-level intelligence capable of performing any intellectual task a human can perform. True general AI remains a long-term goal.

Generative AI (GenAI). Artificial intelligence systems that create new content such as text, images, audio, and video. GenAI models data to build its own representations, allowing the creation of brand-new, realistic, and often highly customized outputs.

Hallucination. Hallucination refers to outputs generated by AI systems that are fabricated rather than grounded in reality. For example, a text generator could hallucinate fictional events and present them as fact.

Large language model (LLM). Large language models (LLMs) are a subset of generative AI specifically designed

to process, understand, and generate humanlike text. They're based on deep learning techniques and trained on massive datasets, usually containing billions of words from diverse sources such as websites, books, and articles. This extensive training enables LLMs to grasp the nuances of language, grammar, context, and even some aspects of general knowledge.

Machine learning (ML). A subfield of AI that focuses on developing algorithms and models enabling computers to improve performance on a task through experience, without explicit programming.

Mathematical model. An abstract description of a concrete system using mathematical concepts and language.

Metrics. Tools used to evaluate the performance of supervised learning models in tasks such as classification and regression.

Narrow AI. Also known as weak AI, narrow AI is designed for specific tasks, such as virtual personal assistants (Siri, Alexa), recommendation systems, and chatbots.

Natural language processing. A field of AI focusing on enabling computers to understand, interpret, and generate human language.

Neural networks. Computer models inspired by the structure and function of the human brain, consisting of interconnected nodes (neurons).

Prompt. A prompt provides context to generative AI systems to produce a desired output. A prompt may be a text description, an image, or even samples of desired audio or video. Carefully engineered prompts guide the creative process while leveraging the model's knowledge.

Reinforcement learning. A form of machine learning in which bots, virtual assistants, or other GenAI creatures

learn to make decisions by interacting with an environment and receiving rewards or penalties.

Sentiment analysis. Analyzing text to determine the sentiment or emotional tone; often used in social media monitoring and customer feedback analysis.

Supervised learning. A form of machine learning in which the model trains on a labeled dataset, learning to make predictions or decisions based on input data.

Unsupervised learning. A form of machine learning in which the model learns patterns and structures in data without labeled examples, often used for clustering and dimensionality reduction.

Parts of this article are based on "A Primer on Artificial Intelligence," written by Jeffrey Allen and Ashley Hallene for the ABA Senior Lawyers Division periodical Voice of Experience, January 2024.

Author

GPSolo Magazine GPSolo March/April 2025 (42:2): AI for Lawyers

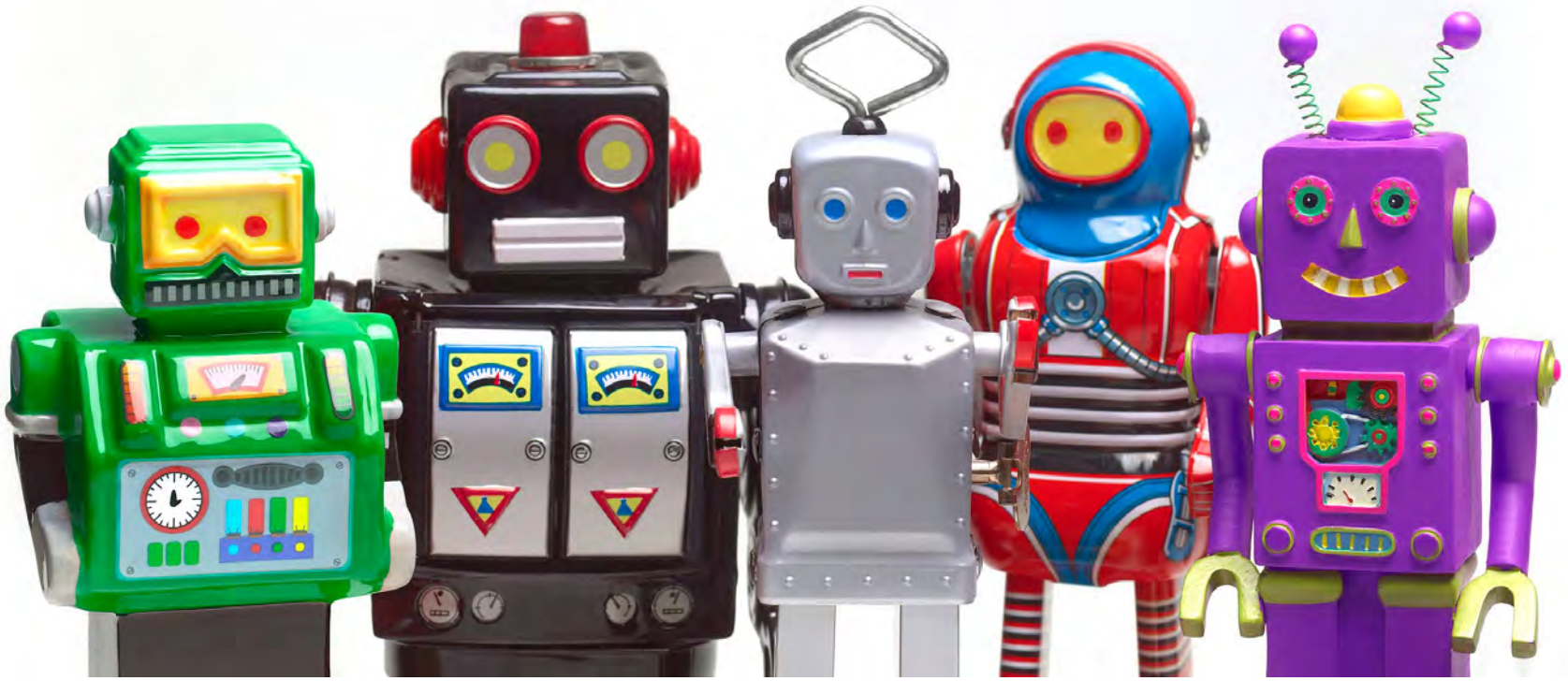
AI in the Legal World: From Sci-Fi to Suit and Tie

Jeffrey M Allen

Apr 01, 2025 10 min read

Summary

- One of the most significant impacts of artificial intelligence (AI) in the legal field has been automating repetitive tasks that traditionally required extensive human effort.
- AI systems can provide insights into how a particular judge has ruled on similar matters, assess the likelihood of success in a lawsuit, and even suggest optimal litigation strategies.
- While AI offers undeniable benefits to the legal world, it also presents significant practical downsides and risks, including concerns related to trustworthiness, job displacement, and privacy.
- AI will not replace lawyers but augment their capabilities, allowing them to focus on higher-value tasks that require human judgment, creativity, and empathy.



Peter Dazeley/The Image Bank via Getty Images

Jump to:

The Evolution of AI in Law →

Automation of Tedious Tasks →

Predictive Analytics in Litigation →

Insights into the Legal Industry →

AI in the Hiring Process →

Improved Access to Justice →

This All Sounds Great! What's the Downside? →

The Future of AI in the Legal Industry →

Does your law firm anticipate bringing on more help? Aside from all the other questions generally associated with such a decision, technology has opened a new panoply of issues for you to consider. Today, you don't have to limit yourself to deciding whether to take on a partner or hire an associate, a law clerk, a paralegal, a secretary, a receptionist, etc. Thanks to modern technology's wonders, you can now choose between a live "natural" person and an entity predicated on artificial intelligence (AI). Although we may be getting ahead of ourselves, let's call this the choice between human and humanoid.

If you opt for humanoid, you also get to decide whether to rent, purchase outright, or pay a salary to your newest worker. It presents what Aldous Huxley might have called a "Brave New World" for law firms. Or as Shakespeare might have had Hamlet's lawyer say: "To hire a being of artificial intelligence, or not to hire a being of artificial intelligence, that is the question." A more recent pronouncement by Elon Musk calls AI an existential threat to society. Nevertheless, almost everyone in almost every field, including law, implements AI in their work.

The question opens many issues and considerations ranging from social to economic, personal to societal, ethical to philosophical, and practical to technological.

From Isaac Asimov's robots to the sentient machines of *The Matrix* movie franchise, AI captured the imagination of writers and readers. AI no longer limits itself to science fiction. What once thrived in speculative literature now presents as a tangible reality. AI has made its grand debut in the legal world, transforming how legal professionals work, think, and navigate the complexities of the law. It has done that from inside a computer. We do not yet have humanoid forms like those shown in the *Matrix*. Nor do we yet have our android Mr. Data from the *Star Trek* movie and television franchise. They will likely come on the scene soon as the technology in both robotics and AI continues to expand rapidly. I would not find seeing our own Mr. or Ms. Data surprising within the next five years. The good news is that they will not be limited to video appearances, and they probably won't fight for the corner office or care about the size of their office, their view from the office, or even if it has windows!

When deciding between a human and a humanoid, consider that humanoid workers do not require coffee breaks, water coolers, vacations, medical leave, child care leave, etc. They will work tirelessly day in and day out. No sick days. For the foreseeable future, they will not have a significant other to fight with or become distracted by the resulting emotional turmoil. By the way, humanoid workers produce infinitely faster than human workers.

Simply put, going humanoid over human offers many advantages. Conversely, humanoid workers lack emotional intelligence, human judgment, and an internal moral compass. Life is never perfect. With technology, you take the good with the bad.

The Evolution of AI in Law

Appreciating the significance of AI in the legal world requires understanding its evolution. In its simplest form, AI

refers to machines' simulation of human intelligence. This encompasses a range of technologies, including machine learning, natural language processing, and computer vision. These technologies enable machines to perform tasks traditionally requiring human intelligence, such as decision-making, problem-solving, and language comprehension.

AI's journey began in the mid-20th century, with early pioneers such as Alan Turing and John McCarthy laying the groundwork for what would become a transformative field. Turing's seminal work on machine intelligence and McCarthy's coining of the term "artificial intelligence" in 1956 marked the beginning of a new era. Over the decades, AI research progressed in fits and starts, with periods of optimism followed by "AI winters"—times when progress stalled due to technical and funding challenges.

However, the turn of the 21st century brought about a renaissance in AI research and development. Advances in computing power, the availability of vast amounts of data, and breakthroughs in machine learning algorithms propelled AI from the fringes of academia into mainstream applications. Today, AI is ubiquitous, powering everything from search engines to virtual assistants, and its foray into the legal world represents a natural progression of this technological evolution, particularly since the development and introduction of generative AI, sometimes referred to as "GenAI."

Automation of Tedious Tasks

One of AI's most significant impacts in the legal field has been automating repetitive tasks that traditionally required extensive human effort. These tasks often involved teams of junior associates working long hours. AI allows lawyers to focus on higher-level strategic work rather than routine administrative tasks.

Legal Research

Legal research has traditionally been labor-intensive and time-consuming, requiring lawyers to sift through vast amounts of legal texts, case law, statutes, and regulations to find relevant information. This process often involved hours of manual work and came with the ever-present risk of human error.

Enter AI-powered legal research tools. These tools leverage natural language processing (NLP) and machine learning algorithms to analyze and understand legal texts with remarkable accuracy. By training on vast corpora of legal documents, AI systems can quickly identify relevant precedents, statutes, and case law, providing lawyers with precise and contextually relevant information in a fraction of the time of a human worker (or even a team of human workers). While AI is not perfect and may misinterpret something (humans do that as well), it comes with a much-reduced likelihood of simply missing something in comparison to human workers.

Contract Analysis and Review

Contracts are the lifeblood of the legal profession, governing relationships, transactions, and obligations. However, reviewing and negotiating contracts is often fraught with complexity and risk. Human errors, ambiguous language, and overlooked clauses can lead to costly disputes and legal battles.

AI is revolutionizing contract analysis and review by automating many tasks traditionally performed by lawyers. AI-powered contract analysis tools can quickly scan and review contracts, identifying key clauses, potential risks, and inconsistencies. These tools use machine learning algorithms to understand the language and structure of contracts, allowing them to flag problematic provisions and suggest improvements.

Document Generation

Document generation is another area where automation through AI can save time and increase quality. Document generation is a fundamental aspect of legal practice, encompassing everything from drafting

pleadings and motions to creating contracts and agreements. Traditionally, this has been a manual and time-consuming process, requiring lawyers to painstakingly review documents to ensure accuracy and compliance.

AI-powered document generation tools can create legal documents based on predefined templates and user inputs. These tools use natural language generation (NLG) algorithms to generate contextually relevant and legally sound text, speeding up the process and reducing the risk of errors and inconsistencies.

Predictive Analytics in Litigation

AI's capabilities extend beyond simple automation. They also play a crucial role in legal analytics and case outcome prediction.

Litigation is inherently uncertain, with outcomes often hinging on many factors, including the strength of evidence, the persuasiveness of arguments, and the inclinations of judges and juries. AI, and in particular, GenAI, brings a new level of predictability to litigation. Using statistical models and machine learning algorithms to analyze historical case data, AI systems can provide insights into how a particular judge has ruled on similar matters, assess the likelihood of success in a lawsuit, and even suggest optimal litigation strategies. These predictive analytics can help lawyers make more informed decisions about case strategy, settlement negotiations, and resource allocation, ultimately improving their chances of achieving favorable client outcomes.

Insights into the Legal Industry

AI is also being used to analyze legal markets and industry trends. AI-powered tools can provide insights into the competitive landscape and help law firms identify growth opportunities by analyzing data on law firm

performance, client demand, and market dynamics. This allows legal professionals to stay ahead of the curve and adapt to the changing legal environment.

AI in the Hiring Process

AI plays a significant role in hiring, fundamentally changing how law firms and legal departments recruit new talent. Traditionally, hiring a new employee has involved manually reviewing résumés, conducting interviews, and assessing candidates based on subjective criteria. This process was time-consuming and prone to biases.

AI-driven recruitment tools have introduced a new level of efficiency and objectivity to the hiring process. These tools use machine learning algorithms to analyze résumés, cover letters, and other application materials, identifying the most qualified candidates based on predefined criteria. By eliminating human biases, AI ensures a more fair and equitable hiring process. It also introduces a new set of standards, concerns, and requirements in those situations where the pool of available workers includes AI-driven entities.

AI-powered tools can streamline the onboarding process for new hires. By automating administrative tasks, such as document verification and compliance checks, AI allows HR teams to focus on more strategic activities, such as training and development. This accelerates the onboarding process and ensures that new employees are better prepared to succeed in their roles.

Improved Access to Justice

Beyond improving efficiency in law firms, AI also plays a crucial role in making legal services more accessible. Chatbots and AI-driven legal assistants provide preliminary legal guidance to individuals who may not have the means to hire an attorney. These tools help users understand their rights, generate essential legal documents,

and even navigate simple legal disputes. By bridging the gap between legal expertise and the public, AI helps democratize access to justice and helps ensure that legal assistance is not just a privilege for those who can afford high-priced lawyers.

This All Sounds Great! What's the Downside?

I have said for many years that we must always see technology as a double-edged sword. The introduction of GenAI and the expansion of the utilization of AI supports that conclusion. While AI offers undeniable benefits to the legal world, it also presents significant practical downsides and risks. This discussion will explore the potential challenges and implications of integrating AI into legal practice, focusing on bias, trustworthiness, job displacement, privacy concerns, the erosion of professional judgment, and ethical decision-making.

Bias and Fairness

One of the most pressing ethical risks associated with AI in the legal field is the potential for bias. Machine learning models train on large datasets; if these datasets contain biased information, the AI will inevitably learn and perpetuate those biases. This can lead to unfair, discriminatory, and sometimes just plain incorrect outcomes, particularly in areas such as sentencing, bail decisions, and hiring practices.

To mitigate this risk, we need regular auditing and human oversight of AI systems to identify and mitigate biases, a complex process that can require extensive resources. Legal professionals must also vigilantly monitor AI outputs and implement corrective measures when they detect biases, for instance, shifting to more diverse and representative training data. This requires a deep understanding of both the technical aspects of AI and the ethical implications of its use.

Trustworthiness

AI has a checkered past regarding trustworthiness. When tasked with research and/or the generation of a brief or memorandum, AI has made up cases that did not exist and cited cases and statutes incorrectly or for propositions contrary to their intent. Accordingly, using AI to draft a brief or memorandum of points and authorities poses serious risks to the legal professional. To protect our own reputation and our clients' interests, we must carefully monitor AI's output for such issues and ensure that we correct them before they ever leave our office. As of the current time, AI has no internal moral compass and no independent means of evaluating or even comprehending right and wrong. While that may change in time as AI continues to evolve, we must diligently verify the accuracy of all citations and factual assertions made by an AI-powered entity or program.

Job Displacement and Workforce Impact

While AI has the potential to automate many routine and repetitive tasks, it also raises questions about job displacement and the future role of legal professionals, as well as support staff. Ideally, AI will not replace lawyers but augment their capabilities, allowing them to focus on higher-value tasks that require human judgment, creativity, and empathy. Unfortunately, we have no guarantee of that outcome. It remains possible that AI entities will ultimately replace a variety of law office staff, from receptionists to junior attorneys.

Legal professionals and support staff must develop new skills and competencies to remain relevant in an AI-driven legal landscape. This includes proficiency in data analysis, technology management, and ethical decision-making. Law firms and legal departments must invest in training and development programs to help employees adapt to these new realities. As we move forward into this brave new world, it may make good sense for a young person thinking about a career in law to major in computer science as an undergraduate rather than one of the traditional majors for aspiring attorneys.

Privacy and Data Security

AI systems rely on large datasets, often containing personal and confidential information. The storage and processing of this data make it a prime target for cyberattacks. Data breaches can have severe consequences, compromising client confidentiality and damaging the reputation of law firms.

Legal professionals must ensure compliance with data protection regulations, such as the General Data Protection Regulation (GDPR) in the European Union. This includes implementing robust security measures, conducting regular risk assessments, and ensuring that we design AI systems to protect privacy.

Erosion of Professional Judgment

AI systems excel at analyzing large datasets and identifying patterns, but they lack the nuanced understanding and contextual awareness that human lawyers bring to their work. Overreliance on AI could lead to an erosion of professional judgment and a diminished role for human expertise, to say nothing of a number of lesser quality and incorrect decisions.

While AI can provide valuable insights and support decision-making, it should not replace the *critical* thinking and professional judgment of legal professionals. Lawyers must balance leveraging AI's capabilities and maintaining their own expertise and intuition.

Ethical Decision-Making

AI systems may struggle with ethical decision-making, particularly in complex moral dilemmas or sensitive issues. AI has no internal moral compass, so it does not know right from wrong. Human lawyers, drawing on their experience, empathy, and ethical frameworks, can better and more safely navigate those challenges.

The Future of AI in the Legal Industry

AI's big debut in the legal world represents not a momentary trend but a transformative shift reshaping law practice. As technology evolves, we can anticipate AI-driven legal assistants becoming ever more sophisticated, providing real-time legal insights and automating more complex legal tasks. Integrating AI into law practice offers significant benefits, but it also presents substantial practical downsides and ethical risks. As we navigate this brave new world of AI-enhanced legal practice, we must remain vigilant about the ethical and practical implications of our human/humanoid partnership. With due diligence and proper vigilance, the fusion of human expertise with machine intelligence should not end the legal profession as we know it but rather create the dawn of a new era. I hope for one where lawyers practice law with greater precision, efficiency, and accessibility.

Author

Prompt Engineering: The New Art of Asl Questions

Jeffrey M Allen and Ashley Hallene

Oct 12, 2025 6 min read

Summary

- Learn how prompt engineering improves AI accuracy for lawyers.
- Discover practical AI applications in research, contracts, and litigation.
- Reduce AI hallucinations with step-by-step legal prompt strategies.



skynesher vi

Jump to:

What is Prompt Engineering? →

The Problem of Hallucinations →

Breaking Prompts into Small Steps →

Benefits for Lawyers →

Practical Application in Law Practice →

Lawyerly Tropes and Takeaways →

Lawyers have always thrived on the power of the right question. In the courtroom, a precise cross-examination can shift a jury's perception. In a deposition, a carefully framed question can expose the weakness of an opponent's case. Even in a client meeting, clarity of inquiry builds trust and guides decision-making.

Perry Mason, the fictional defense attorney who captivated television audiences for decades, rarely won his cases through grand speeches. Instead, he triumphed through sharp, well-timed questions that unraveled the truth.

Today, lawyers confront a new arena where questions hold similar power: the world of artificial intelligence. As AI tools such as ChatGPT, legal research assistants, and document analyzers move into legal practice, the quality of the results depends heavily on the quality of the questions posed to them. This practice has a new name in technological circles: prompt engineering. For lawyers, who already appreciate the art of inquiry, prompt engineering is less about learning something foreign and more about applying familiar skills in a new context.

Think about in the context of the Socratic Method. Just as Socrates guided his students toward understanding by asking simple, progressive questions, lawyers can guide AI tools toward accuracy by structuring their prompts in smaller, manageable steps.

What is Prompt Engineering?

Prompt engineering refers to the process of carefully crafting instructions for AI systems so that they deliver accurate, relevant, and useful responses. Instead of treating AI like a magic box that provides instant solutions, prompt engineering treats it like a junior associate who requires direction and supervision.

A poorly worded prompt is like asking a witness a vague question. The answer might be irrelevant or misleading. A well-crafted prompt narrows the focus, defines the terms, and makes the AI more likely to provide something that can actually help the lawyer. The practice has quickly become essential because of a growing recognition of how AI systems operate. These tools predict words and phrases based on patterns in massive datasets, which means their output is only as reliable as the way the request is structured.

The Problem of Hallucinations

AI tools often produce what are known as hallucinations. In plain terms, this means the system generates responses that sound convincing but are factually false. Some lawyers have already learned this the hard way, with cases in which AI-produced briefs contained entirely fabricated case citations. Courts have responded with sanctions, warnings, and strong reminders that lawyers cannot delegate their professional responsibility to a machine.

Hallucinations are the digital equivalent of a witness who testifies with confidence but lacks any foundation for their claims. If unchecked, they can damage a lawyer's credibility, harm a client's case, and potentially cross ethical lines. For lawyers, who should already understand the value of double-checking every fact, prompt engineering offers a path to minimize these risks.

Breaking Prompts into Small Steps

The most effective way to reduce hallucinations and increase accuracy is to break prompts into small steps. Instead of asking AI to complete a sweeping task such as "Write a client memo on liability under this contract," a lawyer can divide the request into a sequence of smaller questions.

For example:

1. Ask the AI to summarize the contract provisions in plain English.
2. Next, ask it to identify which provisions might create legal risk.
3. Finally, ask it to outline possible strategies for addressing those risks.

This step-by-step method mirrors how lawyers naturally work. When preparing for a cross-examination, you never begin by asking the witness to admit the ultimate fact. Instead, you build the foundation with smaller, targeted questions that create a logical path toward your conclusion. The same principle applies in prompt engineering. By controlling the sequence, the lawyer controls the accuracy and transparency of the AI's reasoning process.

The Socratic Method offers another useful analogy. Socrates did not lecture his students with final answers. He asked them a series of small, carefully designed questions that forced them to examine their assumptions and reach conclusions step by step. Those who adopt this method for prompting AI will find that it leads to more reliable and verifiable results.

Benefits for Lawyers

When lawyers break prompts into smaller steps, the results often feel more reliable and far less frustrating. Accuracy is the most immediate benefit. By narrowing the scope of each request, the AI has less room to wander into irrelevant speculation or invent details that do not exist. What emerges is a response that stays closer to the facts at hand.

Transparency also improves. Instead of waiting for a finished product that may contain errors, lawyers can see the process unfold one stage at a time. If an AI tool stumbles on the summary of a contract clause, the lawyer can intervene before the analysis moves forward. The experience is not unlike reviewing the work of a junior associate: it is easier to correct a misstep early than to rewrite an entire draft later.

Smaller prompts also save time. Errors are inevitable, but they are far less costly when the task is broken into pieces. If one answer falls short, only that portion needs to be reworked. The rest of the process can continue intact. This efficiency makes the interaction feel more like a conversation than a one-off request, with the lawyer guiding the exchange toward a useful outcome.

Perhaps the most significant benefit is confidence. Many senior lawyers approach AI with caution, wary of overpromises and concerned about ethical risks. Prompt engineering gives them a way to stay firmly in control. Instead of acting as passive recipients of whatever the machine produces, they become active supervisors, shaping the output step by step. In that role, the lawyer retains the same authority he or she exercises in every other part of practice: asking sharp questions, checking the answers, and ensuring the work meets professional standards.

Practical Application in Law Practice

Prompt engineering already has clear and practical uses across many areas of law. In legal research, for example, lawyers often want to move from facts to holdings to application. Rather than asking an AI system to deliver a polished memorandum in one pass, it works better to stage the process. Begin by requesting a summary of the facts, then ask for the holding, and only afterward inquire how that holding might apply to the situation at hand. By breaking the task into steps, the lawyer can more easily spot errors before they multiply.

Communication with clients offers another strong opportunity. Lawyers know how difficult it can be to translate dense legal concepts into plain language. With AI, the process becomes easier if handled in stages. The lawyer might first ask for a simple summary that captures the essence of the issue, then refine that output into a version that is appropriate for client correspondence. This method ensures clarity without sacrificing accuracy or professionalism.

Contract review also benefits from this approach. Large agreements often overwhelm even seasoned attorneys, and an AI assistant can help by isolating specific clauses one at a time. A lawyer might direct the system to identify indemnification provisions first, then move on to termination clauses, and finally highlight governing law. This mirrors the methodical way senior attorneys train junior associates, focusing on one issue before moving on to the next.

Litigation preparation may be the area where prompt engineering feels most familiar. Building a case has always involved starting with a broad set of possible arguments, refining them into stronger points, and then supporting them with authority. AI can assist in the same way. By asking for an outline first, then narrowing to key arguments, and finally requesting supporting cases, the lawyer creates a stepwise path that echoes the process of drafting cross-examination notes: broad at the start, precise at the finish.

Lawyerly Tropes and Takeaways

Lawyers can lean on familiar tropes to understand prompt engineering.

- **Channel Your Inner Perry Mason**. Just as Perry Mason relied on carefully timed questions rather than flashy speeches, prompt engineering rewards lawyers who ask clear, deliberate questions in the right sequence.
- **Think Socratically.** The Socratic Method teaches that truth emerges from step-by-step questioning. Apply that principle to AI, treating it as a student whose learning requires guidance.
- **Practice Like Cross-Examination.** Never ask compound or rambling questions. Keep prompts tight, focused, and purposeful. Just as in court, clarity is your strongest weapon.

Prompt engineering is not a new trick for young technology enthusiasts. It is a natural extension of skills that lawyers already possess. Asking precise questions, structuring inquiry step-by-step, and supervising the work of others have always been part of the profession. The difference is that the "other" in this case is not a junior associate but an AI system.

By embracing prompt engineering, lawyers can reduce the risks of hallucination, increase the accuracy of AI tools, and maintain professional control. The lesson is simple but powerful: in the courtroom, the right question can win the case. In the digital age, the right prompt can win the answer.

Authors



Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...



Ashley Hallene

Ashley Hallene is an Attorney and Land Acquisition Specialist with Demeter Land Development. She is based in Houston, Texas. She is the co-author of several books, including Technology Tips for Seniors Volume 2.0 (2018),...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-october/prompt-engineering/

Voice of Experience Voice of Experience: May 2026

How to Avoid Accidental Disclosure Whe Using AI

Ashley Hallene and Jeffrey M Allen

May 10, 2026 6 min read

Summary

- AI tools can improve legal drafting, research, and efficiency, but they also create client confidentiality risks when prompts and documents are processed on external cloud-base systems.
- Lawyers must treat AI use as a professional responsibility issue by understanding data re training practices, vendor terms, and the risk of accidental disclosure.
- Clear AI policies, secure platforms, staff training, and careful prompt drafting help law fir reduce disclosure risk while using artificial intelligence responsibly.



sportpoint via G

Jump to:

Confidentiality Reaches Far Beyond Privileged Communications →

AI Feels Private, but Often Is Not →

Routine AI Use Can Lead to Confidentiality Problems →

Four Habits That Lower the Risk of Disclosure →

Supervision and Training Cannot Be an Afterthought →

AI May Be New, but the Duty Is Not →

AI Column

Artificial intelligence tools are now part of everyday legal practice. Lawyers use them to

draft documents, summarize contracts, research legal issues, and generate ideas. Used well, these tools can save time and improve workflow. Used carelessly, they can expose confidential client information.

That risk deserves attention now, not later. Many AI tools operate through cloud-based platforms that process user inputs on external servers. A lawyer who pastes facts into a prompt, uploads a draft agreement, or asks for help refining strategy may be sending sensitive information outside the firm without fully understanding where it goes, how long it stays there, or who may have access to it. Because confidentiality is a core professional duty, lawyers need to understand how these tools handle data before using them in client work.

It does not take a dramatic mistake to create a confidentiality problem. A lawyer might type what feels like a routine prompt, such as “revise this indemnity provision for our client’s $20 million acquisition of a regional manufacturing company,” without pausing to consider how much that single sentence reveals. In just a few words, the lawyer may have disclosed the type of deal, the size of the transaction, the client’s position, and enough context to identify the matter. The real danger is not exotic misuse. It is ordinary convenience.

Confidentiality Reaches Far Beyond Privileged Communications

The duty of confidentiality is broad. It generally extends to all information relating to the representation of a client, not just information protected by the attorney-client privilege. That includes litigation strategy, draft contracts, financial information, internal legal analysis, and business plans. It can also include information that is publicly available, if it relates to the representation in a way that makes its use or disclosure problematic.

That matters in the AI context because lawyers may think they are safe as long as they avoid sharing a final document or a privileged email. But confidentiality risks can arise much earlier. A prompt that names the parties, describes a dispute, or summarizes a negotiation position may already reveal too much.

The governing principle is familiar. Lawyers must take reasonable steps to protect client information from unauthorized disclosure. Technology does not change that duty. It changes the setting in which the duty must be carried out.

AI Feels Private, but Often Is Not

AI tools are not inherently improper, but they create risks that differ from those that arise from more traditional office software. Many AI tools operate through external, cloud-based systems. When a lawyer enters text into an AI interface, the information may be transmitted to servers controlled by the provider rather than kept entirely within the firm's own environment.

What happens next depends on the platform. Information may be processed and deleted, stored for a period, reviewed by human personnel, or used to improve the system. Lawyers cannot safely assume that all AI tools handle data the same way or that a conversational interface is private simply because it feels private.

That point is easy to miss. AI tools often feel like digital research assistants. They are quick, polished, and conversational. Many function more like web-based services that receive, process, and sometimes retain user inputs outside of the organization. If lawyers treat these systems like private notebooks or internal colleagues, accidental disclosure becomes much more likely.

Routine AI Use Can Lead to Confidentiality Problems

Most confidentiality problems with AI will not come from reckless misconduct. They will come from ordinary, hurried work. Picture an ordinary workday. A lawyer is on deadline, the client wants revisions quickly, and the redline still needs work. To move faster, the lawyer drops part of the draft into an AI tool and asks for a tighter clause or a cleaner summary. It feels like a harmless productivity move, but if that text includes client names, transaction details, or strategy, a routine shortcut can become a confidentiality problem.

That same pattern appears in other everyday situations. A lawyer may upload a contract for summary, paste facts into a prompt to test an argument, or ask an AI tool to draft a clause tailored to a specific transaction. A paralegal may use a free public tool to clean up a client communication. A junior lawyer may try a personal AI account for research because it is faster than approved systems.

Each of those choices may seem minor. Together, they show how easily confidential information can move outside of approved channels.

Several common situations deserve special care:

- Uploading client documents, including draft contracts, discovery materials, due diligence files, or internal memoranda
- Entering detailed prompts that include party names, dispute facts, transaction terms, or litigation strategy
- Using AI tools to draft documents that contain client names, settlement amounts, or deal-specific provisions
- Allowing lawyers or staff to use personal or unapproved AI tools for work-related tasks

The pattern is simple: The more specific the prompt or upload, the greater the risk. Lawyers do not need to attach a full document to create a problem. A detailed prompt alone may reveal the heart of the matter.

Four Habits That Lower the Risk of Disclosure

The good news is that accidental disclosure through AI is a manageable risk. It requires judgment, policy, and training, not panic.

First, adopt a clear policy for AI use. Lawyers and staff should not be left to guess which tools are allowed or what information may be entered into them. A sound policy should identify approved platforms, explain whether documents may be uploaded, define

what information must never be entered, and require human review of AI-generated work before it is used in client matters.

Second, avoid entering identifying client details unless there is a clear reason to do so and an approved platform is being used. In many cases, a lawyer can get useful help from a generalized prompt. A request for an indemnification clause in a commercial acquisition agreement is usually safer than a prompt that names the parties and states the purchase price.

Third, choose tools with stronger confidentiality protections. Many organizations now use enterprise AI platforms that provide better safeguards than free public versions. Depending on the provider, those protections may include encryption, limits on retention, contractual confidentiality commitments, and settings that prevent user inputs from being used to train future models. Even then, lawyers still need to confirm how the platform works.

Fourth, read the provider's terms. Before using an AI tool for legal work, lawyers should know the answer to a few basic questions: Is user input stored? Can the provider access it? Is it used to train the model? How long is it retained? Those are threshold questions, not technical details to ignore.

Supervision and Training Cannot Be an Afterthought

Even a good policy will fail if no one enforces it. Law firm leadership and legal department management need to take an active role in supervising AI use. That means more than approving a platform once and moving on. It means setting expectations, training personnel, and monitoring whether people are following the rules in practice.

This is especially important for junior lawyers and staff, who are often the quickest to experiment with new tools. Their interest in efficiency is understandable and often helpful, but it also creates risk if they do not understand the confidentiality implications of a prompt, an upload, or a personal account. Supervising attorneys should ensure that AI use complies with firm policy, that confidential information is not entered into unapproved systems, and that a human carefully reviews AI-generated work.

Training is one of the best safeguards. Many avoidable mistakes happen because users do not understand how AI systems process data or assume that a polished interface means the tool is private and secure. Clear, practical training can prevent those assumptions from turning into disclosure problems.

AI May Be New, but the Duty Is Not

AI tools can deliver real benefits. They can help lawyers draft faster, organize information, and generate ideas more efficiently. Those benefits are worth pursuing. But they must be balanced against the lawyer's duty to protect client information.

That balance is not difficult to describe, even if it sometimes takes discipline to maintain. Lawyers should understand the technology they use, put reasonable safeguards in place, choose platforms carefully, and keep humans responsible for the final judgment. AI may change how legal work is performed, but it does not change the professional duty that sits underneath that work.

Client trust still depends on the same promise it always has—that lawyers will protect sensitive client information. AI may be new, but the lawyer's job is not: Protect the client, protect the information, and use good judgment.

Authors



Ashley Hallene

Ashley Hallene is an Attorney and Land Acquisition Specialist with Demeter Land Development. She is based in Houston, Texas. She is the co-author of several books, including Technology Tips for Seniors Volume 2.0 (2018),...



Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-may/client-confidentiality-and-ai-how-to-avoid-accidental-disclosure/?utm_source=chatgpt.com

Voice of Experience Voice of Experience: July 2025

How to Navigate the Future of Artificial Intelligence

Jeffrey M Allen and Ashley Hallene

Jul 18, 2025 8 min read

Summary

- AI Systems can amplify existing inequalities, necessitating robust oversight to prevent harm to vulnerable communities.
- Industry leaders and lawmakers are divided on regulating AI, balancing innovation with ethical concerns.
- AI promises advancements in legal practice, but it won't replace human judgment and experience.



DNY59/iStock/Getty Images Plus via Getty Images

Jump to:

The Big Buzz: Why Congress Is Taking AI Seriously →

Divergent Perspectives: Industry Leaders vs. Political Leaders →

What's on the Table? →

AI's Role in the Legal Field →

The Future of AI: Opportunities and Challenges on the Horizon →

What Attorneys Should Keep in Mind →

Summing It Up →

A Bill for AI—NOT! →

Resources →

If you've followed the news (or indulged in a good podcast), you've probably heard about the congressional hearings on artificial intelligence (AI) that have recently grabbed headlines. Those of you still practicing might wonder what this all means for your practice. All of us might wonder what it bodes for the profession and the legal landscape as a whole.

The Big Buzz: Why Congress Is Taking AI Seriously

Formerly the stuff of science fiction movies, AI now has real-world implications. We find AI everywhere, from our homes to offices, self-driving cars, medical diagnostics, and legal research tools, to name just a few places. At recent hearings, members of Congress sat down with industry leaders, ethicists, and researchers to endeavor to make sense of AI's growing impact on society and figure out how to regulate it responsibly.

One of the key figures at the forefront of these conversations is Sam Altman, CEO of OpenAI, the brains behind

ChatGPT. During a recent Senate Judiciary subcommittee hearing, Altman emphasized, “If this technology goes wrong, it can go quite wrong.” (Source: Senate Judiciary Subcommittee Hearing, May 2023) That’s not exactly comforting, but it’s refreshingly honest. Altman and others called for regulations to ensure AI serves humanity without veering into dystopian territory.

Divergent Perspectives: Industry Leaders vs. Political Leaders

While most everyone acknowledges AI’s transformative potential, the hearings have revealed notable differences in opinion between industry leaders and political leaders. These differences reflect the complexities of regulating a rapidly evolving technology that touches nearly every aspect of modern life.

Industry leaders like Altman have generally supported the idea of regulation, but prefer a collaborative and flexible approach. Altman, for instance, suggested the creation of a new government agency to oversee AI development. “We think that government regulatory intervention will be critical to mitigate the risks of increasingly powerful models,” he told the Senate. However, he also warned against stifling innovation, adding, “Over-regulation could slow down the advancement of systems that genuinely benefit society.”

Another prominent voice, Sundar Pichai, CEO of Alphabet Inc., has espoused a different position. Pichai emphasized the need for global cooperation, stating, “AI development is not limited by borders. Effective regulation requires international collaboration to ensure uniform standards and prevent misuse.” Pichai and other international technology leaders pointed to the risks of fragmented regulations that could result in uneven ethical standards worldwide.

On the other hand, some lawmakers have expressed skepticism about whether self-regulation within the technology industry can suffice. In a pointed exchange, Senator Josh Hawley questioned whether we could trust major AI companies to prioritize public interest over profit. Hawley remarked, “The track record of technology

companies doesn't exactly inspire confidence. Why should we believe this time will be different?" Other legislators echoed his concerns, expressing fear that leaving too much control in the hands of industry could lead to monopolies or misuse of AI.

Another powerful voice in the hearings, Dr. Joy Buolamwini, founder of the Algorithmic Justice League, highlighted the ethical challenges. "AI systems are already being used in ways that harm vulnerable communities," she testified. "Bias embedded in these systems reflects and amplifies existing inequalities. Without robust oversight, these injustices will only worsen." Her call for stricter guidelines resonated with several lawmakers advocating for immediate intervention to address bias and systemic inequities.

What's on the Table?

Congress is grappling with several critical questions:

- **Transparency**: How do we ensure the transparency of AI systems regarding their manner of operation? For attorneys, transparency matters deeply—imagine relying on AI-driven case law research without knowing which algorithms were used to prioritize the results.
- **Bias:** AI doesn't escape bias just because it's a machine. Bias can be devastating in any system. Congress has asked tough questions about how to eliminate it from AI models.
- **Accountability:** Who's liable when AI fails to perform as designed? This question has particular relevance to attorneys handling contracts, intellectual property disputes, or cybersecurity breaches caused by AI errors. It will also affect personal injury and property damage litigators when dealing with an accident involving one or more self-driving vehicles.

- **Innovation vs Regulation**: How do lawmakers strike the right balance? Excessive regulation might stifle innovation, but lax oversight risks exploitation and various economic and societal harms.

While not involved in the congressional hearings, let's not forget or easily dismiss Elon Musk's warning that AI poses an existential threat to humanity. Musk is not the only one to warn about the risk posed by AI with a certain amount of religious fervor. In his address at the G7 Summit in June 2024, Pope Francis described AI as "an exciting and fearsome tool," acknowledging its capacity to revolutionize various sectors, including medicine, education, and labor. However, he cautioned that AI could exacerbate social inequalities and contribute to a "throwaway culture" if not guided by ethical considerations. Additionally, in his inaugural address to the College of Cardinals, Pope Leo XIV highlighted AI's potential to disrupt labor markets, exacerbate social inequalities, and challenge the very notion of human dignity. [That sounds existential…]

AI's Role in the Legal Field

AI isn't just a buzzword—it's changing how we practice law. From streamlined research to AI-powered contract analysis platforms, technology can make your job faster and arguably more precise. But that comes with a caveat: AI doesn't replace your experience or judgment. It's a tool, not a substitute.

At the congressional hearings, some experts questioned whether AI could inadvertently erode the human element of professions like law. Clients don't just hire attorneys for technical expertise; they rely on attorneys' wisdom, intuition, and ability to read a room (or a jury). Could AI eventually render these qualities less valuable? It's an unsettling thought, but one requiring consideration.

Former Attorney General Eric Holder weighed in during an AI-focused panel discussion, stating, "Legal professionals must approach AI with skepticism but not fear. The technology is a tool for empowerment, not a

replacement for human judgment. However, understanding the risks is vital to ensuring fairness in its application." Holder's remarks underscore the importance of training and adapting without losing sight of ethical principles.

The Future of AI: Opportunities and Challenges on the Horizon

As we look ahead, the future of AI is poised to offer incredible advancements while presenting equally significant challenges. In the legal field, expect AI's capability to predict case outcomes, analyze massive datasets, and even draft legal documents to evolve further. This could lead to greater efficiency and cost savings for firms and clients.

For instance, AI-driven predictive analytics might one day provide highly accurate forecasts about the likelihood of success in litigation, based on historical data and trends. Imagine having a virtual assistant that organizes your research and recommends strategies tailored to specific judges or opposing counsel. These advancements hint at a promising future, but they also raise ethical questions about fairness and transparency in decision-making processes.

Experts have predicted that AI will increasingly play a role in cybersecurity. As legal professionals store confidential data and sensitive case files, AI-powered systems could offer advanced protection mechanisms against breaches and hacks. Conversely, malicious actors can weaponize this same technology, highlighting the need for regulations to safeguard against misuse. As Senator Amy Klobuchar emphasized during the hearings, "The dual-use nature of AI makes it vital to legislate for both its benefits and its risks."

Beyond the legal sphere, AI's future will likely reshape industries like healthcare, education, and entertainment. Using AI to develop personalized treatments, optimize learning experiences, or create immersive media has the potential to redefine societal norms. However, experts caution that we must weigh these benefits against risks

such as privacy infringements, intellectual property theft, and ethical dilemmas around automation replacing human labor.

What Attorneys Should Keep in Mind

If you feel overwhelmed by all this AI talk, take a deep breath. AI isn't here to push you out of the profession, but to enhance it. Your decades of experience, sharp intuition, and ability to connect with clients are irreplaceable. AI might help you draft contracts faster or predict case outcomes more accurately, but it won't replicate your humanity.

So, what's your homework? Stay informed. Follow these hearings, read up on AI advancements, and consider taking a course or attending a seminar on AI in the legal field. The best attorneys adapt to change while staying true to their core values.

Summing It Up

The congressional hearings on AI are a wake-up call—not just for technologists or policymakers but for all of us. This is an opportunity to embrace innovation while safeguarding the principles that make law a deeply human enterprise. As AI continues to reshape the landscape, one thing remains clear: your wisdom will always have a place, no matter how advanced the machines become.

Here's to navigating the future together, one case—and one algorithm—at a time.

A Bill for AI—NOT!

Likely, you have heard about the Trump administration's omnibus bill that the president likes to call the BBB (Big Beautiful Bill). Other people spent a lot of time coming up with other expansions of that acronym, many of them not complimentary. Elon Musk, formerly a golden boy in the Trump administration, has objected to the bill and ignored the acronym game. He describes it as a "disgusting abomination." To be politic (never our strong suit), we have decided to opt for description rather than advocacy; accordingly, in this article, "BBB" stands for "Big Bulky Bill" (apt as it exceeds 1000 pages).

The House version of the BBB provided for federal preemption of AI regulation. That meant that the federal government would have primary authority to regulate AI technologies. The rationale behind this provision is to establish a uniform regulatory framework nationwide, ensuring consistency and preventing a patchwork of state regulations that could hinder innovation and create compliance challenges for AI developers and companies. (Anybody remember the mud flap cases and the Interstate Commerce Clause?)

The House iteration of the BBB would have restricted states from enacting their own AI-related legislation that conflicts with federal regulations. This provision was intended to prevent states from imposing additional requirements or restrictions on AI technologies that could create barriers to innovation and economic growth. The Senate version of the bill did not include federal preemption of AI legislation. The Conference Committee version ultimately passed by both the House and the Senate and was signed into law by the President, following the Senate's course, leaving out that provision.

Without regard to your feelings about the rest of Big Bulky, there is a lot to be said about a national policy on something as ubiquitous as artificial intelligence. The idea that states, with their diverse social, political, economic, and technological orientations, can each pass their own regulations and seek to compel industry compliance poses a daunting problem for the industry, which desperately needs regulation. Ultimately, if the Supreme Court follows long-standing precedent (no longer a safe bet), it will ultimately rule that subjecting the industry to the demands of 50 states is an inappropriate burden. Does anybody remember the mudflap cases from Constitutional Law classes in law school? See, e.g., *Bibb v. Navajo Freight Lines*, 359 U.S. 520 (1959)."

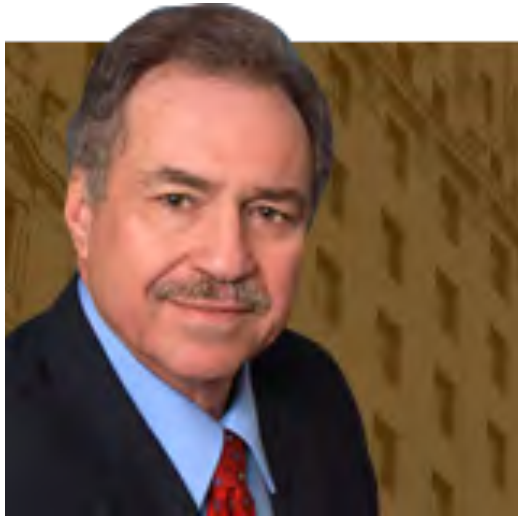
Resources

If you want to read more about the topics in this article, here are a few places to start:

- Transcript: Senate Judiciary Subcommittee Hearing on Oversight of AI (Tech Policy.Press)
- OpenAI Chief Says His 'Worst Fear' Is That Tech Causes 'Significant Harm To The World' (HuffPost)
- Sam Altman Warns Against Over-Regulation of AI: Why America Must Lead the AI Revolution (Education Next)
- Sundar Pichai on regulating AI: 'Technology's virtues aren't guaranteed' (SiliconRepublic)
- Hawley Op-Ed: Break Up Big Tech Behemoths to Reclaim American Freedom (Josh Hawley)
- Dr. Joy Buolamwini on Algorithmic Bias and AI Justice (Sanford School of Public Policy)
- Unmasking the bias in facial recognition algorithms (MIT Sloan School of Management)
- Elon Musk: Artificial Intelligence Is Humanity's 'Biggest Existential Threat' (LiveScience)
- Pope Francis Attends the G7 Session on Artificial Intelligence (Vatican)
- Pope Francis urges ethical use of artificial intelligence (Vatican News)

- Pope Leo XIV speaks out against AI: ‘A challenge of human dignity, justice and labour’ (The Independent)

Authors



Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...



Ashley Hallene

Ashley Hallene is an Attorney and Land Acquisition Specialist with Demeter Land Development. She is based in Houston, Texas. She is the co-author of several books, including Technology Tips for Seniors Volume 2.0 (2018),...

How to Stay Safe from Utility Scams

Jeffrey M Allen

Jul 14, 2025 7 min read

Summary

- Scammers use robocalls and live agents posing as utility representatives, demanding immediate payment to avoid disconnection with just enough believable information from previous data hacks to make victims act without thinking.
- Victims experience financial loss, stress, and fear, with some even facing medical risks due to scam-induced panic.
- To protect yourself and others, verify calls with the utility company directly, avoid trusting caller ID, and spread awareness.



dlewis33 via Getty Images

Jump to:

A Real-Life Utility Scam →

Anatomy of a Utility Scam →

Why This Scam Works →

Real-World Impact →

How to Protect Yourself and Others →

Technology Is a Double-Edged Sword →

An Advocate's Role Never Retires →

When the phone rings, you're at home, reading the paper or checking email. A serious voice claims to represent your electric company. They have a "disconnect order" on your account. They tell you the company will cut off your service within the hour unless you immediately pay the overdue balance.

It sounds dramatic, but it happens every day. This type of scam has plagued the country for years, and it's still evolving. Sharp, experienced, and generally skeptical attorneys aren't immune. Scammers often count on our tendency to trust official-sounding voices and structured procedures. Let's unpack how these utility scams work, examine a real-life case, understand its mechanics, and lay out steps to protect yourself and those around you.

A Real-Life Utility Scam

The Case of the Phantom Power Company

In 2021, scammers launched an aggressive campaign impersonating major utility companies like PG&E in California, Con Edison in New York, and ComEd in Illinois. They employed chillingly effective tactics.

One pervasive scheme used automated robocalls to tell victims that their power company would disconnect their electricity in 30 minutes unless they paid a delinquent bill. Some victims were transferred to live agents posing as customer service representatives, who cited account numbers, addresses, and even recent usage patterns—details scraped from past data breaches or public databases that suggested legitimacy.

In Texas, an elderly couple lost nearly $900 after a scammer claimed they had tampered with their smart meter. The scammer warned that unless the couple immediately paid a fine, via prepaid debit card, a technician would arrive within the hour to shut off service and involve law enforcement. In a panic, the couple complied. *ABC7 Eyewitness News (Chicago)*, "Elderly Couple Scammed by Fake Electric Company Call," April 2021.

In Chicago, scammers used VoIP (voice over internet protocol) to make it look like calls came directly from ComEd. The fraud was so convincing that a suburban dental office paid $1,200 to "avoid a shutoff" during business hours.

According to the Federal Trade Commission (FTC), tens of thousands of people fell for similar scams that year, losing more than $196 million to imposter scams, many of which involved utility companies. The utility scam became so widespread that in 2021, the Federal Communications Commission (FCC) warned consumers about utility-related phone scams, specifically those involving utility disconnection threats. Scammers often impersonate utility company representatives and demand immediate payment, sometimes using prepaid cards or other non-refundable methods, to avoid disconnection. The FCC advises consumers to be skeptical of calls claiming immediate payment is needed to avoid service cutoffs and always to verify the legitimacy of the call with the utility company directly.

The damage wasn't just financial. These calls created stress, fear, and in some cases, medical risk. One Illinois woman reported nearly missing her insulin delivery after shutting off appliances and trying to conserve what she thought was soon-to-be-disconnected power.

Anatomy of a Utility Scam

Fraudsters design these scams precisely, building in intense pressure, time limits, and enough believable information to induce the victim to act without thinking.

1. Target Selection

Scammers don't dial mindlessly. They often use stolen or purchased data, compiled from previous hacks or sold by shady data brokers, to build profiles of likely victims. Seniors, especially those living alone or on fixed incomes, are prime targets.

Some scammers call businesses during peak hours, knowing employees are busy and less likely to verify details.

2. Spoofed Caller ID and Language Mimicry

Thanks to spoofing technology, scammers can make your caller ID display your actual utility company's number. They may include authentic company logos and language in follow-up emails or text messages, increasing perceived authenticity.

These fake agents use utility jargon, such as "reconnect fee," "smart meter fault," or "disconnection order issued"—language that sounds plausible but serves to intimidate.

3. The Threat of Disconnection

The core of the scam is urgency: "Pay now or lose service." This pressure causes victims to stop questioning and

start reacting. The scammer often mentions a service truck “in the area” or “dispatched already.” They may even put the victim on hold and return pretending to have “checked with dispatch.”

This creates a false but powerful sense of immediacy.

4. Untraceable Payment Demands

The scammer insists on payment via:

- Prepaid debit cards (e.g., Green Dot, MoneyPak)
- Gift cards (Amazon, Apple, Google Play)
- Cryptocurrency wallets
- Mobile payment apps (Zelle, Cash App, Venmo)

Scammers favor these methods because they’re nearly impossible to trace or recover. They often tell victims to read card numbers aloud or send screenshots, giving scammers immediate access to the funds.

Why This Scam Works

You might ask, “How do people fall for this?” As attorneys, we pride ourselves on critical thinking, but fear and urgency can short-circuit logic, and that’s the scammer’s playground.

Fear of Loss

Heat, refrigeration, and medical devices are essential services requiring power. The thought of losing them creates emotional panic, especially for seniors or those with health conditions.

Realistic Setup

These scams often involve multiple layers: a robocall, a live agent, and even a follow-up email. They sound official. They use professional language. Sometimes, the scammer has just enough personal data, like a last payment amount, to convince you they're the real deal.

Social Engineering

Scammers mirror legitimate companies' exact methods: phone menus, call-back numbers, and confirmation codes. By the time the call ends, victims are often stunned to learn the truth.

Real-World Impact

According to the Federal Trade Commission (FTC), imposter scams (including scammers posing as utility companies) were the *most reported scam category* in 2021, with Americans losing more than $2.3 billion overall. Federal Trade Commission, *Consumer Sentinel Network Data Book 2021*, https://www.ftc.gov/system/files/ftc_gov/pdf/csn-2021.pdf

Utility scams ranked high among older adults in terms of financial losses and emotional impact. Many victims hesitate to report these crimes due to embarrassment or fear of appearing vulnerable, especially retired

professionals used to being the helpers, not the helped.

Let's not overlook the psychological harm. Victims report feelings of shame, anxiety, and loss of self-confidence. Some become reluctant to answer phone calls or respond to legitimate mail. The ripple effects of financial fraud often linger long after the economic loss.

Real Victims, Real Harm

Consider the case of Mary Lopez, a 72-year-old retired nurse in El Paso, Texas. She received a call allegedly from El Paso Electric. The caller, a polite man who knew her address, said her account was overdue by two months and service would be cut off in 30 minutes.

"I panicked," she later told the *El Paso Times*. "I thought, 'I need my oxygen machine—what if they turn it off?'"

Mary rushed to a nearby Walgreens, bought $500 worth of Green Dot cards, and gave the scammer the numbers over the phone. When she called the real utility company later, they confirmed her account was current and that she'd been scammed. *El Paso Times*, "El Paso Electric Scam Targets Elderly Residents," (March 15, 2021), https://www.elpasotimes.com

In another case in Chicago, a law office received a similar call. The scammers told the receptionist that the firm's utilities would be disconnected unless $1,200 was paid immediately. The office manager, sensing something was off, called ComEd directly. Sure enough, there was no outage or overdue balance. The firm had narrowly avoided becoming a victim.

For every close call, however, countless others—often older Americans or those living alone—lost hundreds or thousands of dollars. Worse, victims frequently felt ashamed or embarrassed, making them reluctant to report the crime.

Legal, Ethical, and Technological Dimensions

From a legal perspective, utility scams often fall into wire fraud and elder financial abuse categories. Unfortunately, prosecuting perpetrators is difficult, especially when operations are based overseas.

In many cases, money is funneled through “money mules,” individuals who unknowingly help launder funds before disappearing into cryptocurrency markets, making recovery exceptionally rare.

States like California and New York have begun mandating that utility companies publish scam alerts and implement additional customer protections. Several states have passed *elder abuse protection laws* aimed at financial scams, but enforcement varies.

How to Protect Yourself and Others

You don’t need to live in fear of every phone call. But a little strategy goes a long way.

1. Know the Real Procedure

Utility companies:

- Send written notices of overdue accounts
- Offer payment plans, not ultimatums
- Don’t demand payment via gift or prepaid cards

If you receive a threatening call, hang up and call the number on your latest bill—not the one the caller gives you.

2. Don't Trust Caller ID

Caller ID spoofing is rampant. Never rely on the number displayed as proof of authenticity. If a caller pressures you, tell them you will call the company back directly. A legitimate representative will understand.

3. Spread the Word

Talk to friends, family, and neighbors about these scams. Many retired attorneys still hold roles of influence in community groups, church boards, and bar associations. Use that credibility to educate others.

Hold a brief fraud awareness session at your HOA or local library. Sharing stories like Mary Lopez's can make others pause before paying a scammer.

4. Freeze Your Credit and Use Strong Passwords

Many scammers pull your data from compromised accounts. Mitigate risk by:

- Placing a freeze on your credit files with Experian, TransUnion, and Equifax.
- Use unique, secure passwords for online utility portals.
- Enabling two-factor authentication wherever available.

5. Report the Scam

If you or someone you know is targeted:

- File a complaint with the **FTC**: reportfraud.ftc.gov
- Notify the **state attorney general**
- Contact the **utility company**'s fraud department
- Inform the **local police**, especially if there's financial loss

Reporting isn't just about justice—it helps authorities spot patterns and alert others.

Technology Is a Double-Edged Sword

As AI-driven robocalls have become more sophisticated and scams evolve into SMS text threats and phishing emails, awareness must keep pace with innovation.

Voice-cloning tools can already impersonate loved ones. AI-generated scam emails appear more polished than ever. Scammers have even weaponized QR codes to divert people to fake utility payment sites.

Utility scams will morph—but so will our defenses. Older adults, particularly those with legal backgrounds, can become fraud-fighting ambassadors. Use your experience to help decode these schemes and build a firewall of community knowledge.

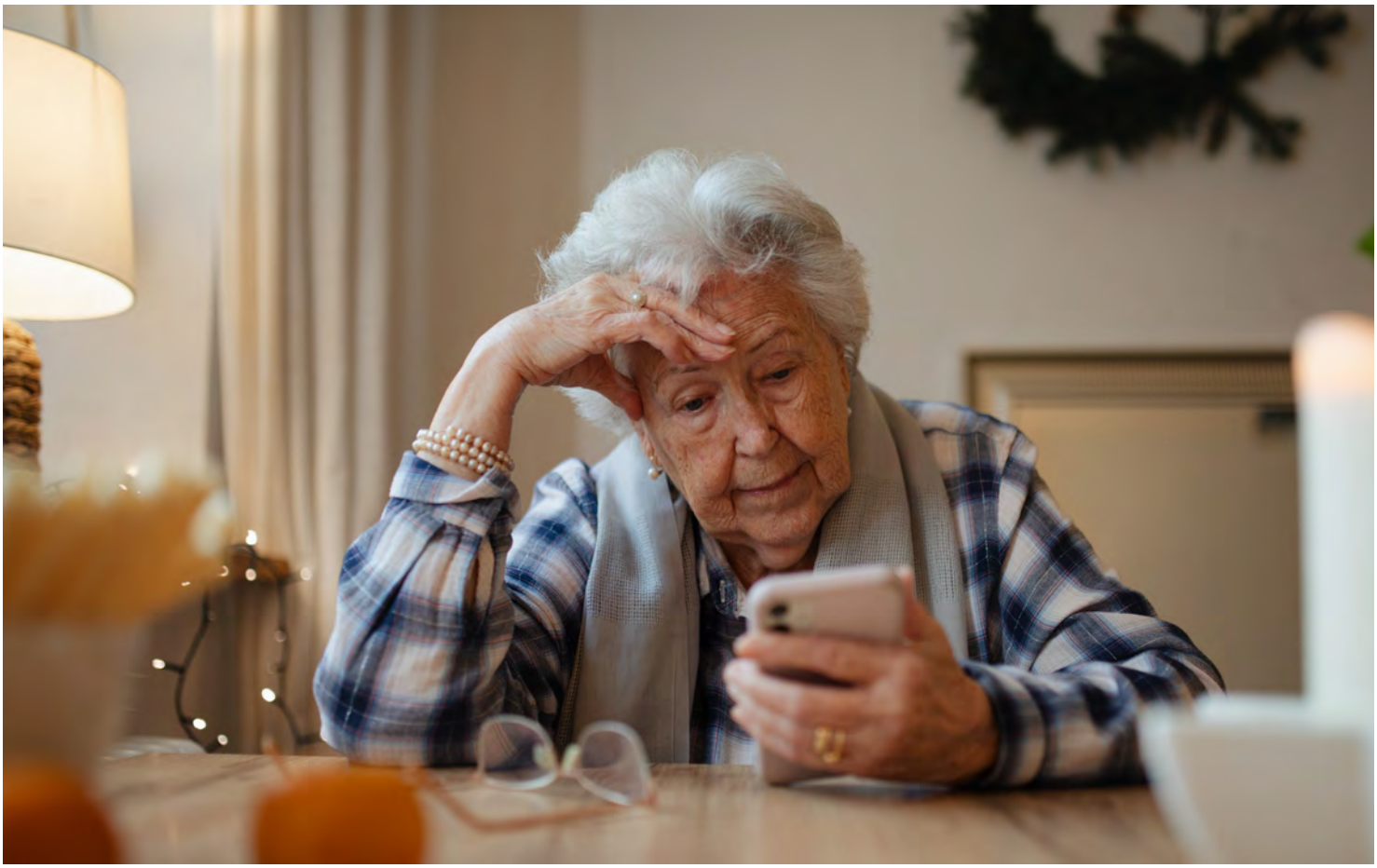
Lessons for Senior Lawyers on AI Mishap Legal Practice

Jeffrey M Allen and Ashley Hallene

Nov 06, 2025 10 min read

Summary

- Even tech-savvy lawyers are vulnerable to “hallucinated” cases if they trust AI output with verification.
- Lawyers must independently verify all AI-generated legal research to avoid ethical breach sanctions.
- Implement multi-level review protocols and ongoing education to ensure the safe integra AI into legal practice.



istock.co

Jump to:

The Rise (and Risks) of AI in Law →

Recent Reality Checks →

A New Kind of Professional Risk →

Practical Guardrails for Experienced Practitioners →

How to Verify AI-Generated Legal Research →

Embrace AI—But Don't Abdicate Judgment →

The recent article by Ethan Baron, *"Palo Alto Lawyer: AI Made Cases Up,"* in the East Bay Tim 2025), provides a timely reminder about the use of AI and inspired this article. Baron recour of a Palo Alto lawyer who discovered that the AI tool he used hallucinated—"made up"—cas he filed. We hope this is not the first time you have heard of such an occurrence, but it may

time you have encountered it involving an experienced attorney with expertise in technolog should set off alarm bells among all of us. (Credit to Baron and the East Bay Times for bringi light.)

According to Baron's reporting, the lawyer used an AI tool to help draft a court filing, only to later that several of the cited cases didn't exist. No malicious intent, just misplaced trust. Un this episode isn't an isolated embarrassment. But it serves as a cautionary tale for every atto unpack what's happening, why it matters, and how you—yes, even you, a senior partner—ca becoming the next headline.

The Rise (and Risks) of AI in Law

AI isn't just a buzzword anymore. From contract review to legal research, AI-powered tools a everywhere. They promise speed, efficiency, and sometimes even a little magic. But as Baro and a growing body of case law demonstrate, they also bring new risks—especially when law them too much.

Why Even Tech-Savvy Lawyers Get Tripped Up: You might think, "I'm careful. I know techn won't happen to me." But here's the rub: AI tools are designed to sound convincing. They're massive datasets, and when asked for a case citation, they'll produce something that looks r it's not.

Cognitive Offloading: As Lars Daniel writes in Forbes, the real danger is "cognitive offloadir AI do the thinking, and assuming its output is correct without human review. The more expe are, the more tempting it is to trust the technology. After all, you've seen it work wonders.

Pressure to Be Efficient: Law firms are under pressure to deliver faster, cheaper, and more comprehensive services. AI promises all that, but the temptation to "set it and forget it" caus

Lack of AI Literacy: Many lawyers—even those in technology—don't fully understand how g works, or its limitations. As the Digital Watch Observatory notes, the real issue isn't the techn but the lack of AI literacy in the profession.

The Paradox of Experience: You might ask: how could a veteran who has litigated, reviewe advised startups, and negotiated AI licensing deals fall prey to AI hallucinations?

1. The Confidence Trap

Experience breeds confidence, and confidence can breed shortcuts. Many of us have spent
mastering research tools, including Lexis, Westlaw, Fastcase, and Casetext. We know how to
citation, vet a source, and spot a phony precedent. That deep familiarity can lull us into thin
know if the AI gets it wrong." But you won't—because when AI "hallucinates," it fabricates wi

We think that technical fluency immunizes us against technology mistakes. Because we und
models, neural nets, licensing, APIs, etc., work on paper, we may extend that confidence int
we can detect when the AI "lies." But generative models are probabilistic engines — they off
seeming outputs, not guaranteed truths. Just knowing how "attention heads" or embedding
not make you immune to deception.

Generative models like ChatGPT or Claude don't *know* the truth; they generate text that is st
probable. That means an invented case can look perfectly genuine, complete with volume n
citation, and a judge's name.

2. The Efficiency Mirage

One of AI's selling points is speed. Draft a motion, pull up a hypothetical, suggest an annotat
temptation is to rely on AI for the first draft, then make minor edits. But if the first draft is bu
fabrications, there's no editing salvo strong enough. The faster the tool, the more seductive
—and the greater the latent hazard. The trouble comes when "first draft" quietly becomes "f
Once the citations are formatted and the prose sounds lawyerly, the temptation to trust it b
immense.

3. The "plausible but false" Trap

Generative AI models are notorious for "hallucinations": statements or citations that sound a
but don't correspond to actual authority. A recent benchmarking study revealed that legal A
hallucinate in a significant proportion of queries—either by misstating the law or citing sour
don't support the assertions. Because we're used to reading polished prose from these tool
be fooled by sophisticated-seeming arguments that collapse under scrutiny.

4. Delegation Drift

Senior lawyers often delegate AI-assisted tasks to juniors, associates, or staff. It's part of hov manage risk and time. The temptation is to treat AI as a "junior associate" whose output nee But by the time it arrives, the senior lawyer may skim crucial parts and assume correctness- "last mile" failure. When you do that, you're no longer supervising effectively; you're rubber- potentially false work. But AI complicates the supervision dynamic. If an associate or paraleg draft a memo, and you only skim it, you might never see the phantom case that slipped in. Courts, however, won't excuse you for not knowing.

5. Complacency About Competence

Rule 1.1 of the ABA Model Rules requires that we provide competent representation. Comm that this duty includes "keeping abreast of the benefits and risks associated with relevant te That language may not have envisioned hallucinating robots—but it covers them now.

6. Overlooking Professional Responsibility

Many experienced attorneys have longstanding habits about checking authority, verifying ci confirming sources. But AI can insidiously erode those habits. If you tell yourself, "The tool is catch the big mistakes," you may stop doing the small but critical granular checks that could flagged an error.

Recent Reality Checks

Baron's *East Bay Times* story was hardly the first warning shot. Over the past two years, cou scolded or sanctioned attorneys for relying on AI-generated fiction.

Mata v. Avianca (S.D.N.Y. 2023): One of the most widely cited "oops" cases is Mata v. Avianca counsel used ChatGPT to draft a motion and included numerous case citations found to be f court dismissed the claims and fined the lawyers $5,000 under Rule 11.

What makes this relevant to senior lawyers is the gaffe, and that many now regard *Mata* as a point in how courts view AI-assisted drafting. The case circulated fast as a warning: if you rel on generative AI, you risk sanctions, and your credibility is on much thinner ice.

Sanctions and Discipline in Multiple Jurisdictions

Let's look at a few recent cases, so you know this isn't just a one-off:

- **Texas:** A lawyer was sanctioned for submitting a brief with two non-existent cases a quotations, all generated by AI. The court imposed a $2,000 penalty and required cc education on AI.
- **California:** Amir Mostafavi, a California attorney, was fined $10,000 for citing 21 fak appellate brief. He claimed he didn't know AI could hallucinate, but the judge made lawyers must verify every citation.
- **Pennsylvania:** An attorney was sanctioned after submitting briefs with fabricated ci product liability case. The court found the referenced cases didn't exist or containec errors.
- **Florida:** A lawyer was suspended for citing non-existent AI-generated cases in a fede pleading, highlighting the ethical implications of AI misuse.
- **UK:** The High Court sounded the alarm after lawyers cited dozens of fictitious cases, profession to take swift action to address AI misuse.

And these are just a few. As of mid-2025, there have been at least 156 cases where lawyers generated cases in court documents.

Reuters: AI Hallucinations in Court Papers Spell Trouble for Lawyers

Reuters reported in early 2025 that at least seven similar incidents had occurred nationwide one in Wyoming, where a judge threatened to impose sanctions after discovering false AI-ge authorities.

Reuters: Anthropic's Lawyers Take Blame for AI Hallucination. Even big firms aren't immune. 2025, Latham & Watkins acknowledged that a false citation in a filing originated from a gene tool called Claude, developed by Anthropic. A Latham & Watkins attorney admitted to an "e and unintentional mistake" in a citation, caused by Claude, that misattributed authors and f

the citation. The lesson? Even a top-tier firm got caught by an AI hallucination — and had to firm publicly accepted responsibility for what it called "an embarrassing and unintentional m

> If you want a brain teaser, consider this: If Anthropic, the developer of Claude, sues La & Watkins for malpractice, does Latham & Watkins have a viable affirmative defense t damage claim based on the fact that the plaintiff, Anthropic, developed the defective AI?

- LA Times: AI Hallucinations Are Becoming a Real Problem for Lawyers
  Los Angeles Times columnist Michael Hiltzik observed that judges are growin increasingly impatient with "AI excuses." *"Courts don't care whether the br written by ChatGPT, your intern, or your cat. They care whether the law yo actually exists."*

- Stanford HAI: AI on Trial (2024)
  A 2024 Stanford study found that leading AI legal-research tools hallucinated in roug of six benchmark queries.

- Large Legal Fictions: Profiling Legal Hallucinations in LLMs (2024)
  In *"Large Legal Fictions: Profiling Legal Hallucinations in Large Language Mo* et al. examined multiple models and found hallucination rates for law-dom as high as 58% with ChatGPT-4 in certain jurisdictions and query types. Th hallucination is not a fringe phenomenon; it's baked into existing models.

A complementary study, *"Hallucination-Free? Assessing the Reliability of Leading AI Legal Re Tools,"* found that for open-ended legal queries, hallucinations either misstate law or misatt sources with a disturbing frequency. Tools that appear reliable can sometimes be subtly fla dangerous ways.

A New Kind of Professional Risk

These misfires carry real consequences. Courts may impose sanctions, but the deeper dang reputational. A single hallucinated case can make a lawyer appear careless—or worse, dishc

Malpractice insurers are paying attention. Several carriers have begun asking applicants wh use AI in legal drafting and, if so, how they verify results.

Ethics authorities are watching too. The ABA's Formal Opinion 512 (2024) underscores that l using generative AI must ensure "the accuracy of its output" and must not delegate indepen judgment to the machine.

Practical Guardrails for Experienced Practitioners

If the above sounds like a litany of doom, don't despair. AI still holds enormous promise. Ho must approach it as a powerful tool that requires strict handling. Here are some guardrails a practices—meant especially for experienced technology and litigation attorneys, but valuabl attorneys.

1. **Adopt a "Trust but Verify" Policy**
   Assume every AI citation is wrong until proven right. Verify the existence, accuracy, a relevance of data in a primary database.

2. **Prefer Retrieval-Augmented Systems**
   Choose AI tools tethered to verified legal repositories. Always ask: "Where does this from?"

3. **Build structured review protocols**

Set up multi-level review processes:

- Associates or researchers generate with AI, but annotate every citation candidate.
- A mid-level attorney manually checks each candidate.
- The senior does a final "spot check" on high-risk sections (e.g., novel arguments, larg rather than skim the whole thing superficially.

4. Document Your Oversight
Keep notes on the AI you used and how human verification was performed.

5. Maintain a "hallucination red flag" checklist

Some patterns are suspicious and deserve extra caution:

- Citations to obscure or niche cases in jurisdictions unrelated to your matter.
- Universe-shifting language: "As held in X, which established that all Y must do Z," wh statement is sweeping.
- The case name seems formulaic (e.g., Smith v. Acme Products, 1987), but you can't f
- Quoted passages that don't appear (or appear in a different context).

If the tool flags "uncertain" or "unsupported" citations, treat those as especially suspect. Enc staff to flag them automatically.

6. Use AI Where Stakes Are Low
Safe uses include outlines, summaries, and brainstorming. Avoid unsupervised use in legal f

7. Train and Supervise
Conduct office-wide education on AI risks and error spotting. Encourage an open culture arc mistakes. Don't let the younger generation be the only ones experimenting with AI. Mandate training sessions on hallucination, reviewing cases like *Mata*, and sharing "almost got me" st current on developments in AI law, professional responsibility rules, and ethics guidance. Th opinion on generative AI in law was issued in 2024 (following *Mata*) and contemplates a lawy of competence, supervision, confidentiality, and verification, even in the context of AI use.

8. Review Client-Disclosure Obligations
Be candid if AI was used in client deliverables. Transparency builds trust.

9. Stay Educated
Follow ongoing ethics updates from the ABA and your state bar.

How to Verify AI-Generated Legal Research

Here's a quick checklist for verifying AI-generated legal content:

- **Check Citations:** Look up every case in official databases.
- **Review Quotes:** Read the full text of cited cases to confirm quoted language and its
- **Assess Reasoning:** Make sure legal arguments are grounded in real law, not plausib fiction.
- **Use Verification Tools:** Platforms like CiteStrike can cross-reference citations again databases.
- **Ask "Are You Sure?":** Prompt AI tools to double-check their own output, but never r their self-assessment.

For more detailed guidance, see Paxton AI's best practices and Simbo AI's verification steps.

Embrace AI—But Don't Abdicate Judgment

AI is here to stay, and it's transforming legal practice in ways we're only beginning to unders Ethan Baron's reporting and a growing body of case law clarify, even the most experienced t attorneys can—and do—get it wrong. The lesson? Don't let the promise of efficiency blind yo need for diligence. Treat AI as a powerful assistant, not a replacement for your expertise. Ve everything, stay current on ethics, and never be afraid to admit and correct mistakes. If you not only avoid the pitfalls that have tripped up some of your peers—you'll set the standard f responsible, effective use of AI in law.

Authors





Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...

Ashley Hallene

Ashley Hallene is an Attorney and Land Acquisition Specialist with Demeter Land Development. She is based in Houston, Texas. She is the co-author of several books, including Technology Tips for Seniors Volume 2.0 (2018),...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-november/senior-lawyers-avoiding-ai-mishaps/?utm_source=chatgpt.com

GPSolo Magazine GPSolo, May/June 2026 (43:3): What to Do When . . .

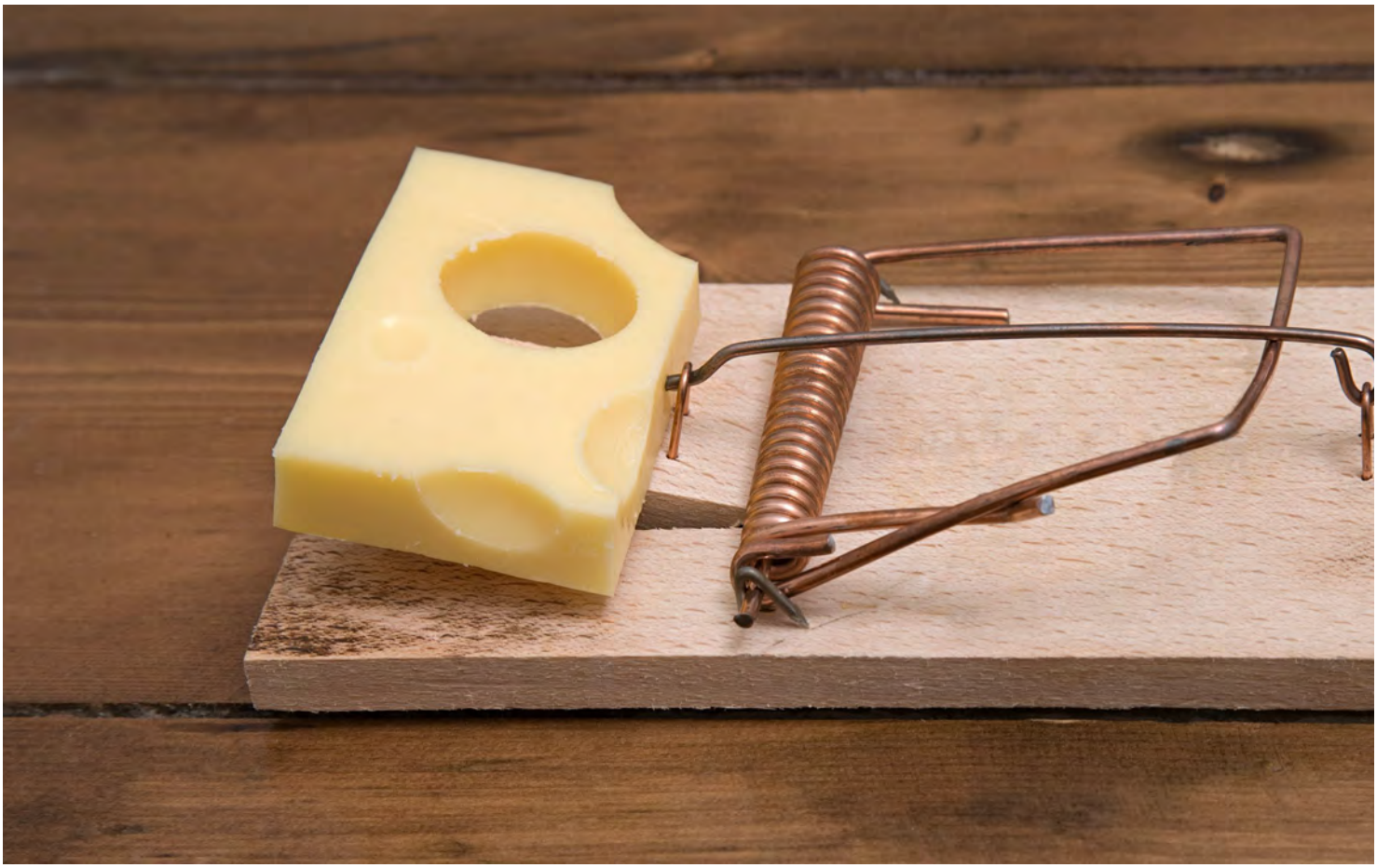
How AI Is Reengineering Scams Aimed at Lawyers

Jeffrey M Allen

Jun 02, 2026 10 min read

Summary

- Using AI, scammers can scrape public court dockets, law firm websites, bar listings, Linke profiles, marketing pages, and social media posts to generate convincing messages that authentic and even routine.
- For solo and small firm lawyers, AI-enabled scams can have existential consequences. A s incident can threaten client trust, bar discipline, malpractice coverage, and the survival o practice itself.
- Lawyers working outside the office are particularly vulnerable as they are more likely to multitask and rely on mobile devices or unfamiliar networks, and less likely to have acces colleagues or staff.
- You cannot defeat AI scams by telling people to “be careful.” Scams are defeated by implementing systems that create process friction—deliberate obstacles that slow things



Connect Images via G

Jump to:

Why Lawyers Are Prime Targets (and Always Have Been) →

From Typos to Tone Matching: The Death of the Obvious Scam →

The New Generation of AI-Powered Legal Scams →

Why Mobility Changes Everything →

Why Smart Lawyers Still Fall for This →

The Statistical Reality (Briefly and Without Drama) →

Ethical Duties Don't Care How the Scam Worked →

Why "More Training" Does Not Suffice →

Structural Defenses That Actually Work (Especially for Mobile Lawyers) →

AI Threat Vectors for Lawyers Working Outside the Office →

The Coming Wave: AI vs. AI →

A Cultural Problem, Not a Technical One →

Final Thoughts from the Road →

After enough miles on the road, you learn that every profession attracts its own predators. Truck stops have them. Trade shows have them. The legal profession—despite its education, ethics rules, and fixation on risk—has always had them as well. In earlier iterations, they arrived as bad investments, fictitious clients, forged checks, or "urgent" wire-transfer requests sent five minutes before a Friday holiday.

Long before artificial intelligence (AI) entered the conversation, lawyers who worked outside the office already navigated ethical and operational risk: confidential calls taken in public, sensitive email reviewed on small screens, deadlines managed between hearings, and consequential decisions made in the absence of time—or colleagues—who might otherwise slow the process.

What has changed is not lawyer carelessness. Scammers can now exploit the modern legal work environment with far greater efficiency, and most lawyers and law firms have not kept up with the scammers.

AI did not invent scams that target lawyers; scammers have run variations for decades. AI has changed the economics of deception: It removes friction for the attacker, increases tempo and pressure for the lawyer, and makes manipulation scalable, personalized, and credible enough to survive brief scrutiny—especially on a phone, in transit, and under deadline stress.

In short, we face a new instantiation of an old problem: the long con, updated for a profession that no longer operates behind a closed office door. The threat landscape has shifted materially. Scammers have made their attacks look less and less like scams.

They now sound like clients you've already met, colleagues you trust, vendors you have paid for years, and judges you would rather not disappoint. They write polished emails, reference real matters, and borrow a firm's internal language. Most importantly, they strike when you are busy, fatigued, and one step behind your inbox.

The engine behind this shift is not merely more sophisticated social engineering. It is AI: industrial-scale, automated, and relentlessly efficient.

This is not a future problem. It is present tense—and lawyers sit squarely in the crosshairs.

Why Lawyers Are Prime Targets (and Always Have Been)

Let's be honest: Scammers have always seen attorneys as attractive marks.

Lawyers move money. They maintain escrow and trust accounts. They communicate under urgency. Professional norms train them to respond rather than doubt; courts and clients condition them to comply quickly with authoritative requests.

Scammers have exploited this for decades. The "fake client with overseas funds" scam. The counterfeit settlement check scam. The bogus vendor invoice. The spoofed managing partner email asking accounting to "just take care of this."

What's different now is *scale* and *precision.*

AI allows scammers to:

- Study law firm websites and LinkedIn profiles at scale
- Mimic writing styles with uncanny accuracy
- Generate personalized messages instantly
- Operate dozens of simultaneous scam campaigns without human fatigue

We no longer contend with handcrafted cons; we contend with manufactured cons.

Solo and small firm lawyers—who often combine intake, accounting, client communication, and case management in a single person—face an unusually broad attack surface. They have fewer internal checkpoints and a reduced number of

informal “does this look right to you?” moments. That structure reduces the opportunities for someone else to slow the process down.

From Typos to Tone Matching: The Death of the Obvious Scam

For years, lawyers comforted themselves with a simple heuristic: *real professionals don’t write like that*. Bad grammar. Strange phrasing. Foreign idioms. Misspelled names. Those were the tells. The red flags. The easy outs.

AI has reduced that playbook to ashes.

Large language models don’t just write correctly—they write *convincingly*. They can replicate the tone of a senior partner, the cadence of a court clerk, or the clipped efficiency of a long-time client. Just as important, they retain details, avoid fatigue, and rarely introduce the clumsy errors that once gave scams away.

Modern scam operations no longer rely on a single badly written email or an implausible story. They rely on volume, variation, and context. With AI, scammers can scrape public court dockets, firm websites, bar listings, LinkedIn profiles, marketing pages, and social media posts, then assemble profiles showing how a lawyer writes, who they work with, what kinds of matters they handle, and how their firm communicates.

Using that information, scammers generate messages that feel internal rather than foreign.

That difference matters.

The modern scam email doesn’t look rushed or sloppy. It looks *reasonable*. Sometimes, it looks boring. And that’s exactly the point. Often, the message does not demand immediate action. It asks for confirmation. Clarification. A routine follow-up.

That is precisely why it works.

Scams no longer announce themselves as emergencies. They present as normal work—

work that a lawyer expects to see and expects to handle quickly.

The New Generation of AI-Powered Legal Scams

Let's focus on what practitioners face in real time—not hypotheticals or marketing copy, but recurring patterns appearing in firms of every size.

1. Voice Cloning and the "Urgent Call"

Voice cloning used to be a novelty. Now it's a commodity.

Scammers scrape public recordings—webinars, CLEs, podcasts, even voicemail greetings—and generate passable voice replicas. Not perfect, but good enough to bypass a moment's skepticism.

The call comes in late afternoon. The voice sounds like the managing partner or a major client. The request is urgent but plausible: a wire transfer, a confidential payment, a last-minute filing fee.

Because the voice sounds right, the normal friction disappears.

No longer science fiction, voice cloning has been used by scammers to trigger six-figure losses—for example, a 2019 case in which criminals used AI-generated audio to impersonate a CEO's voice and induce a €220,000 (about $243,000) transfer (Catherine Strupp, *Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case*, Wall St. J., Aug. 30, 2019).

2. Deepfake Videoconferences

Video used to be the gold standard for verification.

AI has eroded that standard.

Scammers now use AI-generated video avatars—combined with real-time face mapping—in short meetings to "confirm" instructions. The lighting is slightly off. The eye contact isn't perfect. But when the call is brief and the stakes feel routine, people don't

scrutinize.

The scam doesn't need perfection. It only needs *enough*.

3. Hyper-Personalized Phishing Emails

AI shines here—and lawyers have a particular vulnerability. Scammers no longer send generic emails. They reference:

- Active matters
- Known opposing counsel
- Real judges and clerks
- Actual deadlines

They pull this information from public dockets, firm blogs, press releases, and social media. AI stitches it together into messages that feel internal. An email that says, *"Following up on the Smith v. Calderon TRO—need confirmation we can release funds per yesterday's discussion,"* doesn't raise alarms. It triggers muscle memory.

4. Fake Clients That Pass Initial Screening

AI-generated personas now survive intake often enough to cause real damage.

Many present with polished LinkedIn profiles, respond intelligently to follow-up questions, and supply documentation that looks plausible at first glance. On paper—and often on the phone—they resemble the clients that firms want.

Until money changes hands.

Scammers often steer the matter toward escrow, trust accounts, or third-party payments—areas where lawyers have both access and authority.

Why Mobility Changes Everything

Most discussions of legal-industry scams focus on technology: email security, malware, spoofed domains. Those matter. But they miss a critical factor: environment. The most successful AI-assisted scams focus on the lawyer's *location* when they receive them.

Lawyers in their office have friction working in their favor. Multiple screens, familiar systems, and colleagues nearby. Established procedures for financial or administrative tasks. Even the act of standing up to ask someone a question can interrupt a bad decision.

A lawyer on the road has none of that. Lawyers working outside the office are:

- More likely to rely on mobile devices
- More likely to multitask
- Less likely to have immediate access to colleagues or staff
- More likely to use unfamiliar networks or devices

Working remotely or in transit often means you read and respond on a phone or laptop with limited visibility, while juggling messages between hearings, flights, or client meetings. You respond quickly because practice rarely carves out time for reflection.

This does not reflect poor judgment. It reflects the realities of modern practice. Scammers engineer AI-driven scams to land in those moments. A wire transfer request that would raise questions at a desk can feel routine when reviewed in an airport lounge. An intake email that would prompt follow-up questions in the office can slide through when read late at night in a hotel room.

Mobility doesn't make lawyers reckless. It makes them efficient. Today's scammers exploit that efficiency.

Why Smart Lawyers Still Fall for This

Whenever a firm gets hit, someone inevitably asks the wrong question: *How did they not see it?* That question assumes scams fail because of ignorance. In reality, they succeed because of *context.*

AI scams are engineered to exploit:

- **Urgency:** "We need this done now."
- **Authority:** "This came from the top."
- **Familiarity:** "This looks like how we normally work."
- **Cognitive overload:** "I have ten other things going on."

Lawyers operate in environments where delay can cause harm. That makes them more—not less—susceptible to well-timed deception. These are not bugs in the profession. They are features. Working outside the office amplifies those features. It leaves fewer chances to slow down, fewer informal interruptions, and fewer systems that force verification.

Smart lawyers fall for these scams not due to naivety but because the environment makes the wrong decision easy and the right decision inconvenient.

The Statistical Reality (Briefly and Without Drama)

The numbers are ugly, but we need not dwell on them.

According to the FBI's Internet Crime Complaint Center, business email compromise (BEC) schemes—many now AI-assisted—continue to drive billions in reported annual losses, with professional services firms disproportionately affected.

That's the only statistic you need.

Ethical Duties Don't Care How the Scam Worked

Here's the part that keeps managing partners up at night—and should make solo practitioners lose sleep. Clients don't care whether the theft was caused by AI, social engineering, or human error. Regulators don't either. Trust account rules remain unforgiving. Confidentiality obligations don't soften because the attacker used a neural network. From an ethical standpoint, the *method* of the breach has no relevance. What matters is that a duty was breached.

AI doesn't create new ethical rules—it just makes violations easier. For solo and small firm lawyers, the scam can have existential consequences. A single incident can threaten client trust, bar discipline, malpractice coverage, and the survival of the practice itself.

Why "More Training" Does Not Suffice

Most firms respond to scams the way they respond to every risk: a memo, a training, a checkbox. That approach has reached its "sell by" date.

You cannot defeat AI scams by telling people to "be careful." Scams are defeated by *process friction*—deliberate obstacles that slow things down, just enough to force verification, regardless of who initiates the request or how convincing it sounds.

If your firm relies on individual judgment alone, you're already behind the eight ball.

Structural Defenses That Actually Work (Especially for Mobile Lawyers)

The firms weathering this storm aren't smarter. They're more disciplined. They build systems that slow things down regardless of how convincing the request sounds or who appears to be making it.

Effective measures include out-of-band verification for any financial or credential-related request. Mandatory delays for non-routine transactions. Separation of authority so no single person can initiate and complete sensitive actions.

For lawyers who work outside the office, additional safeguards matter. Smart firms

implement:

- Limits on financial authority while mobile.
- Prohibition on trust-account actions from mobile phones.
- Out-of-band verification for any financial or credential-related request.
- Mandatory delays on unusual transactions, regardless of source.
- Separation of authority, so no single person can execute and approve sensitive actions.
- Clear refusal scripts, so staff can say “no” without fear.

None of this is glamorous. But it does work.

Below is a bullet summary you can use as your own guidelines or share with your team (or both).

AI Threat Vectors for Lawyers Working Outside the Office

Where Risk Increases

- Airports and hotels
- Court facilities
- Home offices
- Conferences and CLEs
- Client sites

Primary AI-Enabled Threats

- Email spoofing with matter-specific details
- Voice cloning targeting mobile phones
- Fake video calls for brief “confirmations”
- AI-generated clients during remote intake

Why Mobility Amplifies Risk

- Limited verification options
- Small screens and reduced context
- Time pressure and multitasking
- Lack of immediate peer review

Highest-Risk Actions While Mobile

- Wire transfers
- Trust-account disbursements
- Credential sharing
- Intake approvals

Practical Risk Reduction

- Pause-and-verify rules

- Out-of-band confirmation
- Transaction delays
- Restricted mobile authorization

The Coming Wave: AI vs. AI

The uncomfortable truth: Humans won't win this fight alone. As scams become faster and more adaptive, firms will rely on AI systems trained to spot anomalies in language, timing, and behavior. The future of scam prevention in law firms looks less like training seminars and more like *automated skepticism*—systems that pause, flag, and require confirmation before damage occurs.

That shift will prove uncomfortable. It will slow things down. And it will save firms millions.

A Cultural Problem, Not a Technical One

This is about culture, not technology. Law firms prize responsiveness. Deference. Speed. Those traits made sense in an analog world. In a synthetic one, they become liabilities. The firms that adapt will normalize verification, tolerate friction, and reward caution—not just efficiency.

Final Thoughts from the Road

I've spent years watching technology change how lawyers work. This shift feels different. AI doesn't just automate tasks. It *automates trust*—and then weaponizes it. Scammers no longer need to fool everyone. They only need to fool one person, once, at the right moment. AI gives them the tools to try endlessly until they succeed.

The road ahead is about realism, not panic. Assume the voice can be fabricated, and the email can be forged. Then treat urgency itself as potentially synthetic—unless and until you verify it.

The long con has gone digital. Lawyers should meet it with eyes open—and with systems designed for today's environment, not the one in which we wish we still practiced.

Author



Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association | https://www.americanbar.org/groups/gpsolo/resources/magazine/2026-may-jun/how-ai-reengineering-scams-aimed-lawyers/?utm_source=chatgpt.com

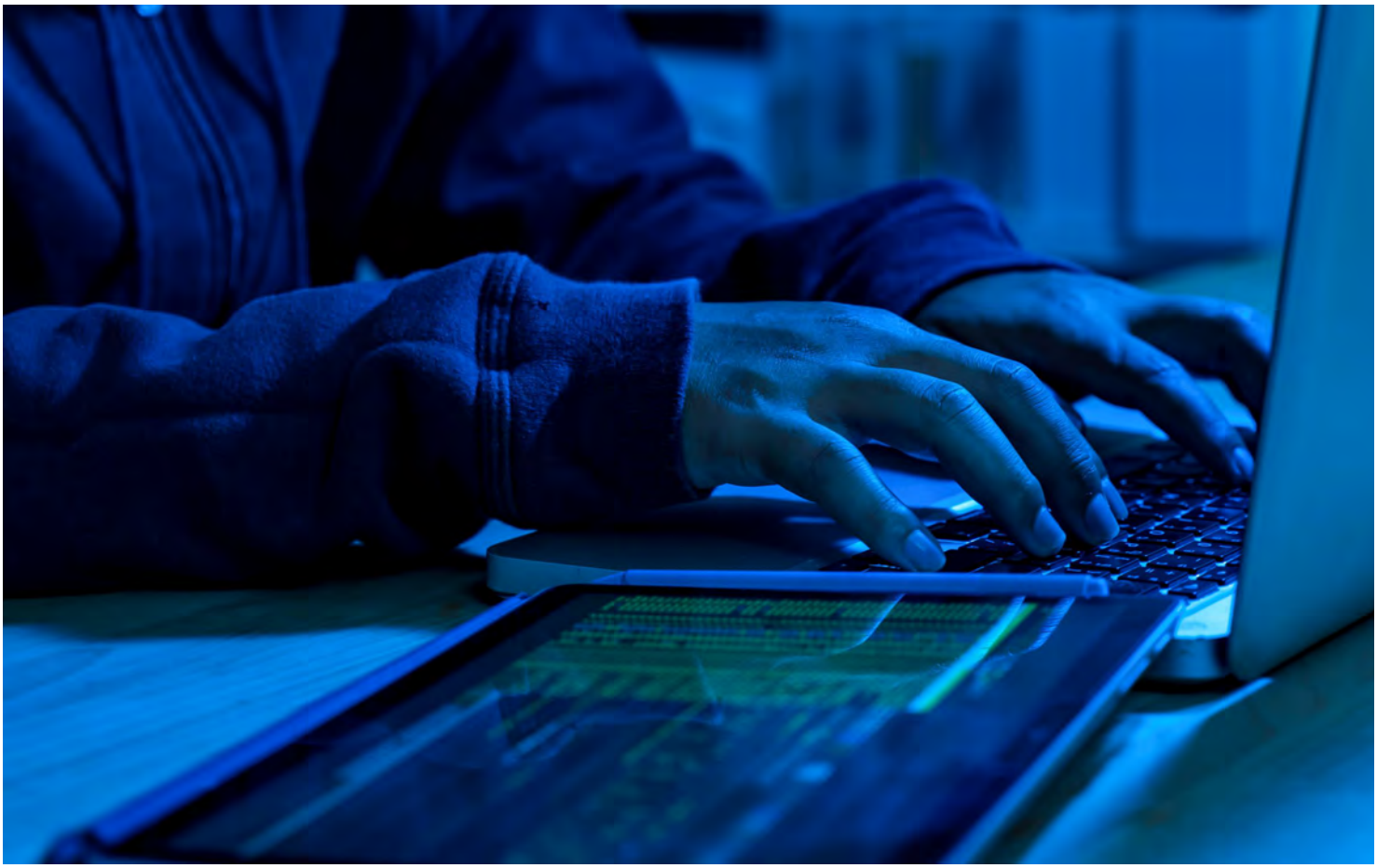
TAPAs: How to Know If You Are the Victim of a Cybercrime

Jeffrey M Allen and Ashley Hallene

Nov 26, 2024 4 min read

Summary

- **T**echnological **A**nd **P**ractice **A**dvice to help you become more efficient and effective. This month: tips for monitoring your financial records and credit reports for signs that you ha hacked.
- Check your real property records regularly to ensure no unauthorized changes or fraudu activities have occurred.
- Regularly review your credit reports from Equifax, Experian, and TransUnion. You are ent an annual free credit report from each bureau through AnnualCreditReport.com.
- Many banks and financial services offer account alerts that notify you of unusual activitie you can stay informed in real time.



boonchai wedmakawand via G

Jump to:

Tip 1. Review Real Property Records →

Tip 2. Monitor Your Credit Reports →

Tip 3. Regularly Check Bank Statements →

Tip 4. Enable and Respond to Account Alerts →

Tip 5. Long-Term Strategies for Protection →

The war continues. It grows and expands in scope and intensity daily. What war? The Russian invasion of Ukraine? The myriad invasions and counterattacks throughout the Middle East? The domestic war against food insecurity and homelessness? The first two sentences apply to all of those, but we speak of something different today. This article addresses the ongoing global Cyber War. We focus on the constant cyberattacks and

the consequent loss of privacy, security, property, and peace of mind. We consider it a slow month if we get only one or two letters advising us that some company we have dealt with suffered a data breach or cyberattack that compromised some of our private information. We would find it surprising if more than a few readers have never received such a notice. Even if you do everything right and take all the precautions, the fact remains that the mistake of a third party over whom you have no control can make you a casualty.

Fortunately, none of the data breaches we have received notices about resulted in any consequences for us. We hope you have been as lucky. We know others have suffered serious consequences and recognize that, at any time, it could happen to us or to you.

In many, if not most, incidents of consequences from such an event, the victim will learn of the problem relatively quickly and usually in no uncertain terms. The new "owner" shows up at your door ready to move into your house, which you did not sell. You receive a bill for a payment on a borrowing you did not make. Your bank denies the use of your credit card when you make a purchase because it saw something suspicious in another transaction and froze your credit card. These offer just a few real-life examples of the consequences that can result from a data breach impacting your personal information.

We have written about how to protect yourself in the past, explaining that the game goes by the name of risk mitigation, as you can never completely avoid all risks. If you become a cyber casualty in this war, you will find it helpful to discover it as soon as possible. The longer it takes for you to learn of the attack, the more damage that likely will have occurred. You cannot take corrective action unless you know that you have become a casualty. This article will address the problem from a different perspective. You need to constantly check to see if you have taken a hit. Hopefully, you have not, but if you have, you want to find out and quickly start to correct the situation.

Tip 1. Review Real Property Records

Check your real property records regularly to ensure no unauthorized changes or fraudulent activities have occurred. This includes verifying the ownership of your real estate and ensuring no new liens or mortgages have been placed on your property

without your knowledge. Most counties or municipalities offer online access to property records. You should check them several times a year. Ideally, you will make it a monthly ritual.

Tip 2. Monitor Your Credit Reports

Regularly review your credit reports from the three major credit bureaus: Equifax, Experian, and TransUnion. You are entitled to an annual free credit report from each bureau through AnnualCreditReport.com. Look for any unfamiliar accounts or inquiries that could indicate fraudulent activity. Check your credit report at least quarterly. Consider subscribing to services that will inform you of any changes to your credit reports.

Tip 3. Regularly Check Bank Statements

Closely monitor your bank and credit card statements. Look for unauthorized transactions or unfamiliar charges, and immediately report any suspicious activity to your financial institution. Statements usually come out monthly, and you should check each as soon as possible after it becomes available. Many banks have facilities that allow you to check prior statements and the current (yet unissued) statement online. We like doing that every seven to ten days. It only takes a few minutes, and you can do it almost anywhere.

Tip 4. Enable and Respond to Account Alerts

Many banks and financial services offer account alerts that notify you of unusual activities, such as large withdrawals or changes to your account information. Enable these alerts to stay informed in real time. Enabling the alerts does nothing if you do not timely respond to them, so if you get a notice of a potential problem or a communication from your bank asking for verification of a transaction, respond immediately. Know that most banks that send requests for transaction verification will freeze accounts until they receive that verification. If you inform them that you do not recognize a transaction, most banks automatically cancel your card and then mail you a new one with a different account number.

Tip 5. Long-Term Strategies for Protection

While immediate actions are essential to mitigate damages resulting from a breach, don't forget to do what you can to help prevent future exposure. Here are a few best practices for you to follow:

Use Strong Passwords and Two-Factor Authentication

Create strong, unique passwords for all your accounts and enable two-factor authentication (2FA) wherever possible. 2FA adds an extra layer of security by requiring a second verification form, such as a code sent to your phone or email address.

Keep Software Updated

Regularly update your software, including operating systems, browsers, and applications. Updates often include security patches that protect against known vulnerabilities. If you reach the point where your hardware no longer accepts operating system or software updates (or they no longer want to talk to your older hardware), understand that this is a message from the cyber police that you have obsolete hardware. Take it out of service and replace it immediately.

Educate Yourself on Phishing Scams

Phishing scams are a standard method used by cybercriminals to steal personal information. Learn to recognize the signs of phishing emails and messages, such as unfamiliar senders, urgent language, and suspicious links. Be careful with such emails and any attachments. We recommend that you simply delete them.

Authors





Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...

Ashley Hallene

Ashley Hallene is an Attorney and Land Acquisition Specialist with Demeter Land Development. She is based in Houston, Texas. She is the co-author of several books, including Technology Tips for Seniors Volume 2.0 (2018),...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |
https://www.americanbar.org/groups/gpsolo/resources/ereport/2025-january/tapas-how-know-if-you-are-victim-cybercrime/?utm_source=chatgpt.com

The Phishing and Fraud Scam

Jeffrey M Allen

Apr 30, 2025 4 min read

Summary

- Email is one of many ways scammers try to reach you; familiarize yourself with ways to recognize a scam email.
- Email phishing attacks prey on fear, urgency, and trust, exploiting even the most cautious individuals.
- When prompted to secure your bank account, do not follow email instructions; call your bank directly to check if there is actually a risk.



istock.com/baona

Jump to:

The Cost of Trust →

The First Red Flag →

How the Scam Worked →

The Spiral →

The Aftermath →

Lessons Learned →

The Cost of Trust

Jonathan Smith (name has been changed) never considered himself naive. A 45-year-old IT professional from Chicago, he prided himself on his analytical thinking and problem-solving skills. He had a stable career and monitored potential risks, especially money-related ones. None of that prepared him for the scam that would strip him of his savings and shake his confidence to the core.

It started innocuously enough: he received an email from his bank, alerting him to unusual activity on his account. The email bore the bank's official logo, used the right fonts, and the correct contact information. It contained a warning that his account might have been compromised. The email instructed him to use an enclosed link to go to the bank's website and secure his account. Jonathan clicked the link, which took him to a website that looked identical to his bank's login page. Without a second thought, he entered his credentials.

Within seconds, a message appeared: "Thank you. Your account is secure."

Jonathan exhaled in relief. He had avoided a disaster. Or so he thought.

The First Red Flag

Jonathan attempted to log in to his bank account using the official app the following day. The app rejected his password. Puzzled, he tried again. Nothing. Then, a notification appeared on his phone: the bank had processed a withdrawal of $9,750. His heart pounded as he called the bank's customer service line.

"I didn't authorize this," he told the representative, his voice shaking.

The agent looked into the account history. "Sir, several transactions occurred yesterday evening, including a wire transfer overseas. Did you approve them?"

Jonathan's stomach dropped. "No, absolutely not! I got your email about a security issue and logged in to fix it."

The agent paused. "Sir, we didn't send any such email."

Reality hit Jonathan like a freight train. He had been scammed.

How the Scam Worked

Jonathan fell victim to a classic phishing attack. Fraudsters had sent him an email masquerading as his bank, tricking him into clicking a link that led to a nearly identical fake website. When he entered his username and password, the scammers captured his login credentials in real-time. With those details, they accessed his actual bank account, changed his security settings, and drained his savings before he even realized what had happened.

But it didn't stop there.

The Spiral

As Jonathan frantically tried to recover his funds, he searched for ways to report the scam. That's when he stumbled into another deception.

He found a website that claimed to specialize in financial recovery for online fraud victims. The site featured testimonials from people who had allegedly recovered stolen funds, and its professional layout inspired confidence. Desperate, he called the provided number.

A man with a British accent answered. "Mr. Smith, I'm terribly sorry to hear about your loss. It may provide you some comfort to learn that many others have fallen victim to this type of scam. We've successfully helped hundreds of clients get their money back. We can begin recovery immediately if you allow us access to your case."

Jonathan hesitated, realized he could not get help immediately, and relented. He explained the scam, including the transactions. The so-called "recovery specialist" told him that his case looked promising and that, upon receiving a $2,500 retainer, they could begin legal proceedings to trace and retrieve the stolen funds.

"I don't have much left," Jonathan admitted, his voice hollow.

"I understand, sir. But the more quickly you act, the greater the chance of recovery. These criminals move fast, so you cannot afford to waste any time."

Desperate to recover his money, Jonathan wired the $2,500.

And just like that, he was scammed again.

The Aftermath

A week later, Jonathan called the recovery service, because he had not received an update. He discovered that the number no longer worked. He could not access the website, and the testimonials, likely fake from the beginning, had also gone missing.

Jonathan's bank refunded a small portion of his stolen funds, about $2,000. However, the international wire transfer, totaling $78,000, was gone—a financial gut punch he never imagined possible.

With no other options, he filed a police report and contacted the Federal Trade Commission. He learned that he had little hope of recovery, as cybercriminals who execute these scams generally operate out of foreign jurisdictions, making legal action nearly impossible.

Lessons Learned

Jonathan's ordeal became a painful lesson. He now double-checks every email claiming to be from his bank, verifying messages by calling official numbers instead of clicking links. He enables multi-factor authentication on all financial accounts, ensuring that a simple stolen password is not enough to access his funds.

For months after the scam, Jonathan felt ashamed. How had he, a tech-savvy professional, fallen for something so devious? But as he read more about phishing attacks, he realized just how sophisticated scammers had become. They prey on fear, urgency, and trust, exploiting even the most cautious individuals.

Jonathan eventually rebuilt his savings, but the emotional toll lingered. The loss of capital did not represent the most significant loss. The betrayal of trust affected him in a much more profound way. In an era of rampant digital deception, he learned that constant vigilance is the only actual safeguard against those seeking to exploit

the gullible.

His final takeaway? If something feels urgent, pause. If something sounds too good to be true, it probably is. And most importantly, verify everything.

The Voice of Experience Board has decided to publish a "scam of the month." The editors want to solicit examples of scams from the membership. If you have been exposed to a scam personally or made aware of one, please write it up for us and send it to Jeffrey Allen at jallenlawtek@aol.com. This will be a continuing column, so please keep this at the top of your pile of work in case you encounter a scam. If you want credit for it, be sure to let us know. Please let us know if you want it to remain anonymous, and we will not disclose your identity. We want the pieces to be 500-750 words in Word format. If you have questions, email Jeffrey Allen at the email address above.

Author

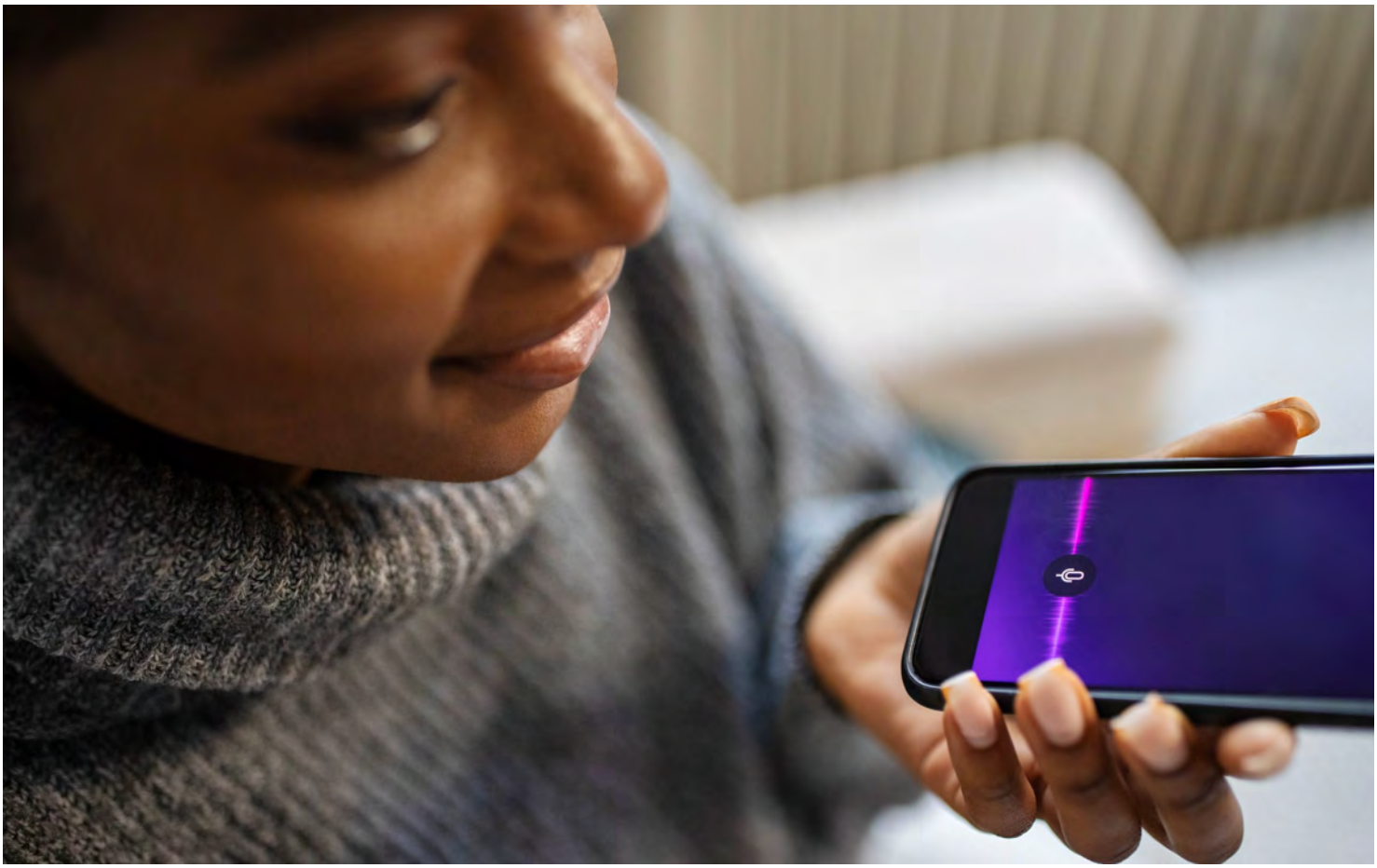
The Rise of the AI-Cloned Voice Scam

Jeffrey M Allen

Sep 10, 2025 5 min read

Summary

- AI technology can clone voices, making scams more convincing and emotionally manipul
- Victims suffer significant financial losses and emotional trauma due to sophisticated AI-enhanced voice-cloning scams.
- Establishing verification protocols and raising public awareness are crucial in defending a AI-enabled scams.



Luis Alvarez via G

Jump to:

Introduction →

The Scam in Action →

AI's Role in the Scam →

The Damages: Financial, Emotional, and Societal →

Avoiding the Trap: Targeted Defense Strategies →

Conclusion →

Introduction

In an age where artificial intelligence can compose symphonies, draft pleadings, and even simulate human emotion, it's easy to marvel at the power of emerging technologies. But any powerful tool can be misused. Sometimes, residents of the dark side use Artificial Intelligence (AI) with chilling precision. One such example unfolded recently in Florida, where a scammer manipulated a woman using a scam so sophisticated and personal that it felt like something out of a dystopian thriller. Except it was all too real.

In this instance, criminals used AI to clone the voice of a woman's daughter, employing it to create a sense of crisis so convincing that it caused a substantial financial loss and lasting emotional trauma. As these attacks proliferate, legal professionals must understand how AI-enabled scams work, how they're regulated, and how to advise clients (and protect themselves).

The Scam in Action

In July 2025, Sharon Brightwell of Dover, Florida, received a call that no parent wants to hear. Her "daughter," crying and distraught, claimed she had been in a car accident, had lost her unborn child, and was in legal trouble. The voice pleaded for immediate financial help to pay for legal representation and to prevent criminal charges.

Overwhelmed by emotion and the apparent need for immediate action (urgency), Brightwell sent $15,000 in cash to a courier, believing it would help her daughter avoid jail. Only after speaking to her real daughter did she realize the deception. She did not hear her daughter's voice on the phone; she listened to an imitation of her daughter's voice artificially generated using AI voice cloning technology.

Sharon rushed to help. During the day, she wired $15,000 to scammers who convinced her that her daughter was in legal peril and that immediate action was needed. She later told *People Magazine* she had "never been so afraid" in her life and "felt like I was in a nightmare."

This scam reflects a growing trend of AI-generated impersonation attacks that target vulnerable individuals by exploiting emotional ties.

AI's Role in the Scam

What makes this story so disturbing is not just the emotional manipulation, it's how stunningly convincing the scam was. Unlike older phone scams that relied on vague impersonations or poor connections, this one was high-tech, excellent, and targeted.

The scammers used voice-cloning technology to replicate her daughter's voice, likely harvesting snippets of audio from social media or public videos. With a few seconds of real audio, tools powered by deep learning models like *ElevenLabs*, *Resemble.AI,* or open-source frameworks such as *Descript Overdub* can create eerily accurate voice replicas. Some of these tools are so advanced that they not only mimic tone and inflection but can simulate emotion.

Academic researchers and security analysts have warned of the growing use of this technology in fraudulent schemes. Dr. John H. Griffin, an AI researcher at the University of Wisconsin, noted in a 2024 campus bulletin that AI-powered scams were becoming more convincing, particularly those involving cloned voices:

"The emotional realism of a cloned voice removes the mental barrier to skepticism. If it sounds like your loved one, your rational defenses tend to shut down." (IT.wisc.edu, 2024).

In this context, AI is no longer a passive tool—it becomes an active participant in crime, enabling deception at a level previously impossible.

The Damages: Financial, Emotional, and Societal

The financial damage in Sharon Brightwell's case—$15,000—is significant, but the emotional toll may be even greater. Victims report feelings of betrayal, fear, and helplessness. There is also a sense of shame, particularly among older victims who feel they should have known better.

Not an Isolated Incident. Unfortunately, Sharon's story is not an isolated case. AI-enhanced scams are on the rise, and their impact is already staggering.

- Global losses from deepfake-enabled fraud reached over $200 million in Q1

2025 alone.

- In early 2024, a UK-based energy firm lost €220,000 after an employee received a phone call from someone who sounded exactly like the company's CEO. The deepfake audio directed the employee to send funds to a "trusted supplier," and because the voice passed all the mental credibility checks, the funds were transferred without question (Forbes).

- In another incident reported by *The Financial News London*, scammers used deepfake audio and video clips of well-known finance executives to promote bogus investment schemes. In these videos, viewers saw and heard what appeared to be legitimate endorsements—except none of it was real (FN London, 2024).

- **Financial sector vulnerability**: A single incident at engineering firm Arup reportedly involved a $25 million loss due to deepfake deception.

- **Widespread targeting**: In the UK's financial "City", scams used AI videos and voices of prominent figures to push bogus investment schemes, with fraud attempts up by over 2,100 % in three years.

- **Scale of AI-based phishing**: In 2024, audio deepfakes were used to fool businesses and individuals, even tricking an energy firm's bank manager into sending €220,000 via an impersonated CEO's voice.

Avoiding the Trap: Targeted Defense Strategies

Although they utilize advanced technology, the scams often rely on the same basic principles as traditional fraud: urgency, emotional pressure, secrecy, and limited time for decision-making. Adding AI to the mix, however, amplifies the effect of the emotional manipulation.

Here are some practical ways to defend yourself:

1. **Establish Verification Protocols.** Use pre-agreed code words or phrases, not

easily guessed, to confirm identity before sending money, even when voices sound familiar.

2 **Resist Pressure to Act Immediately.** Scammers often demand secrecy and urgency. Lawyers and clients should be trained to pause, verify independently, and speak to the actual person before responding.

3 **Don't act under pressure or emotional distress.** Verify claims through trusted, independent means (e.g., call the actual family member or lawyer using previously known contacts). Be especially wary when requests involve secrecy or urgency.

4 **Raise Public Awareness.** Share real-life examples to educate others—families, social groups—on AI risks and tactics employed.

5 **Protect Personal Voice Data.** Limit the availability of voice recordings on public platforms. Lawyers should be especially cautious with podcasts, videos, or social media content that includes long, uninterrupted speech samples.

6 **Train Institutions and Individuals.** Include AI-cloning scenarios in fraud training. Simulations can help users recognize red flags like unexpected emotional pleas, unfamiliar voices, or inconsistent details.

7 **Use Two-Factor Authentication for Financial Transactions.** Even if a request seems to come from a known individual, a second layer of verification can prevent misdirected funds.

8 **Deploy Detection Tools.** Organizations can invest in AI-powered detection—but beware: tools aren't foolproof, and human judgment often still outperforms detection software. Norton's new *Deepfake Protection*, available on mobile, can flag possible deepfake media in YouTube clips, offering a helpful precaution.

9 **Stay Updated on Scam Tactics.** The FBI and FTC both regularly publish scam alerts. Europol has also issued specific guidance to law enforcement about the risks of deepfake crimes (Europol Report).

10 Reporting.

- Victims should file reports with the FTC at reportfraud.ftc.gov and notify local law enforcement. Quick action may assist in asset recovery or investigation.
- Regulatory bodies like the **FTC**, **FCC**, and **Europol** are increasingly recognizing AI fraud risks. Enforcement and clearer legal consequences can deter scammers.
- Create clear avenues for victims to report AI-based scams swiftly.

Conclusion

Using AI to clone voices and impersonate loved ones is not science fiction; it is a present and growing threat. As illustrated by the Dover, Florida scam, artificial intelligence has enabled bad actors to breach one of the most fundamental human defenses: trust.

This Dover audio-deepfake scam demonstrates how AI can weaponize trust, fear, and familiarity to inflict real harm. With rising global losses,from individuals to corporations, the imperative is clear: combine awareness, verification protocols, detection tools, and institutional readiness to confront this evolving threat.

Lawyers must not only stay informed but also play an active role in educating clients, advising them on safeguards, and pushing for clear regulatory standards. AI may offer extraordinary promise, but without proper oversight and vigilance, it can also become a devastating weapon in the hands of scammers.

Author



Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-september/ai-cloned-voice-scam/?utm_source=chatgpt.com

The “Free Genetic Test” Medicare Scam

Jeffrey M Allen

Jan 16, 2026 5 min read

Summary

- Scammers exploit seniors by offering “free” genetic tests, using Medicare coverage as bait to steal identities and bill for unnecessary services.
- Victims face financial, medical, and long-term identity risks—even if they don’t pay directly—due to fraudulent claims and incomplete or misleading test results.
- Only trust tests ordered by your own doctor, guard your Medicare number, and report suspicious offers or charges immediately.



R.Tsubin via Getty Images

Jump to:

A Florida Senior, a Community Event, and an Offer That Looked Legitimate →

What Mary Didn’t Know: Her Doctor Never Ordered The Test →

How the Scam Really Works (and Why It’s So Effective) →

The Bigger Picture: A Multi-Billion-Dollar Fraud Industry →

What This Scam Actually Cost Mary →

What Mary Could Have Done — And What Seniors Should Do Today →

A Final Word of Caution →

Medicare scams have a way of shapeshifting. Just when seniors get wise to fraudulent “back brace” offers or sham home-health services, scammers reinvent the pitch. Lately, one of the most successful schemes has been the “free genetic test” scam — a slick, high-tech con that preys on older adults’ trust in medical innovation.

Let me tell you about “Mary,” a woman living in a Florida retirement community, who found herself caught in one of these schemes. Her case is real, well-documented, and unfortunately far from unique. But it offers a clear look at how the scam works and what seniors (and others) can do to stay safe.

A Florida Senior, a Community Event, and an Offer That Looked Legitimate

In 2019, “Mary” attended a community gathering and came across a booth advertising **“Free DNA testing for cancer risk — fully covered by Medicare.”** She wasn’t looking for genetic testing, and she had no personal history of cancer, but the offer seemed harmless enough. No needles, no cost, just a cheek swab. The person at the booth even said a doctor had “approved” it for her.

Why would she doubt it? Conventional wisdom informs us that early detection improves the odds of survival. The idea that Medicare covers cutting-edge genetics appeals to many seniors. So she agreed. She swabbed her cheek. She handed over her Medicare number. The whole interaction took just a few minutes.

And that’s when the trouble started.

What Mary Didn’t Know: Her Doctor Never Ordered The Test

Months later, a letter from Medicare arrived. The laboratory that took her sample had billed Medicare $21,000. Medicare paid roughly $8,000 of it — taxpayer money gone, just like that.

Confused, Mary eventually spoke with a licensed genetic counselor at Hartford HealthCare who reviewed the test she received. What he found was alarming:

- The test never should have been performed — she didn’t qualify for Medicare-covered genetic testing.
- The test was incomplete, missing an entire category of standard analysis.
- The lab charged an outrageous amount, far above the $1,500–$3,200 price range of reputable genetic tests.

Mary had unknowingly become one of thousands of seniors targeted in a nationwide fraud wave using the same pitch.

How the Scam Really Works (and Why It’s So Effective)

The genius — and the danger — of this scam is that it looks medical. It involves doctors’ names, lab equipment, genetic terminology, and references to Medicare coverage. And that it costs them nothing, because Medicare will cover the expense. For many older adults, this “medical theater” lowers their guard.

Here’s the playbook scammers use:

1. The Approach: “Medicare Covers This!”

Scammers show up at:

- Senior centers
- Health fairs
- Retirement community events
- Art festivals
- Parking lots
- Or they call on the phone, claiming to be from Medicare or a doctor’s office

They promise a **free**, no-risk genetic test. The word “free” is especially effective on older adults who have navigated Medicare’s sometimes confusing cost-sharing rules.

2. The Fake Doctor Order

Scam labs routinely pay telemedicine doctors to rubber-stamp orders for seniors they’ve never treated — sometimes with no interaction. In legitimate medicine, a treating physician who knows the patient must order any genetic test. But scammers sidestep this by paying doctors on the side.

3. The Goal: Your Medicare Number

To the scammers, the cheek swab is almost incidental. They want the beneficiary’s Medicare number, which allows them to:

- Bill Medicare for unnecessary genetic tests
- Bill Medicare for services not provided
- Re-use or resell the Medicare identity

Think of it as health-care identity theft.

4. The Big Payout

Once they have a Medicare number and a bogus doctor’s order, labs submit massive claims — often $10,000 to $30,000 per test. Mary’s case — $21,000 billed, $8,000 paid — is unfortunately typical.

Fortunately for Mary, Medicare did not deny the claim, and she did not get billed for the test or even the

difference between the amount billed and paid. While Mary did not have to deal with claims against her for exorbitant fees denied by Medicare, many victims did. When Medicare denies the claim, the beneficiary remains on the hook.

The Bigger Picture: A Multi-Billion-Dollar Fraud Industry

Mary’s story fits into a much larger pattern. In 2019, the Department of Justice announced Operation Double Helix, charging 35 people connected to $2.1 billion in fraudulent genetic testing claims.

This wasn’t a ragtag group of small-time scammers. It included:

- Telemedicine executives
- Laboratory owners
- Marketing network operators

Their business model depended on the mass-harvesting of Medicare numbers from seniors through exactly the kind of pitch Mary encountered.

And it’s part of an even broader problem: Medicare loses an estimated $60 billion every year to fraud, errors, and abuse. A single unnecessary genetic test may seem minor, but scale it up nationwide and you get a billion-dollar crisis.

What This Scam Actually Cost Mary

Mary didn’t lose money directly — but that doesn’t mean she avoided harm.

1. Financial Exposure

She was lucky; Medicare paid the claim. Many beneficiaries get hit with multi-thousand-dollar bills when Medicare later decides the test wasn’t medically necessary.

2. Medical Risks

Her test was incomplete. That means:

- A false-normal result could have led her to skip preventive care.
- A false-positive could have triggered unnecessary anxiety or medical visits.
- Her medical record may now contain misleading genetic information.

3. Long-Term Identity Exposure

Once scammers have Mary’s Medicare number, they can:

- Submit more fraudulent claims
- Sell her Medicare identity

- Cause inaccurate services to accumulate on her Medicare record

4. Systemic Harm

Every fraudulent claim drains resources from legitimate patient care. It’s not abstract — it increases costs for everyone and damages public trust in Medicare.

What Mary Could Have Done — And What Seniors Should Do Today

Looking back, Mary wishes she’d paused before agreeing to that “free” test. Here are the key lessons she and others can learn:

1. Trust Your Own Doctor — Not a Booth at a Health Fair

Medicare will only cover genetic tests ordered by a treating physician. If someone claims otherwise, that’s a red flag.

2. Guard Your Medicare Number

Scammers treat Medicare numbers the same way identity thieves treat Social Security numbers. If someone pushes you to “verify” your Medicare ID, walk away.

3. Beware the Word “Free”

If someone emphasizes that Medicare “approved” or “covers” a test for everyone, that’s usually a lie. Medicare has specific genetic testing rules — and they do not include random screenings.

4. Check Your Medicare Summary Notice

Beneficiaries should always review their quarterly Medicare Summary Notice for suspicious lab tests or unfamiliar providers.

5. Report Suspected Fraud Immediately

Calling 1-800-MEDICARE, contacting Senior Medicare Patrol, or reporting to the HHS OIG Hotline can stop ongoing fraud and protect others.

A Final Word of Caution

Scams don’t always look like scams. Sometimes they look like modern medicine. Sometimes they look like prevention. Sometimes they come dressed as “free benefits.”

And that’s precisely why they work.

Mary’s experience serves as a reminder that seniors — and those who counsel them — need to stay alert. The merging of medicine, technology, and aggressive marketing has created a perfect storm of vulnerability, which scammers have glommed onto like sharks sensing blood in the water. With proper guidance and a healthy dose

Experience Experience April-May 2026

What Attorneys Need to Know About Age AI

Jeffrey M Allen and Ashley Hallene

Apr 29, 2026 10 min read

Summary

- ChatGPT helps lawyers think and write, and agentic AI acts. That shift from assistance to autonomous action fundamentally changes risk, supervision duties, and professional responsibility.
- GenAI errors stay on the page; agentic AI errors can cause real-world harm.
- Attorneys remain fully accountable for ethics, confidentiality, and outcomes, regardless c sophisticated or autonomous technology becomes.



iStock.cor

Jump to:

Introduction →

What Is ChatGPT/GenAI? →

What Is Agentic AI? →

Detailed Comparison →

Why the Distinction Matters →

What Each Tool Does Well →

What Neither Tool Does Reliably →

Risk: Similar Roots, Different Scale →

Risks and Ethical Considerations →

Client Confidentiality and AI Risks →

Economic Impact on Law Firms →

Regulatory Landscape and Compliance Challenges →

AI in Litigation Strategy and Risk Management →

Conclusion →

Introduction

Just When You Thought You Could Safely Take Your Head Out of the Sand...

Over the past few years, many lawyers have become at least casually familiar with Generative AI (GenAI), sometimes called ChatGPT (imprecisely). ChatGPT, a form of GenAI, has opened GenAI technology to many uses in and out of the legal profession. Because of ChatGPT's impact, many people use the term interchangeably with GenAI.

Some use GenAI regularly, growing increasingly comfortable with it as a partner or an assistant. Others experimented, shrugged (perhaps with disdain), and moved on. Still others saw it as interesting but not something they trusted with anything important. We consider all those reactions reasonable. Some looked at it as a high-tech form of Frankenstein, stuck their heads in the sand, and hoped it would go away. We don't see that as a reasonable approach, but to each their own...

We have come to accept artificial intelligence (AI) (some of us reluctantly), and it has planted itself in our lives and practices. It continues to grow and expand its scope of competence. Many of the sand people have started to emerge, thinking we have some reasonable grasp of AI now and acknowledging that it has come to stay.

But just when they thought they could safely emerge...

Now, a new term has entered the conversation: **Agentic AI**. GenAI raised issues of accuracy, ethics, confidentiality, and professional judgment. Agentic AI continues to

grapple with those problems and adds even more complex concerns.

What Is ChatGPT/GenAI?

A generative AI model developed by OpenAI, ChatGPT, reads prompts and produces human-like text or other media. Because of its ubiquitous presence, many began using the terms “GenAI” and “ChatGPT” interchangeably, much as “Kleenex” became the generic term for tissues.

It may prove helpful to think of GenAI as an advanced autocomplete system—impressive, helpful, and sometimes far too confident for its own good. In most consumer and professional deployments, GenAI operates reactively, responding to prompts rather than initiating actions on its own.

In our experience, GenAI can help attorneys draft contracts, summarize case law, generate marketing content, and translate documents. These tasks save time, reducing repetitive work. For example, an attorney can ask a GenAI application to summarize a 50-page case into a one-page brief. The tool delivers a readable summary in seconds.

GenAI, however, has limits. It cannot act autonomously, guarantee factual accuracy, or reliably provide legal advice. It may hallucinate facts or cite non-existent cases. GenAI has no internal moral compass. It does not perceive right from wrong as humans do. GenAI does not think the way humans do. It predicts language. When you ask a question or give it a task, it responds based on patterns it learned during training. Those responses can come across as impressively fluent, and they often prove helpful. They can also end up confidently wrong. GenAI also does not verify facts the way lawyers expect verification to work. It does not “look up” cases, unless connected to a tool designed to retrieve them, and even then, it may misinterpret what it finds. OpenAI has publicly acknowledged that large language models can hallucinate—producing statements that sound plausible but are completely false. That risk does not disappear just because the writing sounds authoritative.

From a lawyer’s perspective, GenAI works best as a language tool. It drafts, rewrites, summarizes, explains, and organizes information quickly. It can turn a rough idea into a polished paragraph, translate legal jargon into plain English, or condense a long document into something quickly readable.

What Is Agentic AI?

Agentic AI represents the next evolution of AI—yes, already, whether we feel ready for it or not. Agentic AI can act independently. Agentic AI can pursue predefined goals, plan intermediate steps, *and execute tasks* with minimal ongoing human intervention. Imagine an AI agent tasked with filing documents near a deadline, using outdated instructions copied from a prior matter. Or it misunderstands your instructions and sends confidential files to the wrong party—without waiting for your approval. You only discover the error after the damage has occurred.

Agentic AI behaves like a digital worker. It integrates with external tools, adapts to changing conditions, and completes multi-step workflows. Agentic AI can also learn from feedback and adjust its strategies on the fly. Agentic AI builds on the same language-model foundation as ChatGPT, but it adds something new: *the ability to plan, decide, and act across multiple steps without continuous human prompting*. This autonomy makes it a powerful assistant but also introduces new risks. For lawyers, this means that *errors no longer stay on the page. They can turn into actions*.

We like the idea of AI continuing to expand, but we are not quite ready to unleash the full power of Agentic AI on our practices. The concept of AI acting autonomously keeps us up at night. Yet, we know it has arrived and will continue to expand its impact across our practices and personal lives.

Detailed Comparison

While GenAI reacts, Agentic AI moves proactively. In our experience, this shift means lawyers must rethink how they supervise technology. GenAI focuses on generating text and other media. Agentic AI *executes tasks*. GenAI has limited integration and static learning. Agentic AI can dynamically adjust its actions within a task and connect to multiple systems. These differences matter because they affect risk, governance, and ethical responsibilities. Another key difference lies in accountability. With GenAI, the attorney controls each interaction (although sometimes poorly). Agentic AI can act without explicit approval, raising questions about liability. Firms must design workflows that include checkpoints and human review to mitigate these risks. Rethinking workflows only represents a preliminary step. Agentic AI requires that we re-examine

our entire risk-management approach.

Why the Distinction Matters

Lawyers have always relied on tools that increase efficiency. Dictation machines, word processors, legal research databases, and document assembly software all changed how legal work gets done. Agentic AI crosses a line that earlier tools did not.

When a word processor formats something incorrectly, you notice and fix it. When a research database returns irrelevant cases, you refine the search. When you discover that an agentic system makes a mistake, it may already have done something with consequences—sent information to the wrong person, filed the wrong document, updated a system incorrectly, or taken other actions on its own. That difference changes how lawyers must think about supervision, accountability, and risk management of AI. That supervisory role brings with it obligations that resemble those associated with junior staff, outsourced services, or automated filing systems—but with one critical twist: agentic systems operate faster, at greater scale, and with fewer natural pauses than those of us with natural intelligence. What happens when Agentic AI acts faster than we can supervise?

Remember, when something goes wrong, the responsibility does not rest with the AI; it rests with the lawyer or the firm that deployed it.

What Each Tool Does Well

GenAI shines at tasks involving language. It can help lawyers brainstorm arguments, draft correspondence, summarize complex material, and explain legal concepts in ways clients can understand. It works particularly well as a conversational partner, allowing exploration without commitment. We confess to having many conversations with our AI (not all of which were pleasant).

Agentic AI excels at process-oriented work. It handles multi-step workflows that follow defined rules. It can move information from one place to another, monitor systems over time, and coordinate tasks that would otherwise require repeated manual intervention.

When used appropriately, agentic systems can reduce administrative burdens. Misused, they can magnify small mistakes into significant problems—faster than you can say “algorithm.”

What Neither Tool Does Reliably

Neither ChatGPT nor Agentic AI understands professional responsibility as we do. They don’t recognize privilege instinctively. They can’t grasp the reputational consequences of a poorly timed email or an ill-considered filing. They do not exercise judgment about what they *should not* do. They also do not provide much support for accountability.

Agentic systems: they often require access to credentials, tokens, and permissions to function. Once granted, we must manage that access carefully. A system that can read email can often send email. A system that can retrieve documents may also attach them. Every permission expands the potential impact of an error or misuse. Many (most) firms have not considered, let alone properly prepared to handle, that level of supervision. It makes us nervous to think about the consequences.

Risk: Similar Roots, Different Scale

ChatGPT and agentic AI share certain core risks. Both can hallucinate. Both can mishandle sensitive information if used carelessly. Both can perform “confidently,” even when relying on hallucinated “facts.” The AI’s strong presentation, combined with a natural human indolence, encourages our over-reliance on AI, especially when the output looks polished and professional.

Agentic AI adds a new layer of risk by coupling GenAI’s weaknesses with autonomy. A hallucinated fact in a draft memo can prove embarrassing. A hallucination instruction that triggers an automated action poses a potentially far more serious operational danger.

Agentic AI, like GenAi, can work for good or for evil. Consider the social engineering dimension. GenAI can generate convincing, but false messages. Agentic AI systems can generate *and send* compelling, but false, messages at scale. That capability creates obvious concerns about fraud, impersonation, and manipulation—concerns serious

enough that OpenAI and other providers have issued specific policy guidance about agent-based misuse.

As if that lacked sufficiency, Agentic AI complicates audits and defensibility. Lawyers need the ability to explain what happened, why it happened, and who approved of it. That requires logging, transparency, and human checkpoints—features we must learn to design into these systems from the beginning.

Risks and Ethical Considerations

GenAI creates risks around data privacy, misinformation, and overreliance. Depending on the platform and configuration, *GenAI tools may retain and use user-submitted dat***a**, particularly in consumer (or in "free") versions. Many enterprise and professional deployments now allow data-use opt-outs or contractual prohibitions on training. Always look for an opt-out option and take it, but do not rely on that. Anonymize all information you upload to AI entities, and encrypt the data you store with password protection to protect confidentiality in the event of inadvertent mistransmission.

GenAI can fabricate citations or misinterpret statutes, creating ethical violations and malpractice risks if unchecked.

Agentic AI carries all the risks of GenAI and introduces autonomy risks. When a system acts without direct oversight, unintended consequences can multiply. Security vulnerabilities, such as prompt injection attacks, can compromise workflows. Compliance becomes more difficult due to the complexity of auditing autonomous decisions. Ethically, attorneys face accountability questions. Who is responsible if an AI agent makes a mistake? ABA Model Rule 1.1 requires lawyers to maintain technological competence, which now includes understanding AI in its various permutations.

We've found that technical errors do not represent the most significant risk—it's the temptation to trust a system that sounds authoritative but may be confidently wrong.

Client Confidentiality and AI Risks

Client confidentiality remains a cornerstone of legal ethics. AI tools pose a challenge to

this principle because they process sensitive data and may misuse it. Agentic AI compounds the risk by accessing multiple systems and autonomously transmitting data.

Economic Impact on Law Firms

AI changes the economics of legal practice. GenAI reduces drafting time. Agentic AI automates administrative tasks, cutting overhead costs. These efficiencies can increase profitability, but they can also disrupt traditional billing models. Flat fees and subscription services may ultimately replace hourly billing to address these issues.

Technology investments require capital. Smaller firms may struggle to afford advanced AI systems. This gap could widen inequality in legal services, creating competitive pressure.

Regulatory Landscape and Compliance Challenges

Regulators worldwide continue to debate AI governance. The EU's AI Act imposes strict requirements on high-risk AI systems. U.S. states explore transparency and accountability rules. At some point, the federal government may (and should) act in this area. Attorneys must monitor these developments because they affect client counseling and firm operations. Compliance failures can lead to sanctions, reputational harm, economic damages, and malpractice claims.

AI in Litigation Strategy and Risk Management

Attorneys can use GenAI to draft persuasive arguments, summarize case law, and identify trends in judicial decisions. Agentic AI can analyze large bodies of prior rulings to identify statistical patterns and correlations that may inform strategy. Imagine an AI agent that reviews discovery documents, flags privileged material, and suggests deposition questions—all without constant supervision. This level of autonomy saves time but introduces additional risk. Risk management becomes essential. Attorneys must maintain ultimate responsibility for strategic decisions, ensuring compliance with ethical standards and procedural rules.

Attorneys must remain the final decision-makers, no matter how advanced the technology becomes.

Conclusion

For most attorneys today, the safest and most productive use of AI remains **assistive, not autonomous**. ChatGPT and similar tools can provide real value when used as drafting aids, explanatory tools, and brainstorming partners—so long as lawyers verify the output and retain control. Agentic AI requires a more cautious approach. While potentially valuable for tightly controlled internal workflows, particularly where actions remain reversible and subject to review, it should not operate unsupervised in client-facing or high-stakes contexts. Those safeguards include limited permissions, approval gates before taking external actions, clear audit logs, and an easy way to stop or override the system when something looks wrong. We need to treat agentic AI less like software and more like a junior staff member who never sleeps and never improvises wisely.

GenAI and agentic AI do not compete; neither serves as a replacement for the other. They present different tools built on the same foundation, each designed for a different role. These impressive technologies come with risks. We can manage those risks if attorneys understand what these systems do, where they fall short, and how and why autonomy changes everything.

We're genuinely excited by what AI can do for us personally and professionally. But every time we see a new tool, we remember the lessons learned from early missteps. Our advice? Treat these systems as helpful partners but never let go of the steering wheel. The best outcomes result from technology and human judgment working side by side.

Authors



Jeffrey M Allen

Graves & Allen

Jeffrey Allen is a principal in the law firm of Graves & Allen, in Oakland, California. He runs a general practice that, since 1973, has emphasized real estate and business transactions, receiverships and related...



Ashley Hallene

Ashley Hallene is an Attorney and Land Acquisition Specialist with Demeter Land Development. She is based in Houston, Texas. She is the co-author of several books, including Technology Tips for Seniors Volume 2.0 (2018),...

Published by the American Bar Association ©2026. Reproduced with permission. All rights reserved. This information or any portion thereof may not be copied or disseminated in any form or by any means or stored in an electronic database or retrieval system without the express written consent of the American Bar Association.

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/experience/2026-april-may/what-attorneys-need-know-about-agentic-ai/?utm_source=chatgpt.com

What Deepfake Scams Teach Us About AI and Fraud

Jeffrey M Allen

Jun 10, 2025 4 min read

Summary

- Deepfake technology can create highly convincing scams, even impersonating celebrities.
- Lack of social media familiarity can increase vulnerability to sophisticated fraud.
- AI-generated images and videos are used to manipulate victims into transferring large sums of money.



Tero Vesalainen via Getty Images

Jump to:

How the Scam Unfolded →

It Sounds Wild—But It's the New Reality →

What Makes This a Legal Issue? Plenty. →

How Can Lawyers Help? Start with Awareness →

What Should Lawmakers Do? →

The Bottom Line: It's Not Just Brad Pitt →

We all think we won't fall for a scam. But when scammers start using artificial intelligence, fake photos, and voice clones to impersonate Hollywood royalty? Suddenly, the game changes.

That's precisely what happened in a real case involving a French woman and a scammer posing as Brad Pitt. Yes, *that* Brad Pitt. No, not just a catfishing attempt gone wrong, a full-blown, AI-powered, deepfake-fueled fraud that cost the victim nearly a million dollars. In the aftermath, we must wonder what legal tools we have to fight this new breed of deception.

How the Scam Unfolded

In 2023, someone claiming to be Brad Pitt's mother contacted Anne, a recently divorced interior designer living in France, on Instagram. "Brad's" mom told her that Brad "needed a woman just like her." Shortly after, she began an online relationship with someone impersonating the actor. Despite initial doubts, Anne explained that her lack of familiarity with social media left her vulnerable to manipulation. This wasn't someone casually browsing dating sites or looking for trouble. One day, she got a message from someone claiming to be Brad Pitt's *mother*. That strange introduction quickly turned into direct messages from "Brad" himself.

Over the next 18 months, the scammer drew Anne into what she believed was a private, emotionally supportive

friendship with the actor. Detailed and personal messages helped sell the scam. The images? Convincing. Some included "Brad," holding up signs with her name. Others showed him in casual settings, just chatting about life. Ultimately, they turned into requests.

A film project, a medical issue (kidney cancer), and an asset freeze in connection with his divorce from Angelina Jolie provided the background and set the stage. Each crisis came with just enough documentation, fake contracts, fake invoices, even screenshots of bank accounts to feel real. The scammers used AI-generated images and videos to create a convincing illusion. And so, little by little, Anne sent money. Anne transferred funds to cover customs fees for supposed gifts and even provided money for fake medical treatments. By the time it ended, she had sent about €830,000 (roughly $900,000 USD).

When images of the real Brad Pitt with his girlfriend, Ines de Ramon, surfaced in June 2024, Anne began to question the relationship. Eventually, the scammers' demands for more money under the guise of "*Special FBI Agent John Smith*" prompted her to contact the police.

It Sounds Wild—But It's the New Reality

It's easy to read this story and think, "That could never happen to me." But this wasn't some fly-by-night phishing email with broken English. The scammers used cutting-edge AI tools to generate images, videos, and even voice messages that looked and sounded like Brad Pitt. They played the long game, built trust, and targeted her at a vulnerable moment.

And here's the scary part: if it can happen to someone like Anne, it can happen to anyone. That includes your clients. It could even include *you*.

What Makes This a Legal Issue? Plenty.

While the headlines focused on the celebrity angle, this scam raises big legal questions, many of which don't yet have clear answers.

1. Deepfake Impersonation Isn't Just Creepy—It's Criminal

The scam is based on identity theft. However, most existing laws were written long before AI could convincingly replicate someone's face and voice. We'll need legal updates fast to deal with synthetic media being used to commit fraud or impersonate real people.

2. Fake Legal Documents Are Getting More Convincing

The scammers didn't stop at fake photos. They also fabricated legal agreements, medical bills, and even production contracts. These weren't crude forgeries; they were polished, formatted, and plausible enough to fool someone with a strong head on their shoulders. That raises questions about document authentication, digital signatures, and due diligence in a world where seeing no longer equates to believing.

3. Jurisdiction Is a Nightmare

The scam started on Instagram. The victim resided in France. The fraudsters could have operated from anywhere, Paris, London, Newark, Los Angeles. Pick a city, any city. Tracking these criminals, let alone prosecuting them, creates its own nightmare of international law, financial secrecy, and digital anonymity.

4. Emotional Manipulation Is a Legal Harm, Too

Anne didn't just lose money. The scam left her emotionally devastated. Most fraud statutes focus on financial loss, not the trauma of manipulation by what amounts to a synthetic relationship. As these scams grow more personal, the law may need to account for emotional abuse in civil claims.

How Can Lawyers Help? Start with Awareness

Whether you work in elder law, family law, estate planning, or general civil practice, you've probably encountered lonely, grieving, or emotionally raw clients. The very people scammers like to target.

Attorneys can protect clients (and themselves) by:

- **Spotting the red flags.** Does the story sound dramatic, urgent, or secretive? That's a clue.
- **Verifying everything.** Real celebrities don't DM strangers asking for cash. If a story seems off, it probably is.
- **Watching for payment via crypto or wire transfer.** Once it's gone, it's almost impossible to recover.
- **Encouraging clients to slow down.** Scammers rely on urgency. A second opinion can stop a scam from progressing.

What Should Lawmakers Do?

There's no silver bullet here, but the legal system should adapt.

- **Modernize fraud and impersonation laws** to include AI-generated deepfakes and synthetic media explicitly.
- **Increase platform accountability.** Social media and messaging platforms should be required to detect and remove known scams more quickly.
- **Encourage cross-border enforcement agreements** to track international fraud rings more efficiently.

The Bottom Line: It's Not Just Brad Pitt

Today it's Brad Pitt. Tomorrow it could be someone impersonating a celebrity chef, a sports figure, or, more concerning, a lawyer, judge, or client.

AI doesn't just change how we do business. It changes how people commit crimes, how victims suffer, and how the law needs to respond. The tools we use to build trust—photos, documents, conversations—can now be mimicked by machines. That means trust itself has to be earned a little differently.

For legal professionals, that starts with being aware, staying skeptical, and helping clients navigate a world where *reality* may not be quite what it seems. Remember the lesson Anne learned: Scams really are the Pitts!

Author

What to Do in the First 24 Hours After a Data Breach

Ashley Hallene and Jeffrey M Allen

Apr 01, 2026 5 min read

Summary

- Lawyers must act fast to contain data breaches while meeting ethical duties regarding technology competence and client confidentiality within the first 24 hours.
- Centralized communication is critical to protect attorney-client privilege and prevent legal liability by using a single coordinator and secure, out-of-band channels.
- Legal professionals should engage experts, including digital forensics and cyber insurance, to analyze system access and identify mandatory breach notification requirements.



Rawlstock via Getty Imagess

Jump to:

Address Legal and Ethical Obligations →

Communicate with Care →

Work with Outside Experts →

Plan the Next Steps →

Tech Column

A data breach introduces immediate pressure and profound uncertainty. Whether you manage an in-house legal department, a sprawling law firm, or a solo practice, the stakes are doubly high. One must act with speed to contain the threat while simultaneously upholding rigid ethical and legal obligations. Although the most effective response begins long before an incident occurs through a formal response plan, the actions taken in the initial 24 hours determine whether a breach remains a manageable event or becomes a catastrophe.

Address Legal and Ethical Obligations

Once the initial technical chaos subsides, the legal professional must pivot to their specific duties. This phase requires a cool-headed assessment of what was lost and to whom it belonged.

Review Ethical Duties

Lawyers and legal departments carry professional responsibilities that persist even during a crisis. In most jurisdictions, these duties center on competence in technology, absolute confidentiality of client information, and honest communication.

If an attacker accessed or exposed confidential records, you must determine if notification is mandatory. Consider these factors:

- Was client information actually accessed or exfiltrated?
- Does the breach create a material risk of harm to the client?
- Is disclosure necessary for the client to protect their interests?

Evaluate Breach Notification Laws

Every U.S. state maintains data breach notification statutes (see overview from Masuda Funai). These laws typically trigger when specific personal information is exposed. Within the first day, your goal is not to complete a final legal memo but to identify which jurisdictions apply.

Initial Regulatory Checklist

- **Identify Data Types**: Did the breach include Social Security numbers, financial account numbers, or health information?
- **Identify the Victims**: For in-house teams, this includes employees and customers; for firms, it includes clients and opposing counsel.
- **Map Locations**: Identify the residency of affected individuals to determine which state laws apply.
- **Notify Authorities**: Check if the relevant states require notice to the attorney general or credit

reporting agencies.

As the legal team identifies its exposure and the specific data at risk, the focus must shift to how to handle this information internally. Maintaining control over the narrative is essential to prevent further legal complications or a loss of attorney-client privilege.

Communicate with Care

In the wake of a breach, uncontrolled talk creates confusion and legal liability. Information must flow through a single, designated coordinator (such as a general counsel or a managing partner) to ensure accuracy.

Establish the Chain of Command

Establishing a strict hierarchy for information flow prevents the distorted facts that often arise as data passes between departments. The coordinator serves as the ultimate clearinghouse for all data, ensuring that every internal update and external disclosure remains consistent. This centralization is a defensive tactic to protect the attorney-client privilege and work-product doctrine during the investigative phase.

Protocol for Internal Reporting

Define clear reporting lines for IT staff and third-party vendors. Rather than allowing tech teams to send broad status updates via email, require them to report directly to the coordinator. This practice minimizes the creation of “loose” documentation that could be misinterpreted during future discovery or regulatory audits.

Control Internal Communications

Instruct staff and colleagues to limit discussions to the designated response team. Speculation about the cause of the breach or the identity of the attacker often finds its way into discoverable documents. Use secure, out-of-band communication channels (such as encrypted messaging or personal phone lines) whenever possible and document every step of the response.

Secure Information Silos

Apply the principle of “least privilege” to the communication plan. Only individuals with a direct role in the recovery (typically a core group of leadership, IT, and legal) should be privy to the granular details of the investigation. By compartmentalizing information, the organization reduces the risk of an accidental leak by a well-meaning but uninformed employee or colleague.

Managing the Human Element

Acknowledge the stress levels of the team without compromising operational security. The coordinator should provide regular, high-level briefings to the broader staff to quell rumors, but these briefings must focus on the process of recovery rather than the specifics of the vulnerability. Instruct all personnel that “no comment” is the only acceptable response to any inquiry, referring all questions directly to the coordinator’s office.

Avoid Premature Public Statements

Facts are usually incomplete in the early hours. Making a public statement too soon risks spreading incorrect information or making unintended admissions. If the media, board members, or outside parties inquire, stick to

a concise script:

1. The organization is currently investigating a security incident.
2. We have engaged outside experts to assist.
3. We will provide updates as more information becomes available.

Effective communication provides a shield for the legal professional, but words alone cannot solve a technical crisis. To move from damage control to discovery, the practice or department must enlist specialized technical and financial support.

Work with Outside Experts

A legal professional should rarely handle a breach alone. Engaging specialized third parties provides the technical depth and insurance backing necessary for a full recovery.

Engage Digital Forensics

A digital forensics firm performs the “medical exam” of your network. They determine how the attacker entered, what systems they touched, and whether they are still hiding in your environment. For both in-house teams and firms, it is standard practice for counsel to retain these experts directly to help preserve legal privilege over their findings.

Contact Cyber Insurance

Cyber insurance policies are more than just a source of funds; they provide a prevetted stable of investigators, breach counsel, and notification vendors. Contact your carrier or the company's risk management department immediately. Waiting too long to report a potential incident can jeopardize your coverage, even if the breach later proves to be minor.

With the right experts engaged and the insurance carrier notified, the initial fog of the crisis begins to lift. This clarity allows the legal team to transition from reacting to the past to planning for the immediate future.

Plan the Next Steps

As the twenty-four-hour mark approaches, the focus shifts from frantic containment to structured recovery and compliance.

Develop a Seventy-Two-Hour Response Plan

By the end of the first day, establish a clear road map for the remainder of the week. This plan should include:

- Completing the forensic deep dive.
- Finalizing the list of parties requiring notification (clients, employees, or shareholders).
- Coordinating with law enforcement if the situation warrants it.
- Beginning the secure restoration of systems from backups.

Begin Immediate Remediation

Full restoration takes time, but you can take several defensive steps immediately to prevent a "second wave" of the attack.

Immediate Remediation Steps

- **Reset All Passwords**: Force a practice-wide or department-wide password change.
- **Enforce MFA**: Enable multifactor authentication on every entry point, especially email.
- **Patch Vulnerabilities**: Close the holes the attacker used to gain entry (see SecurityScorecard overview).
- **Update Monitoring**: Increase the sensitivity of your security alerts.

Securing the perimeter and drafting a timeline provides the foundation for long-term recovery. These early technical and strategic victories ensure the legal professional emerges from the first day with their reputation and the trust of their organization intact.

The first day of a breach is a test of preparation. By focusing on five priorities (containing the threat, preserving evidence, engaging experts, understanding the scope, and evaluating legal duties), an organization protects its clients, colleagues, and its reputation. Preparation makes these first 24 hours easier, turning a potential disaster into a disciplined professional response.

Authors