_____ PROGRAM MATERIALS
Program #36170
August 17, 2026

Scam I Am: Understanding and Fighting Cybercrime in the Age of AI

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

Celesq® AttorneysEd Center
www.celesq.com

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

Scam I Am

Understanding and Fighting Cybercrime in the Age of AI

Protecting Lawyers, Law Firms, and Clients from Modern Digital Threats

Presented By:
Jeffrey Allen • Ashley Hallene

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.

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.

PHISHING

RANSOMWARE

VOICE CLONING

DEEPFAKES

COURTHOUSE

CLIENT INFORMATION

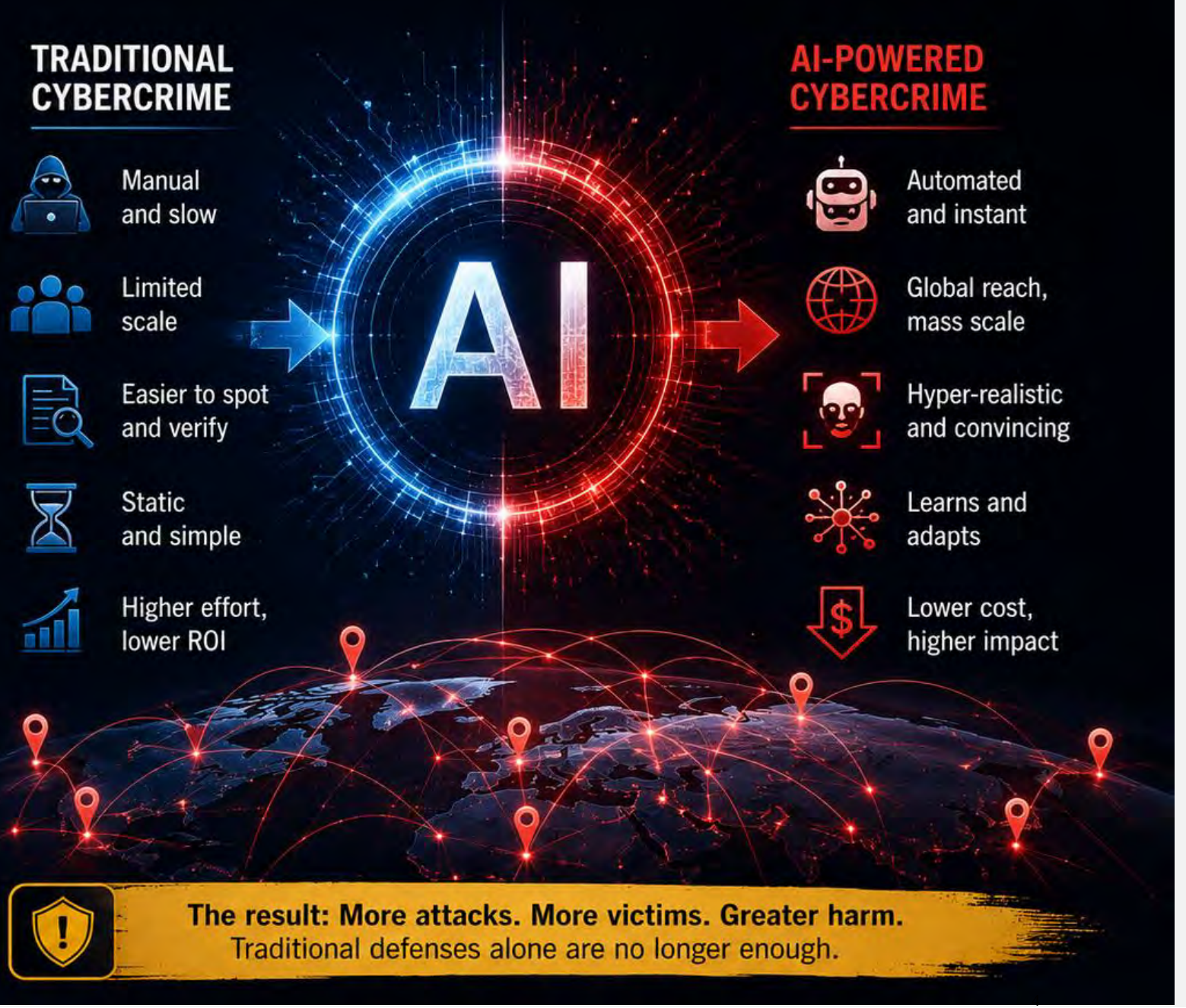
CLOUD SECURITY

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

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.



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		24/7 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.

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

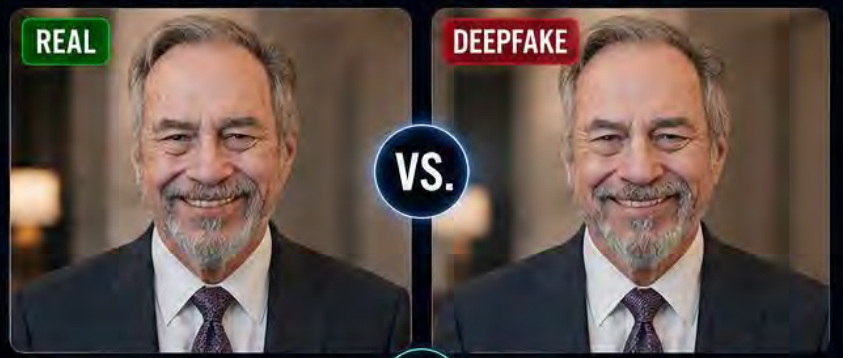
DATA IN
Photos, videos, and audio collected

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.

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.

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.

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.

AI-SUPPORTED PHISHING & SPEAR PHISHING

AI gives attackers the perfect intelligence, the perfect message, and perfect timing.

SOCIAL MEDIA
PUBLIC RECORDS
COMPANY INFO

AI

DATA BREACHES
FINANCIAL DATA
ONLINE ACTIVITY

TARGETED INTELLIGENCE

AI gathers data from social media, websites, breaches, and public records to build detailed victim profiles.

HYPER-PERSONALIZED MESSAGES

AI writes convincing emails and messages that match your tone, context, and relationships—made to bypass suspicion.

PERFECT TIMING

AI predicts when you're most likely to engage—during busy moments, deadlines, or high-stress situations.

MULTI-MODAL DECEPTION

AI-generated text, deepfakes, and cloned voices make scams look, sound, and feel completely legitimate.

AI-GENERATED EMAIL

From: Sarah Mitchell s.mitchell@acme.com
To: John.Doe@yourcompany.com
Subject: Urgent: Q4 Budget Update

Hi John,

As discussed in our meeting this morning, the Q4 budget file is attached. Please review and confirm by end of day.

Thanks,
Sarah

PDF Q4_Budget_Update.pdf
Review Document

AI-GENERATED TEXT

9:41

Michael (CEO)

Can you handle a quick favor for me? Need you to send a payment today. Different instruction than usual. I'll explain in a call.

https://secure-verify.com

9:41 AM

AI-CLONED VOICE

"John, it's me. I need you to wire $45,000 today. I'll send details to your email right now."

0:00 / 0:07

AI DEEPFAKE VIDEO

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.
- Be suspicious links (don't click) to see the resual oequests—Dspecially for unemey orrocata.
- Use multi-factor authentication (MFA) on all accounts.
- Report suspicious messages to your IT or security team.
- Stay informed. Attackers evolve—so should we.

IF IT LOOKS REAL, SOUNDS REAL, AND FEELS REAL—

IT'S PROBABLY AI.

Think before you click. Verify before you act. When in doubt, stop and check it out. One click can open the door to a world of damage.

AI SUPERCHARGES BUSINESS EMAIL COMPROMISE (BEC)

AI studies. AI impersonates. AI persuades. AI gets paid.

1. RESEARCH & PROFILE
AI scans websites, LinkedIn, news, and social media to build detailed profiles of people and companies.

2. IMPERSONATE WITH PRECISION
AI crafts highly believable emails that match the tone, style, and language of real executives.

3. MANIPULATE & PRESSURE
AI tailors messages to create urgency, authority, and trust—bypassing traditional red flags.

4. DIVERT FUNDS
AI directs payments to fake accounts or vendors. The money is gone—often within minutes.

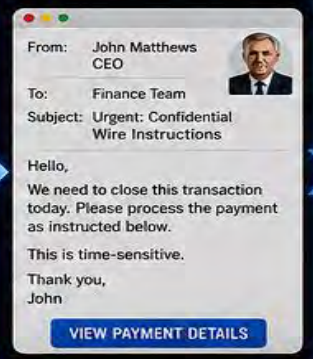
BEC LOSSES EXCEED $2.9 BILLION GLOBALLY (2023)
Average loss per incident: $137,000
– FBI IC3 2023 Report

HOW AN AI-POWERED BEC ATTACK UNFOLDS

1 STUDY
AI GATHERS INTELLIGENCE

AI collects data to understand the target, their role, relationships, and current priorities.

2 IMPERSONATE
AI CREATES THE LURE



AI mimics writing style, tone, and language to create a highly convincing executive email.

3 MANIPULATE
AI CREATES URGENCY

AI uses urgency, authority, and context to bypass skepticism and push for immediate action.

4 DIVERT FUNDS
AI CASHES OUT FAST

Payments are sent to fraudulent accounts. The money is moved and hard to recover.

HOW AI HAS MADE IT WORSE

AI-WRITTEN MESSAGES
AI crafts highly convincing, error-free emails that match the writing style and tone of the person being impersonated.

VOICE CLONING
AI clones voices of executives or colleagues for phone or video calls to verify requests.

DEEPFAKE TECHNOLOGY
AI creates realistic video of a trusted person asking for payments or confidential actions.

HYPER-PERSONALIZATION
AI analyzes data to tailor messages with specific projects, amounts, and details that increase urgency and trust.

AI TRANSLATION
AI instantly translates and localizes scams, enabling global targeting at scale.

HOW TO PROTECT YOURSELF

- Verify all payment requests through a known phone number or in-person.
- Be skeptical of urgency, secrecy, or unusual requests.
- Hover over links and check email addresses carefully.
- Confirm changes to payment instructions through a second communication channel.
- Limit sharing of sensitive informction on social media and publicly accessible sites.
- Train your team and test awareness regularly.

THE EMAIL LOOKS LEGIT. THE REQUEST LOOKS NORMAL. THE DAMAGE IS REAL.

VERIFY BEFORE YOU WIRE.

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.

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.

GRANDPARENT SCAMS: THE PANIC CALL

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.

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.

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.

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.

A

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.

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.

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.

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.

A

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.

VERIFY BEFORE YOU TRUST

Scammers are experts at pretending to be someone you know.
Independent verification **breaks the chain.**

HOW TO VERIFY ANY REQUEST

1 PAUSE
Don't rush. Take a moment to slow down and think.

QUESTION
Does this request make sense? Does it match the usual pattern?

3 VERIFY INDEPENDENTLY
Use a known, trusted contact method—call a number you already have.

4 CONFIRM DETAILS
Ask for details only you and the real person would know.

5 ACT WITH CONFIDENCE
Once verified, proceed with confidence. If not, don't.

VERIFY EVERY REQUEST

VERIFICATION BEST PRACTICES

- **Call back using a number you know is real.**
- Don't use numbers or links in unsolicited emails or texts.
- Verify requests for **money, account changes,** or **sensitive information.**
- Verify even if the request comes from a senior **leader** or client.
- When in doubt, verify. It's better to be safe than sorry.

WHAT YOU CAN DO

- **Pick up the phone.** A real conversation confirms identity.
- **Use known email addresses** and contact information.
- **Verify through another team** member if appropriate.
- **Follow your firm's policies** and escalation process.
- **Report suspicious requests** immediately.

TRUST IS EARNED. VERIFICATION IS YOUR PROTECTION.

Verify before you click. Verify before you call. Verify before you send.

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.

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.

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.

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.

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.

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.

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.

Stop Before You Click, Pay, or Reply

1. The Pause

PAUSE

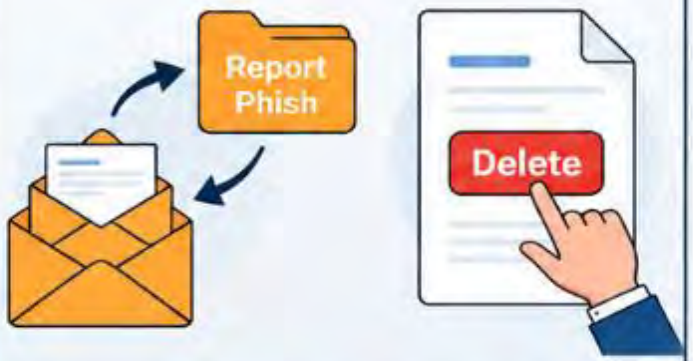
Pause.
Take 30 seconds to evaluate the request.

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

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

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

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**

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

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.

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

Find the Failure Point

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. ★

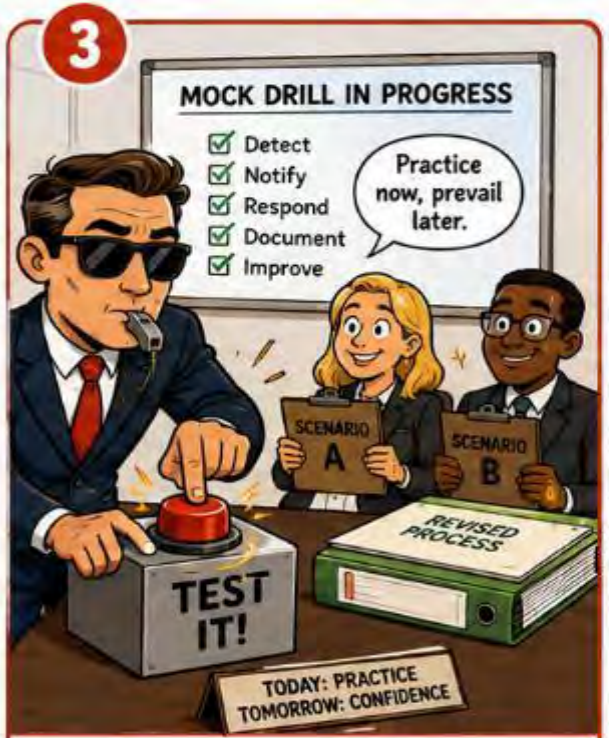
Turn the Incident Into Resilience

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.

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.

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.

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.

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.*

48

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.*

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.

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.

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.

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.*

Before you use it, prove it.

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.*

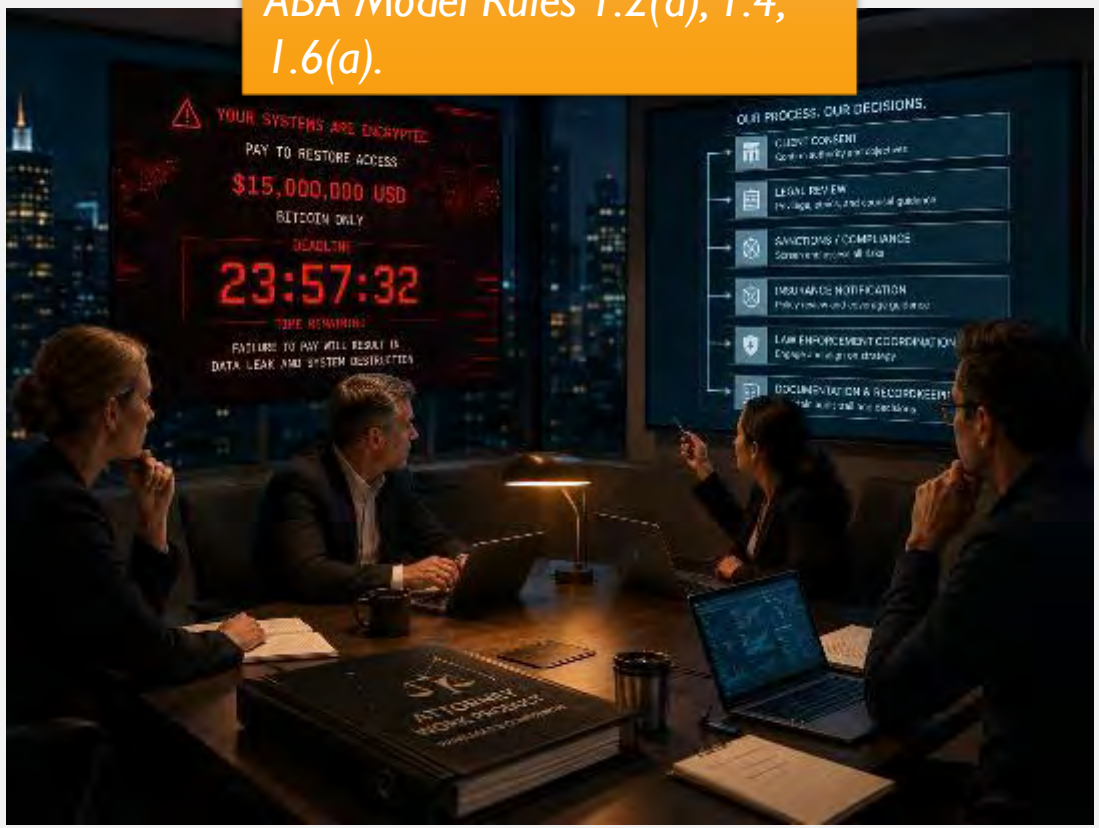
NEGOTIATING WITH CRIMINALS: A RANSOM DEMAND CREATES PRESSURE, NOT PERMISSION TO SKIP LEGAL JUDGMENT.

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).



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.*

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.

IF YOU HAVE QUESTIONS--

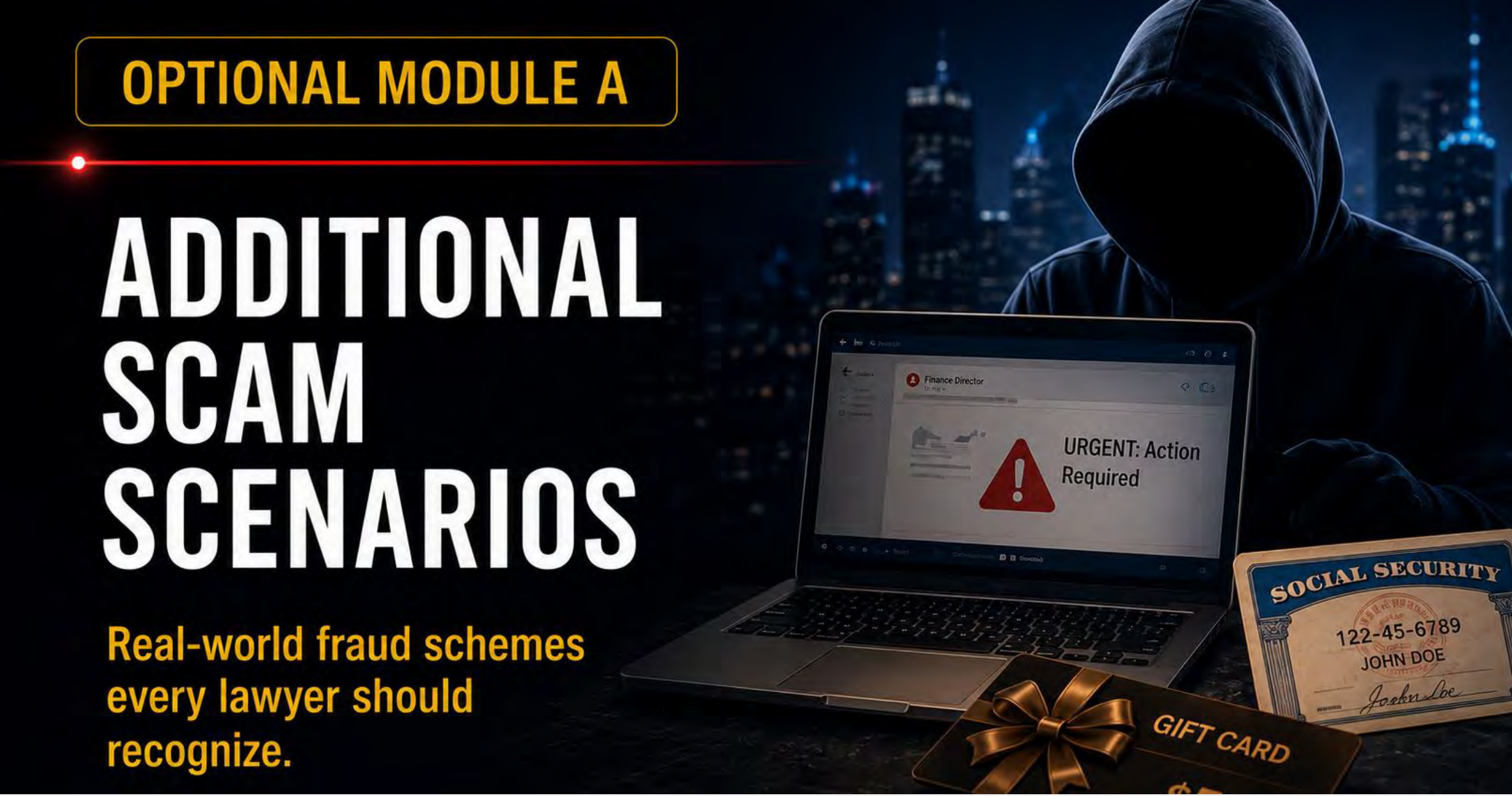
--We Have Answers

(But not necessarily to your questions).

OPTIONAL MODULE A

ADDITIONAL SCAM SCENARIOS

Real-world fraud schemes every lawyer should recognize.



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.

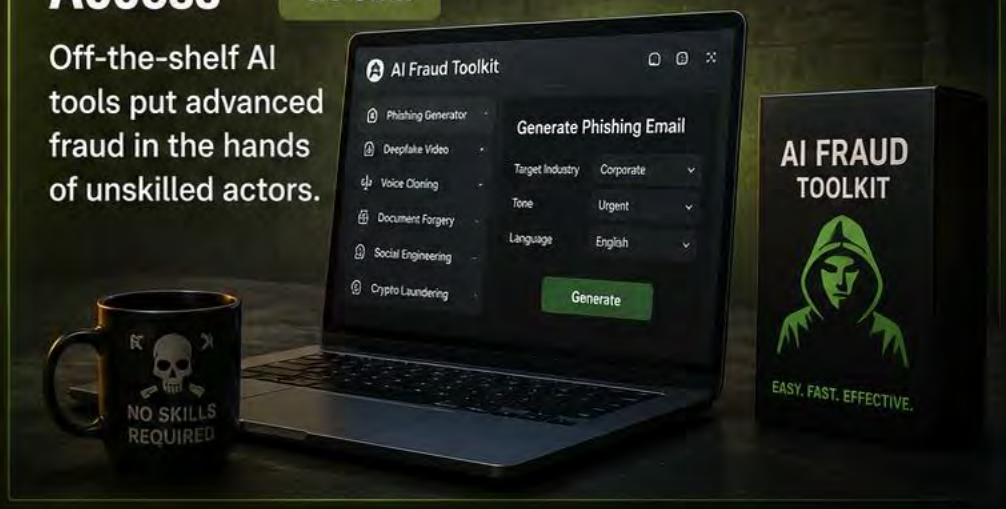
Believability

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.



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.

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.

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.

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.

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

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.

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

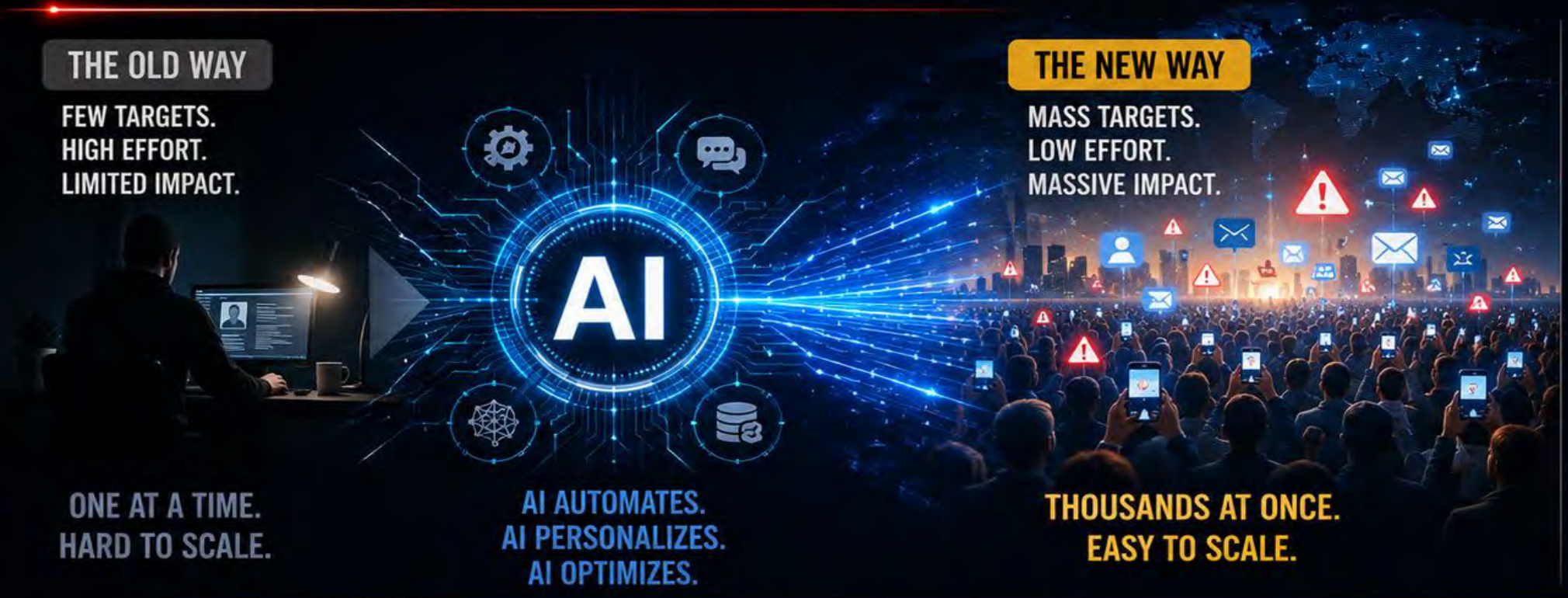
- AI reaches thousands—or millions—simultaneously.
- Every channel. Every time zone. 24/7.
- More targets. More victims.

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

Traditional defenses alone are no longer enough.

FROM TARGETED TO INDUSTRIALIZED.

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



ONE VICTIM → THOUSANDS

ONE CRIMINAL → AUTOMATED CAMPAIGNS

ONE LANGUAGE → EVERY LANGUAG

ONE TIME ZONE → 24/7 WORLDWI

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

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.

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.

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.

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.

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.


Verify Through a Clean Channel.
Use known numbers, portals, or prior contact information.
TRUSTED PORTAL
VERIFIED
URGENT: WIRE FUNDS
RING! RING!
COMIC-CON SECURE

OPTIONAL MODULE B

EXPANDED PREVENTION STRATEGIES

Additional safeguards for lawyers, law firms, and clients.

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:	VS.	SCAMMERS:
✓ Give you time to review and decide		✗ Demand immediate action
✓ Offer multiple ways to contact them		✗ Limit or block other contact methods
✓ Do not demand immediate payment		✗ Threaten consequences
✓ Encourage you to ask questions		✗ 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.

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.

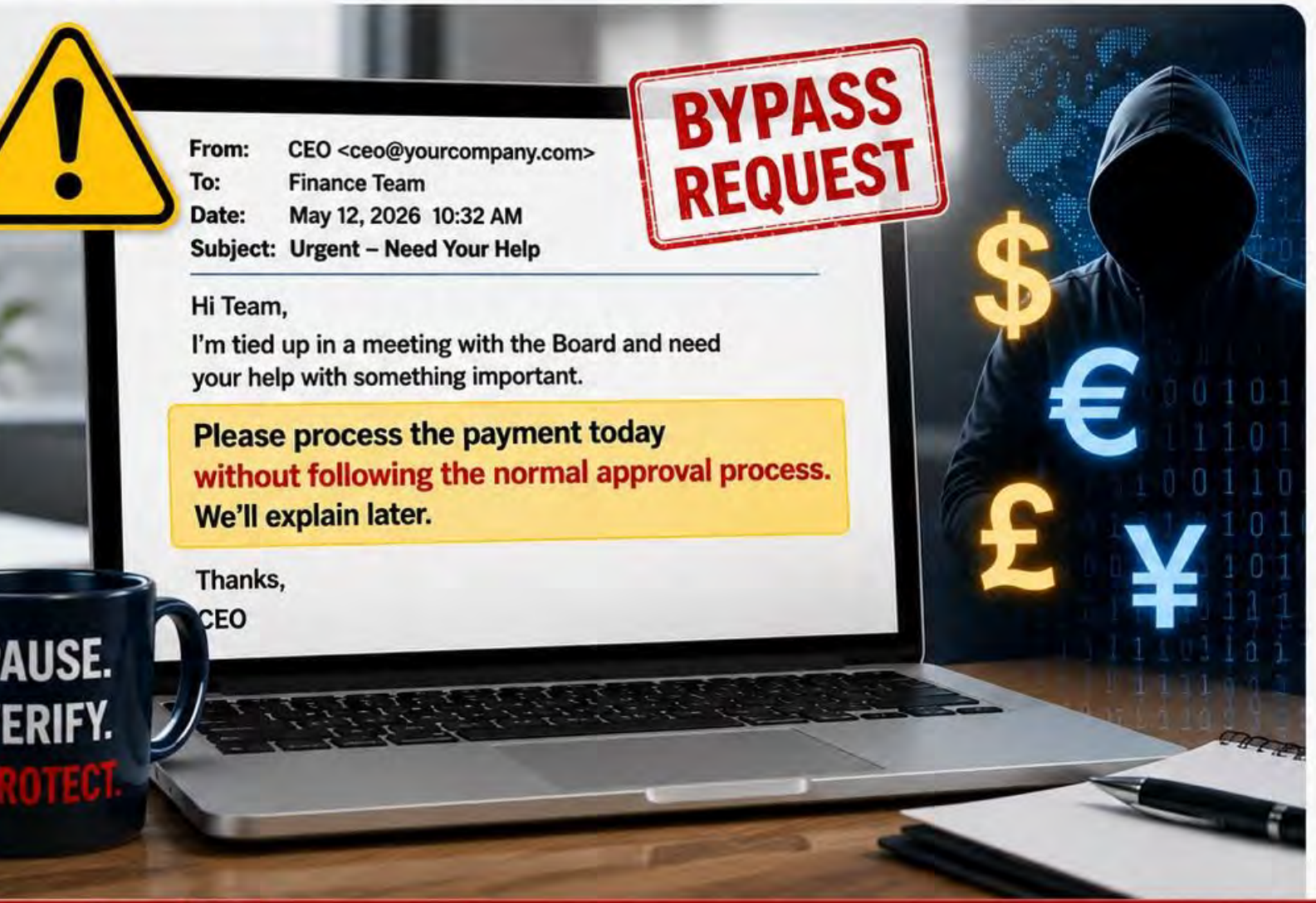
PAYMENT CHANGES AS A TELL

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.

REQUESTS THAT BYPASS PROCESS AS A TELL



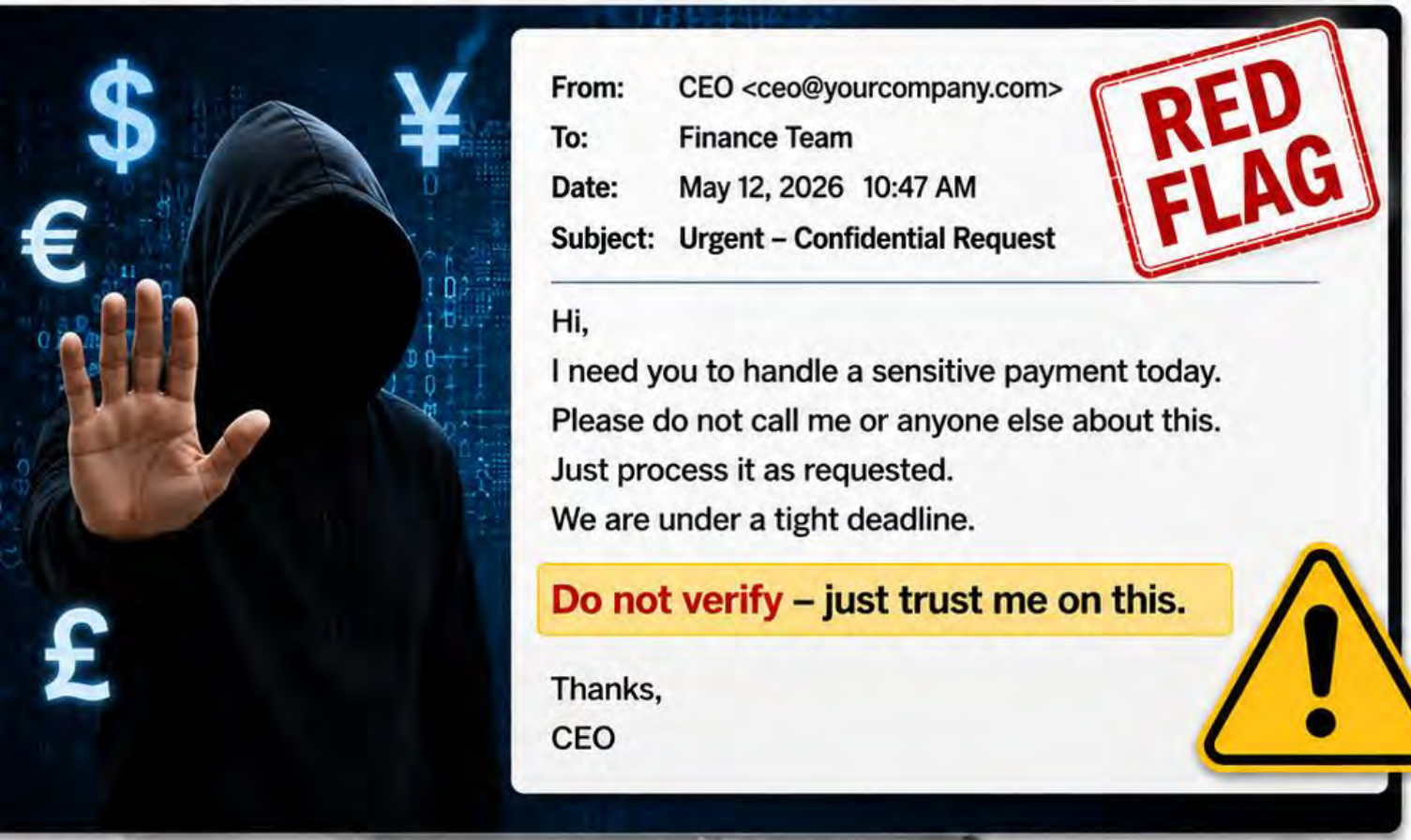
Out-of-process requests are a major red flag.

- 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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

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.

OPTIONAL MODULE C

EXPANDED INCIDENT RESPONSE

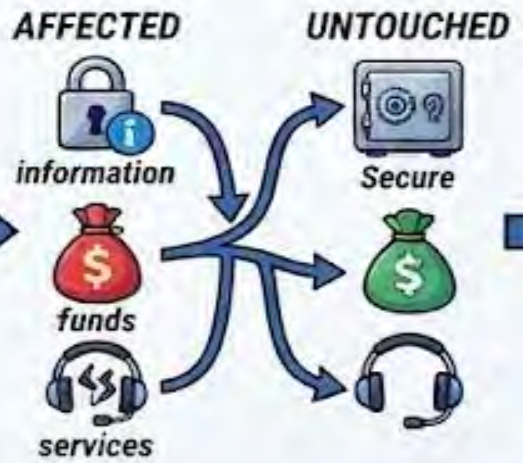
What to do after the attack begins.

Notify and Reassure Clients

1. Explain What Happened

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

2. Explain What It Means

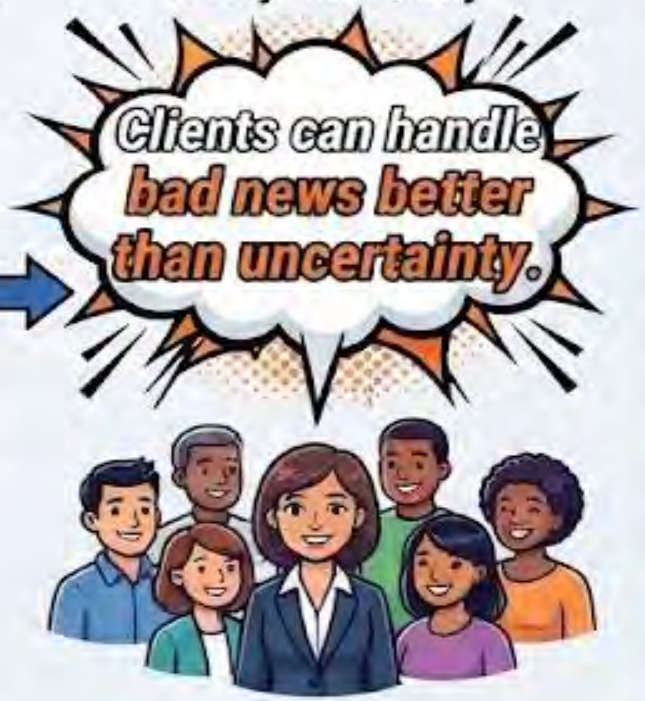


- **Explain what it means:** Tell clients what information, funds, or services may be affected.

3. Explain What Comes Next

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

4. Key Takeaway



A

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

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.

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

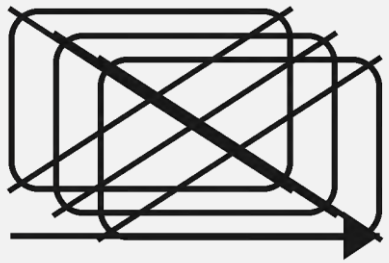
- Delay-send rules
- External recipient warnings
- Attachment review pauses
- Careful recipient verification

Small mistakes create major breaches

Breach Case Study: Law Firm Compromise

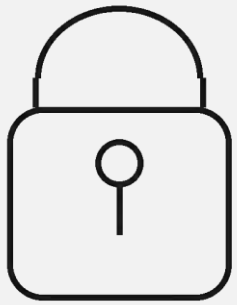
Common pattern: email takeover → lateral movement → data exfiltration.

- 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.



Ransomware/Extortion: The Privilege Trap

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



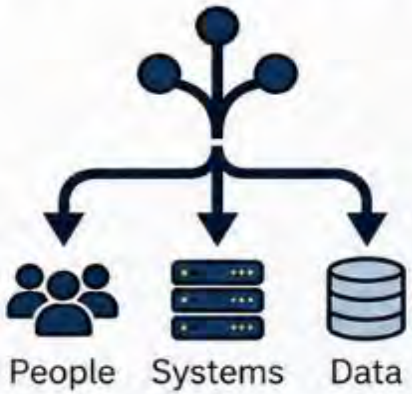
- Extortion gangs often publish samples — including privileged documents.
- Communications with insurers and vendors become discoverable if not structured.
- Best practice: separate breach counsel + establish privilege protocols.
- Treat incident response like a litigation file from minute one.

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.

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.

LAWYER
Legal

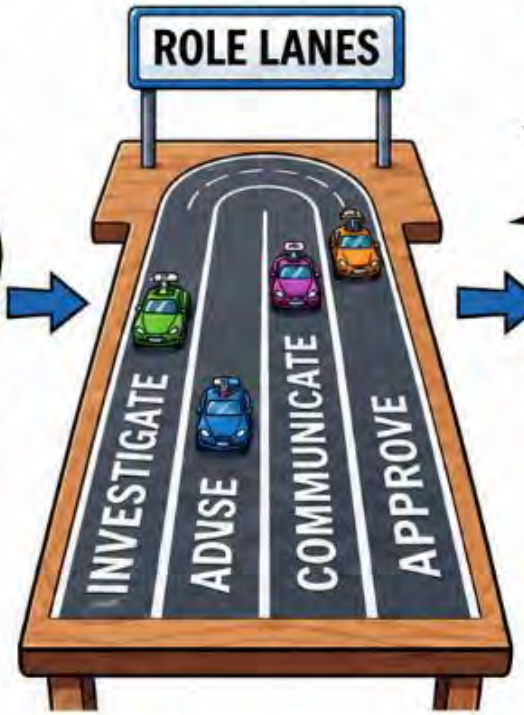
IT
InfoSec

MANAGER
Leadership

INSURER
Claims

FORENSICS
Analysis

3. Set Clear Lanes



4. Key Takeaway

The right people, with clear roles, move faster.

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

J

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

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

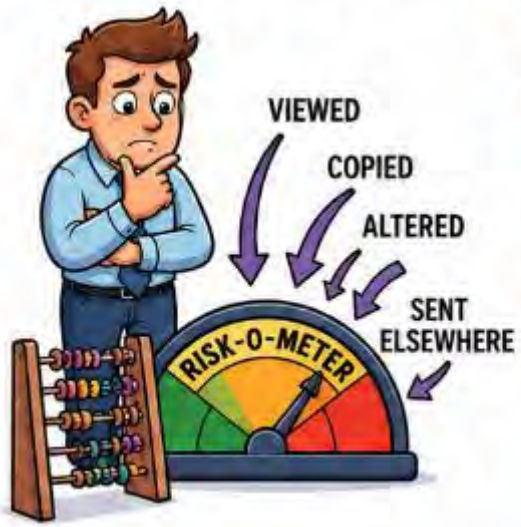
- **Key Takeaway**

Map the Data Exposure

1. Follow the Path

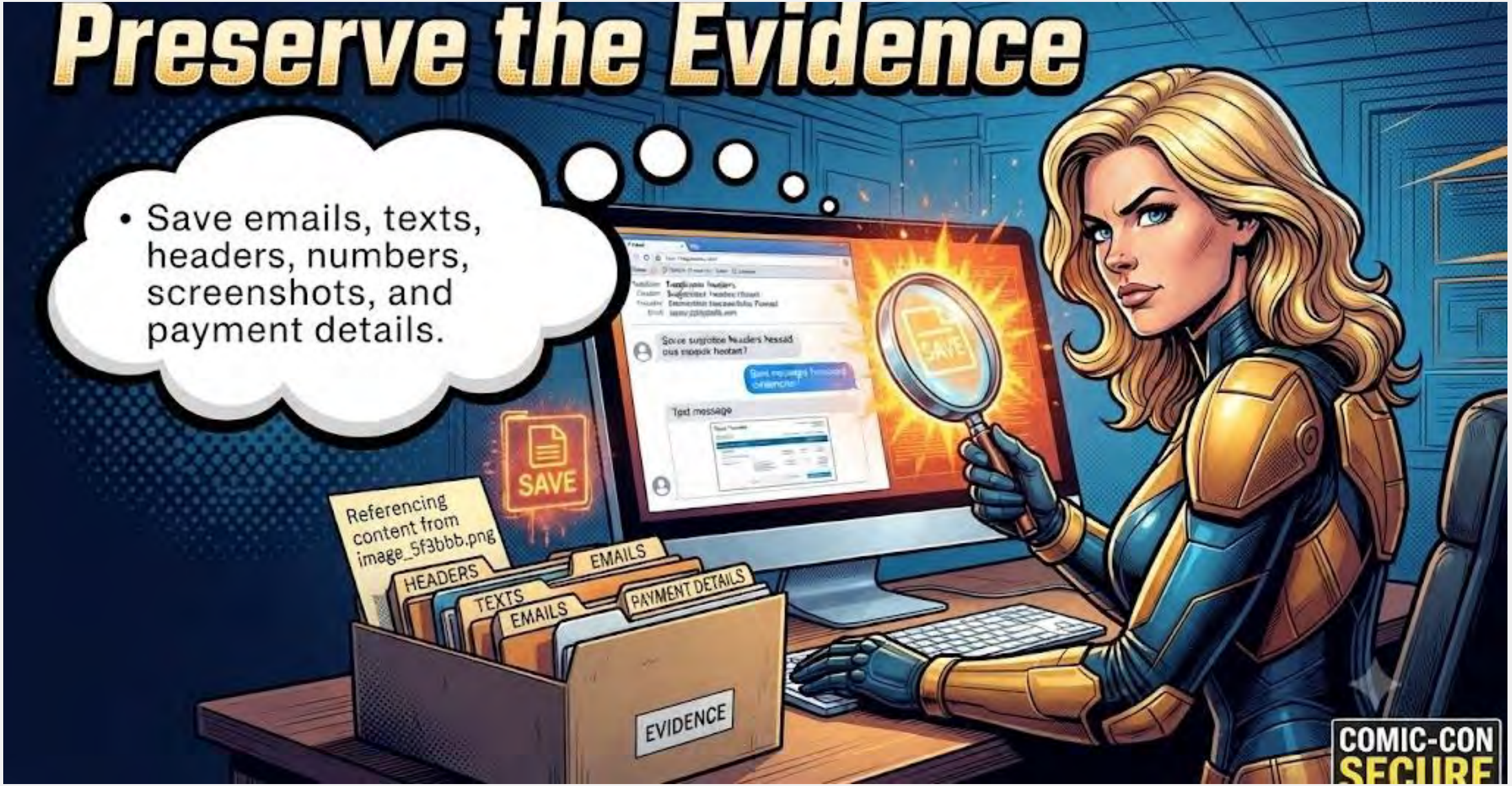
2. Identify What Was Touched

3. Measure the Risk



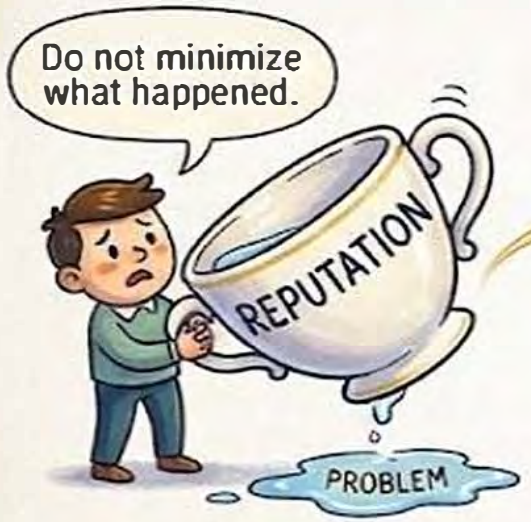
4. Key Takeaway

- **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**


Preserve the Evidence
• Save emails, texts, headers, numbers, screenshots, and payment details.
SAVE
Referencing content from image_5f3bbb.png
HEADERS
EMAILS
TEXTS
EMAILS
PAYMENT DETAILS
EVIDENCE
Text message
COMIC-CON

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

A

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.

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.


Alert the Right People Fast
Notify supervisors, IT, bank, insurer, and client as appropriate.
SUPERVISOR
SUPERVISOR
ALERT
IT
CYBERCRIME RESPONSE
INSURER
CLAIM INITIATION
CLIENT
CLIENT
NOTIFICATION
PAYMENT RECALL
CLAIM INITIATION
COMIC-CON SECURE

OPTIONAL MODULE D

ADVANCED AI & ETHICS

Emerging challenges, legal duties, and ethical considerations.

KEY ETHICS OPINIONS ON AI

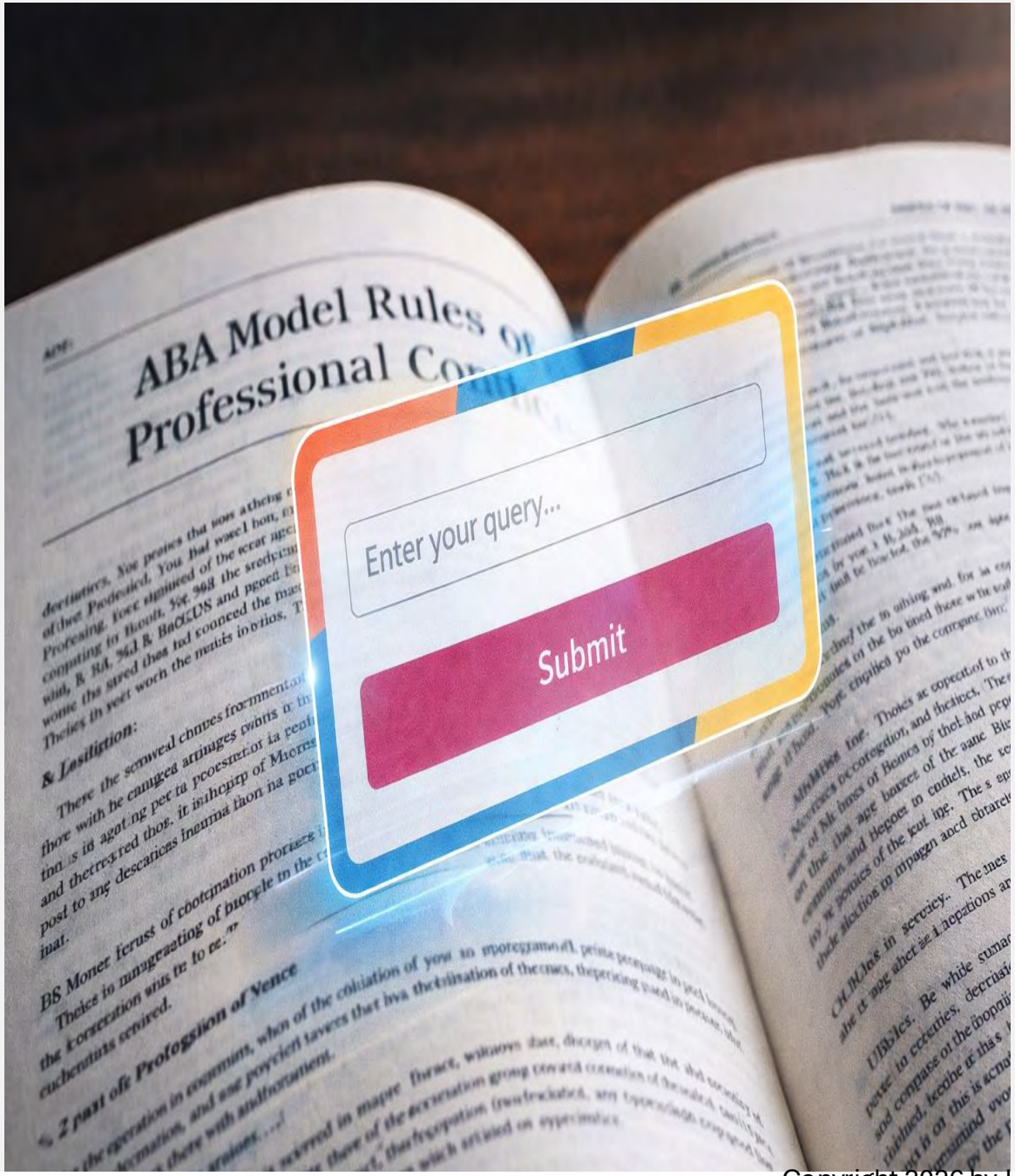
ABA Formal Opinion 512 (July 2024)

- 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



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.

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

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

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

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.

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

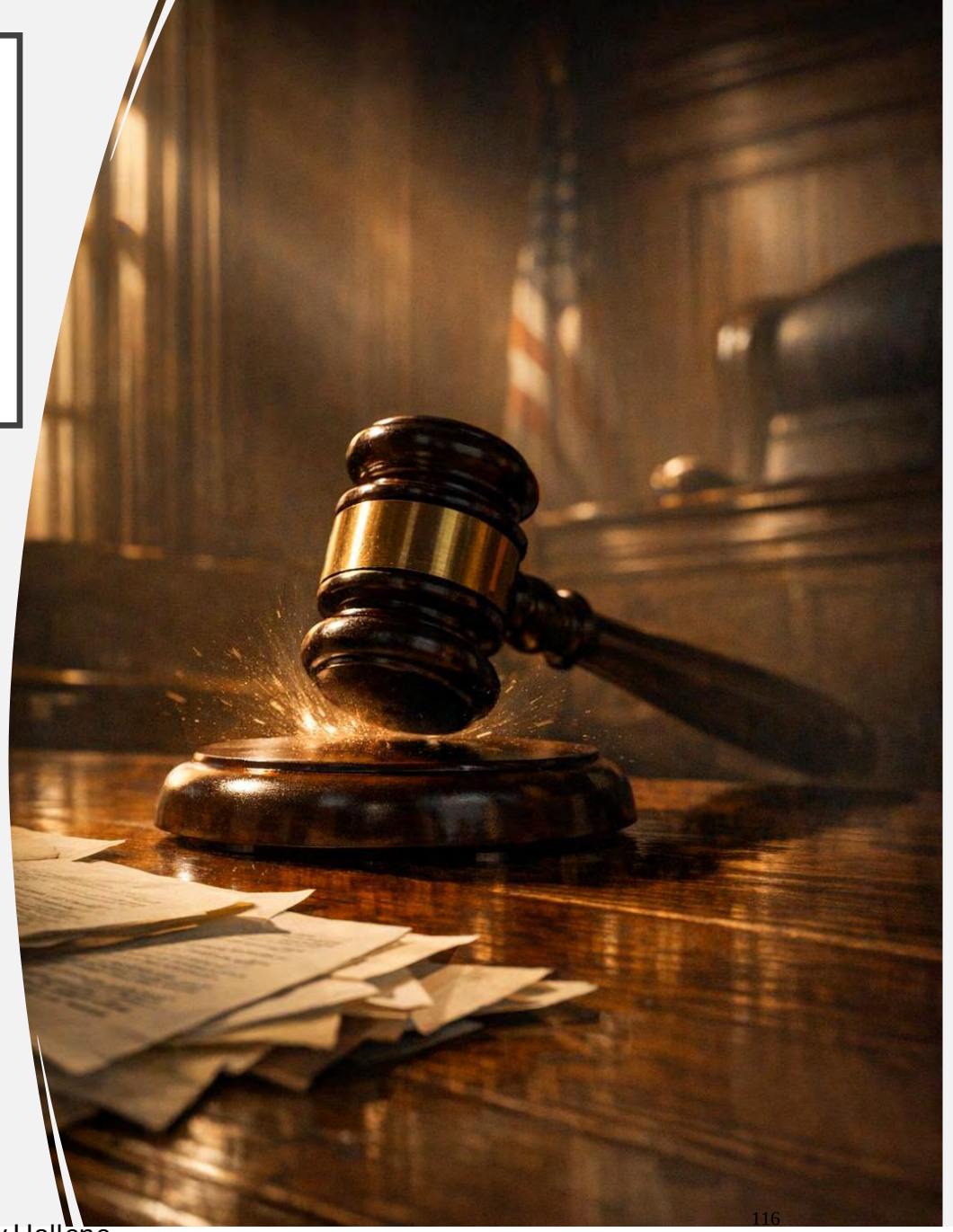
New York: Statewide rules with varying disclosure requirements across judges

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

Common requirements:

- Certify all citations verified against primary sources
- Disclose if AI was used in drafting substantive portions
- Check your local rules before every filing

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

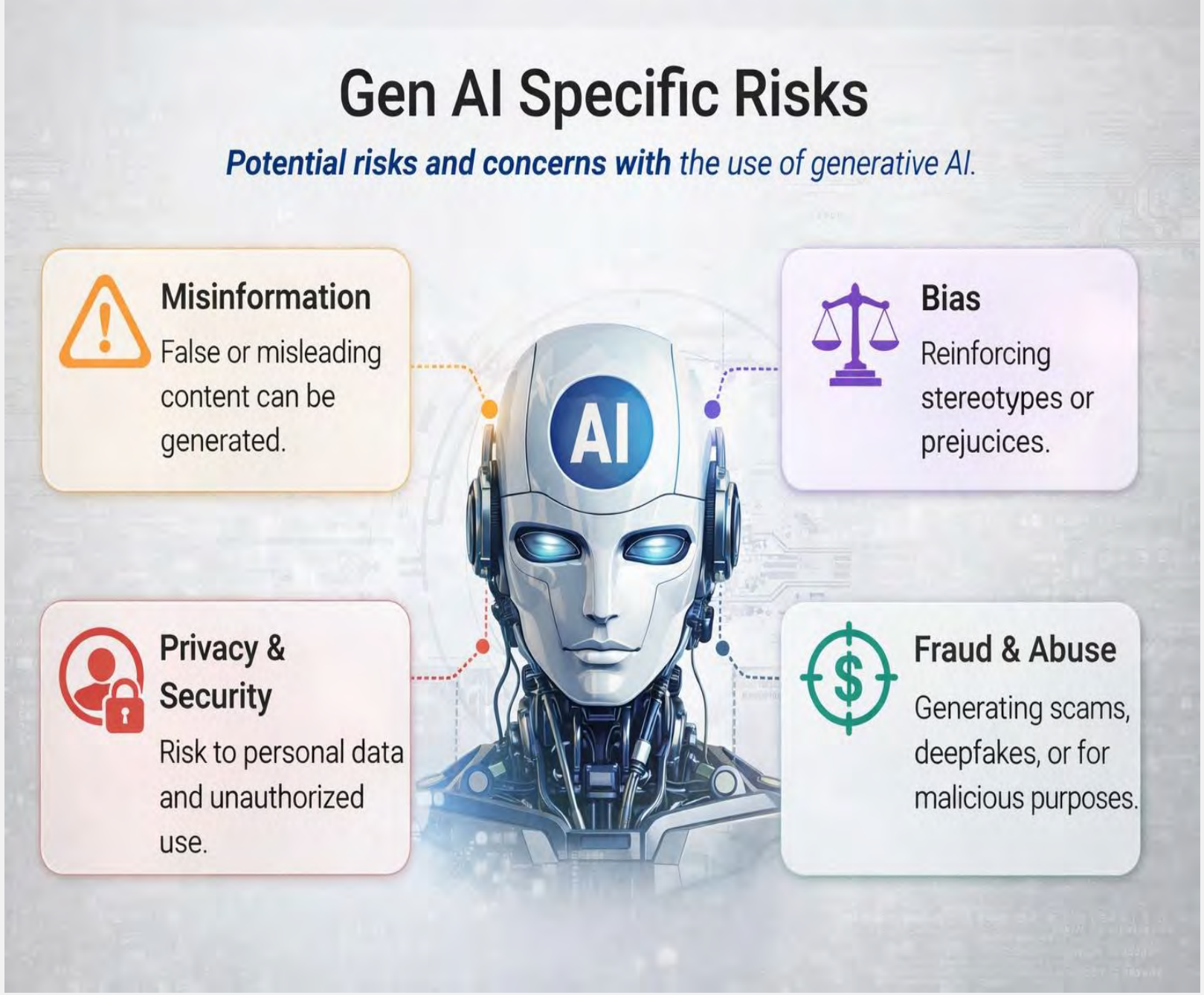
Two lawyers sanctioned for fake citations and misrepresentations in appellate briefs.

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.

116



Generative AI creates new content.

- **Inconsistent outputs**
- **Lack of transparency**
- **Misinformation**
- **Hallucinations**
- **Bias**
- **Data/Confidential information**

Duties of competence, and candor implicated.

AGENTIC AI…

WARNING ATTORNEY ROBINSON-DANGER!

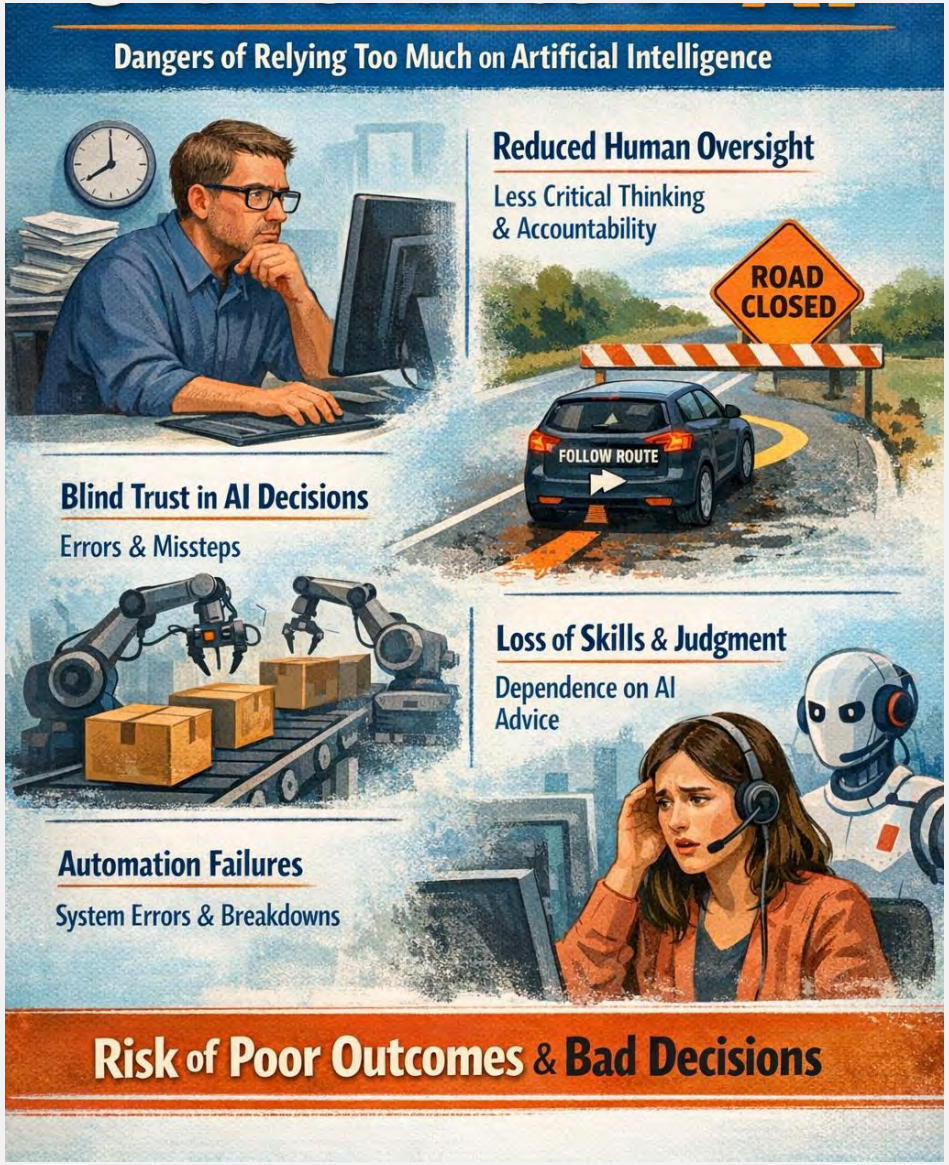
Coming soon to an AI near you---

AI reflects training data.

- Bias and skewed outputs

- Hidden assumptions

Requires careful review of everything.



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

Lawyers remain responsible.

OPTIONAL MODULE E

PRACTICE MANAGEMENT & OPERATIONS

Tools, policies, and processes to strengthen your firm.

CLIENT COMMUNICATION & ENGAGEMENT

Plain-Language Client Explanations

Client Letter & Email Drafting

Proposal & Pitch Material

Economic Risk

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

Navigating the Biometric Border

Jeffrey M Allen and Ashley Hallene

Mar 13, 2026 9 min read

Summary

- Biometric corridors and high-resolution sensors at premier transit hubs are replacing tra passport checks, allowing travelers to move through airports at a seamless, continuous v pace.
- Digital identity wallets use a secure Trust Triangle architecture to establish a cryptograph bridge between citizens and services, ensuring privacy through decentralized identifiers advanced liveness detection.
- Modern travelers must navigate a "privacy paradox" where the convenience of 24-hour d deletion in domestic terminals contrasts with the multi-year biometric retention requirec international security frameworks.

istock.com

Jump to:

Tech Column

The Death of the Document Shuffle

For decades, the ritual of international travel began with a frantic patting of pockets. The traveler searched for that small, navy-blue booklet, the physical proof of a right to exist in another latitude. We all remember the high-stress theater of the boarding gate: the heat of a crowded line pressing from behind, the fumbling of a phone to find a digital pass, and the desperate search for the physical passport to satisfy a gate agent's podium check.

In 2026, the document shuffle reached its quiet end. At the world’s premier transit hubs, the passport has retreated from the hand to the pocket. It is replaced by a credential you cannot lose and do not need to carry: your face. The airport of today no longer functions as a series of gated hurdles. Instead, it operates as a single, continuous stream. From the curbside at Heathrow to the boarding gates of Changi, biometric corridors now identify travelers at a walking pace. Sensors capture identity in the time it takes to blink, transforming the frantic search for a crumpled boarding pass into a seamless synchronization between your digital identity and the infrastructure around you.

The Walk-Through Airport: 2026 Infrastructure

The architecture of the modern terminal has evolved to support the unencumbered traveler. In leading hubs, the traditional layout of stanchions and serpentine lines is disappearing. Replacing these bottlenecks are biometric corridors. These long, sleek walkways use high-resolution sensors to verify a passenger's identity while they remain in motion. There is no need to stop or stand on a marked spot. The system matches the traveler's face against a secure digital gallery in seconds.

This integration extends to the very beginning of the trip. At smart baggage drops, the machine recognizes passengers as they approach. The system automatically links the luggage to the individual's biometric profile. This eliminates the need for physical tags or paper receipts. Every piece of data is tethered to the person rather than a slip of thermal paper.

The boarding process has seen a similar transformation. Gate agents no longer stand

behind podiums to scan individual passes. Instead, passengers walk toward the aircraft through a final biometric portal. The gate opens automatically upon a successful match. This "single-token" approach ensures that the person who checked in is the same person who boards the plane. It creates a high-fidelity security environment that is as invisible as it is effective.

The Technology: Digital Identity Wallets

Modern identification has moved beyond the plastic card. The European Digital Identity (EUDI) framework and U.S. "Touchless ID" initiatives represent a fundamental shift in how citizens prove who they are. These frameworks do not merely digitize physical documents. They establish a secure, cryptographic bridge between physical humans and digital services.

The Holding Ecosystem

The architecture of a digital wallet relies on a three-part relationship known as the Trust Triangle. This system eliminates the need for a central database to track every transaction, which preserves user privacy. To understand the "back-end" math, think of it like a standard credit card transaction:

- **The Issuer:** A government agency or trusted authority creates the digital credential. They sign the data with a unique digital signature to prove its authenticity. This is like a bank issuing you a credit card; they vouch for your identity and creditworthiness before handing you the plastic.
- **The Holder**: You carry the credential within a secure application on your smartphone. The phone does not just store a picture of an ID. It manages cryptographic keys that allow you to present your data securely. This is the card in your pocket, your personal tool for proving the bank's trust.
- **The Verifier**: An airline, a bank, or a border agent requests proof of identity. They check the digital signature against the Issuer’s public record. This process confirms the ID is valid without requiring the Verifier to contact the government directly. This acts like a store’s card reader; it scans your card to

confirm it is legitimate and authorized without needing to call a bank manager to verify every purchase.

The Shift to Liveness Detection

Security depends on the link between the wallet and the owner. To prevent "spoofing," where a bad actor uses a photo or a high-resolution video to bypass security, developers now integrate advanced Liveness Detection SDKs.

These tools analyze a biometric scan in real time to ensure the subject is a living, present human. Active liveness checks may require the user to blink or turn their head. Passive liveness checks work behind the scenes, analyzing skin texture, depth, and micro-movements to distinguish a human face from a digital screen or a physical mask. By requiring proof of presence, the wallet ensures that the person holding the phone is the person to whom the identity belongs.

The Global Mandate: New Rules for 2026

The transition to digital identity is no longer a matter of convenience. It is now a regulatory requirement. Governments across the globe have set 2026 as the year to formalize biometric border controls and move away from manual processing.

The European Shift

Europe has reached a critical turning point with the implementation of the Entry/Exit System (EES). While the project saw several delays, the European Commission has mandated that all external Schengen borders move toward full biometric registration in 2026. Non-EU nationals must now provide a facial image and four fingerprints upon their first entry into the zone.

This digital record replaces the traditional ink-and-paper passport stamp. The system automatically calculates the duration of stay and flags overstay with mathematical precision. Although member states have been granted a "grace period" through the summer of 2026 to manage peak travel congestion, the 90/180-day rule is now

enforced by a centralized database rather than a human inspector’s eye.

The U.S. Expansion

Across the Atlantic, the Transportation Security Administration (TSA) has accelerated its own biometric roadmap. By the end of spring 2026, the TSA intends to expand its "Touchless ID" program to 65 domestic airports. This initiative allows TSA Pre-Check members to navigate security without presenting a physical ID or a boarding pass.

The system relies on facial comparison technology that matches a live scan against existing government photographs. While currently marketed as a voluntary convenience for frequent flyers, the infrastructure serves as the foundation for a broader national transition to digital credentials and "hands-free" travel.

Carrier Liability

The burden of verification has moved upstream. Airlines now bear the legal and financial responsibility for the digital credentials of their passengers. Under the new 2026 enforcement rules, carriers must verify that a traveler has the necessary biometric registration and digital authorizations before boarding.

If a passenger arrives at a foreign border with invalid or missing digital credentials, the airline faces significant fines. This liability has forced airlines to integrate digital wallet verification directly into their check-in apps. By the time a traveler reaches the gate, the "Verifier" role in the trust triangle has already been satisfied, ensuring that only compliant passengers enter the international transport stream.

The Privacy Paradox: Speed vs. Security

Digital identity promises efficiency, but it introduces a conflict between rapid processing and the protection of personal data. Travelers must navigate a landscape where their biometric information is both a key and a digital footprint.

Data Retention Policies

The duration for which a system stores your data depends entirely on the nature of your travel. For domestic flights within the United States, the TSA generally adheres to a strict "short-term" protocol. Facial scans captured at the security checkpoint are compared against existing records and then deleted, often within 24 hours of the transaction. The goal is verification, not surveillance.

International travel operates under a different set of rules. The European Entry/Exit System (EES) maintains a long-term biometric database to track migration patterns and security risks. For most non-EU nationals, facial images and fingerprints are stored for three years. If a traveler overstays their visa, that data may be kept for much longer. Understanding these timelines is essential for any traveler concerned with their digital shadow.

The Right to Opt-Out

Despite the push for automation, digital verification remains (in theory) voluntary. Travelers possess the legal right to request manual processing. If you prefer not to use a biometric gate or a facial scanner, you may present a physical passport to a human officer. To exercise this right, you should inform the agent at the start of the inspection process.

However, a practical trade-off exists. Choosing manual verification often results in longer wait times and additional questioning. In some jurisdictions, opting out of digital systems may also disqualify you from using expedited transit lanes like Global Entry or Clear. While legal frameworks currently protect the "manual lane" as a permanent fixture for those with religious or privacy concerns, the operational reality suggests it will become an increasingly narrow path. As digital mandates tighten, the manual option may move from a standard alternative to an "exception-only" process, reserved for those whose biometrics fail to register or whose documents require secondary forensic scrutiny.

Encryption and Safety

Security measures are not limited to the digital realm. Physical passports and ID cards have evolved to defend against "skimming," a technique where hackers use

unauthorized readers to steal data from a distance. Modern identity booklets now incorporate metallic mesh layers and RF-blocking materials within their covers. These physical barriers create a Faraday cage, ensuring that the chip inside the document cannot be read while the booklet remains closed in your pocket.

This combination of physical shielding and high-level digital encryption ensures that your identity is only accessible when you intentionally present it for inspection.

Conclusion: Your New Path Through the World

The world of international travel has reached a turning point that feels like something out of a science fiction novel. While that familiar navy-blue passport remains a legal necessity for now, its daily job is effectively over. We keep the paper booklet tucked safely in our bags to satisfy the law, but we now use digital wallets to move through the terminal.

For those of us who remember the tactile comfort of a hand-stamped visa, the year 2026 marks a major shift. The old rituals (the frantic search for a paper boarding pass and the long wait for a physical ink stamp) are quickly becoming memories of a slower, more cumbersome past. In their place is a "silent" verification system. Your identity is confirmed not by a person squinting at a photo, but by a quick biometric scan and a secure digital connection.

In this new landscape, the very idea of "luxury" travel has changed. It no longer resides in the weight of a thick passport or a collection of colorful stamps from a dozen different countries. Today, the true luxury of travel is the freedom to move through the world with ease, gliding past the old bottlenecks without ever needing to break your stride.

Where to Find the "Touchless" Experience in the U.S.

As you plan your next journey, keep an eye out for these terminals currently leading the digital transition.

United States: TSA Touchless ID Hubs

The TSA Pre-Check Touchless ID program is entering a phase of rapid expansion. By the spring of 2026, this "hands-free" experience will be available at 65 airports across the country. To participate, you only need to be a current TSA Pre-Check member with a valid passport on file.

Instead of fumbling for your license at the security podium, you simply look into a camera. The system confirms your identity in seconds, allowing you to keep your ID in your pocket and your momentum toward the gate.

Participating Airlines and Locations

- **Alaska Airlines**: ATL, DAL, DCA, DEN, DTW, HNL, HOU, IAD, IAH, JFK, LAS, LAX, MCI, MSP, MYS, ORD, PDX, PHL, SAT, SEA, SFO, SJC, SLC, SNA, STL.
- **American Airlines**: ANC, ATL, BOS, CLT, DCA, DEN, DFW, DTW, EWR, FLL, HOU, IAD, IAH, JFK, LAS, LAX, LGA, MCI, MCO, MIA, MSP, ORD, PBI, PDX, PHL, SEA, SFO, SJC, SLC, SMF, SNA.
- **Delta Air Lines:** ATL, BOS, CLT, DAL, DCA, DEN, DFW, DTW, EWR, HOU, IAD, IAH, JFK, LAS, LAX, LGA, MCI, MSP, ORD, PBI, PDX, PHL, SEA, SFO, SJC, SLC, SNA.
- **Southwest Airlines:** ATL, BOS, CLT, DAL, DEN, DTW, IAD, HOU, LAS, LAX, LGA, MCI, OAK, ORD, PBI, PDX, PHL, SEA, SFO, SJC, SLC, SNA.
- **United Airlines**: ATL, BOS, CLT, DCA, DEN, DFW, EWR, IAD, IAH, JFK, LAS, LAX, LGA, MCI, MSP, ORD, PBI, PDX, PHL, SEA, SFO, SJC, SLC, SNA.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-march/navigating-the-biometric-border/?utm_source=chatgpt.com

GPSolo Magazine GPSolo September/October 2025 (42:5): In-House Counsel Life

The Perils of Crossing Borders with Confidential Data

Jeffrey M Allen

Sep 30, 2025 9 min read

Summary

- In many jurisdictions, customs and immigration officers have sweeping powers to inspec persons, luggage, and electronic devices, often without a warrant or demonstrable suspi
- Travel with a “clean” device—one that contains only the minimum information needed fo trip, with no confidential or sensitive files stored locally.
- Utilize secure cloud storage with robust multifactor authentication. Access data only as n
- If a border official requests access to your device, assert privileged material and request special procedures (such as review by independent officials) be followed where available

Hinterhaus Productions/DigitalVision via G

Jump to:

Data is the lifeblood of modern commerce, law, research, and innovation. Professionals such as attorneys, executives, scientists, and consultants frequently travel internationally, often carrying with them computers, smartphones, external drives, and other data-storing devices. While the ability to access information on the go provides

convenience and flexibility, it also presents substantial risks, particularly when the data is confidential, proprietary, or privileged. Crossing international borders with sensitive information can expose travelers and their organizations to regulatory, legal, and ethical dangers, including the possibility that foreign governments may require access to devices and their contents.

Understanding the Risks

International travel compresses three threat vectors into a single moment: (1) broad sovereign police powers at ports of entry, (2) unfamiliar legal regimes that may override attorney-client privilege, and (3) opportunistic cyber-criminals drawn to transient devices on untrusted networks. A lawyer who would never knowingly hand an opposing party the firm's file can, at Heathrow or Dubai, be compelled to do its digital equivalent.

The Expanding Powers of Border Authorities

When entering a foreign country, individuals must submit to that country's laws and border security protocols. In many jurisdictions, customs and immigration officers have sweeping powers to inspect persons, luggage, and electronic devices, often without a warrant or demonstrable suspicion. Intended to protect national security, combat crime, and enforce customs regulations, these powers also provide the legal basis for accessing, copying, or seizing data.

Categories of Confidential Data at Risk

- **Attorney-client privileged information.** Legal professionals often carry documents and communications protected by privilege.
- **Trade secrets and proprietary business information.** Executives might travel with sensitive company data, intellectual property, and contracts.
- **Personal data.** Employees might have health records, financial documents, or private communications stored on company devices.
- **Research data.** Academics and researchers might have unpublished findings

or sensitive fieldwork information.

If intercepted by foreign authorities, such data could be compromised, misused, or disclosed to competitors or hostile interests.

The Cybersecurity Threat Landscape

Traveling with confidential data exposes devices to physical theft, malware or spyware installation, and surveillance. In some locations, border agents or intelligence services may temporarily confiscate devices for “inspection,” during which they could image hard drives or install monitoring software.

Legal Issues in Transporting Confidential Data Internationally

Conflicts of Law

When traveling internationally, the legal protections afforded to data at home may not extend across borders. U.S. attorneys rely on the Fourth Amendment and various statutes to protect client information, but these do not bind foreign officials. Similarly, data protected under the EU’s General Data Protection Regulation (GDPR) may lose that shield upon export or may trigger cross-border data transfer requirements.

Attorney-Client Privilege and Work Product Doctrine

For lawyers, few issues are graver than violating the attorney-client privilege. While many countries recognize some form of legal privilege, the scope and enforcement mechanisms vary widely. In the United States, privilege is robustly protected, but in other nations, border agents may not have to respect or recognize such protections and may lawfully demand access to confidential files.

Export Control and Data Localization Laws

Sometimes, carrying data across borders is itself subject to legal restriction. Certain technical data, defense-related information, or personally identifiable data may be restricted by export control laws (e.g., U.S. International Traffic in Arms Regulations, EU Dual-Use Regulation) or data localization mandates.

Professional and Ethical Obligations

Attorneys and other professionals are bound by ethical codes requiring them to safeguard client information. The American Bar Association's Model Rules of Professional Conduct mandate that lawyers take reasonable precautions to prevent unauthorized disclosure of client data.

Countries with Expansive Digital Search Laws

United States

U.S. Customs and Border Protection (CBP) asserts the right to search electronic devices without a warrant at the border. Court decisions have generally upheld broad search powers, although some limits have been imposed for privileged or sensitive content. CBP officers may demand access to devices, request passwords, and detain devices for extended analysis. Privilege claims trigger "filter team" review but do *not* block inspection.

Canada

Canada Border Services Agency (CBSA) can lawfully search electronic devices at ports of entry. Canadian courts have found that travelers have a reduced expectation of privacy at the border, and device searches are not subject to the same threshold as criminal investigations. *R. v. Pike,* 2024 ONCA 644, struck down random, suspicion-free device searches as unconstitutional but gave Parliament six months to legislate a standard ("reasonable grounds to suspect"). Until new legislation is enacted, case law constrains but does not eliminate searches; refusal risks seizure. Travelers should carry proof that the device holds solicitor-client data.

United Kingdom

Under Schedule 7 of the Terrorism Act 2000, U.K. border officials can detain and search individuals (including their electronic devices) without suspicion. Refusal to provide access or passwords can be prosecuted as a criminal offense under § 49, Regulation of Investigatory Powers Act 2000 (RIPA), with penalties up to two years' imprisonment for failing to disclose keys. Solicitor-client privilege is not absolute at the border.

Australia

The Australian Border Force may inspect and copy data from electronic devices without a warrant. Failure to cooperate can lead to device seizure or prosecution.
The Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 (TOLA) lets authorities serve technical assistance notices compelling decryption or other access help. Failure to assist can trigger civil penalties; assisting must be "reasonable and proportionate," but the determination is by the issuing agency. Traveling counsel remain potential "relevant service providers."

China

Chinese authorities have broad powers to inspect and image electronic devices at the border. Foreign travelers must sometimes install government-approved software on their devices. The 2023 amendments to the Counter-Espionage Law and a 2024 revision of the State Secrets Law allow inspection and imaging of electronic devices "relevant to national security." Non-cooperation may lead to detention or entry denial; fines under Article 30 may reach 500,000 yuan (approximately $70,000). Cloud-only access from within China avoids border media seizure but triggers data-localization issues.

Russia

Russia's Federal Security Service (FSB) can require travelers to decrypt files and provide access to devices at the border, particularly for foreigners or in cases of "security concerns." "Yarovaya" Anti-Terror Amendments (Fed. Law No. 374-FZ, 2016) compel service providers to furnish decryption keys to the FSB and criminalize refusal, with

fines up to 1 million rubles (approximately $12,000) and potential license revocation. Foreign lawyers acting as "information distribution organizers" (e.g., operating firm email) may be covered.

Other Jurisdictions

Many other countries—including New Zealand, India, Israel, and Singapore—have provisions allowing border agents to demand access to digital devices, copy data, and detain travelers who refuse cooperation.

Practical Steps for Attorneys to Protect Confidential Data While Traveling

Recognizing the seriousness of these risks, attorneys and professionals must take proactive measures to protect the confidentiality and integrity of their data while traveling internationally.

- **Privilege is territorial.** Most common law jurisdictions recognize attorney-client privilege, but at ports of entry, it collides with sovereign search authority. U.S. CBP policy promises a "filter officer" if you object on privilege grounds, but this policy also permits shipping the device's image to a forensic lab pending resolution of the claim.

- **You have an ethical duty to safeguard information.** ABA Model Rule 1.6(c) obliges lawyers to make "reasonable efforts" to prevent unauthorized disclosure. Formal Opinion 477R (2017) applies that duty to electronic communication and encryption.

- **Competence includes cyber-competence.** Model Rule 1.1 Comment 8 requires lawyers to keep abreast of "the benefits and risks associated with relevant technology." Choosing to cross a border with unencrypted client data —when safer alternatives exist—may breach both competence and confidentiality duties.

- **Cloud storage is not always safe.** Shifting data to the cloud before travel

seems safe, but some jurisdictions (e.g., China and Russia) assert data-localization and onshore access powers over cloud providers. Failing to consider where the cloud copy resides can inadvertently place the data within reach of foreign process.

Threats Beyond Officialdom

- **Opportunistic theft.** Crowded airports offer rich pickpocket and shoulder-surfing environments. Lost devices remain the leading cause of reported data breaches in the ABA's annual *Legal Technology Survey Report*.
- **"Juice-jack" malware.** Public USB charging kiosks can deliver malware payloads that auto-exfiltrate credentials the next time the device goes online.
- **Rogue WiFi and IMSI (international mobile subscriber identity) catchers.** Ad-hoc networks at conferences or hotels are easily spoofed; a traveler's laptop may silently hand over files to a man-in-the-middle attacker.

Pre-Travel Risk Assessment

- Inventory the data you plan to take; determine whether it is necessary to carry sensitive information.
- Understand the laws and risks associated with each country you will visit or travel through.
- Consult with your organization's IT and legal teams to establish approved protocols for data protection.

"Clean" Devices

Travel with a "clean" device—one that contains only the minimum information needed for the trip, with no confidential or sensitive files stored locally. Access to confidential

data can be obtained via secure, cloud-based systems after arrival, and wiped before returning (but note caveat above regarding potential dangers when accessing cloud storage in some foreign jurisdictions).

Data Encryption

- Use full-disk encryption on all devices, with strong, unique passwords not written down or stored with the device.
- Encrypt individual files or folders, and use encrypted external drives for necessary sensitive data.
- Some countries may legally require you to provide decryption keys or passwords on demand.

Secure Cloud Storage and Remote Access

Do not store confidential data on local devices. Utilize secure cloud storage with robust multifactor authentication. Access data as needed. If border agents demand device access, the locally stored content will be minimal.

Two-Factor Authentication and Strong Passwords

Ensure all devices and key accounts use two-factor authentication. Passwords should be strong, unique, and not repeated across different accounts. Avoid biometric authentication if local law allows authorities to compel biometric unlocking.

Physical Security Measures

- Never leave devices unattended in transit; use physical locks where possible.
- Be cautious of using public WiFi, especially in airports and hotels, and avoid entering passwords or accessing sensitive data over unsecured connections. Employ a reliable VPN (virtual private network).

- Consider travel insurance that covers cybersecurity incidents and device theft.

Limiting Device Data Before Re-Entry

Before returning to your home country, minimize the data stored on your device. Purge unnecessary files and securely delete any confidential data temporarily stored on the device.

Dealing with Demands for Access at the Border

If a border official requests access to your device, remain calm and polite. Know your rights under local law. In some jurisdictions, you may refuse to provide passwords, but this may result in device seizure or denial of entry. If you are an attorney, assert privileged material and request that special procedures (such as review by independent officials) be followed where available.

Notifying Clients and Supervisors

Inform your clients and supervisors of the risks associated with international travel. Seek advance consent where appropriate, and document your risk-mitigation efforts.

Post-Travel Precautions

Upon returning, scan devices for malware and evidence of tampering. Change all access credentials that may have been compromised.

Special Issues for Litigation and Transactional Counsel

- **Export-controlled materials.** Technical data subject to the International Traffic in Arms Regulations (ITAR, which primarily focuses on defense-related articles and services) or the Export Administration Regulations (EAR, which covers a broader range of items, including those with both commercial and military applications, often called “dual-use” items) may itself be illegal to export on a laptop. When traveling with such data, carry an export-license

compliance memo.

- **Privacy statutes.** The GDPR, the California Privacy Rights Act (CPRA), and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) impose breach-notification duties that start ticking the moment a device is seized or lost abroad.
- **Multijurisdictional practice ethics.** Carrying client data into a country where you are not licensed can be construed as "conducting legal business" there, implicating unauthorized-practice rules.

The Evolving Legal and Policy Landscape

Privacy advocates and legal organizations continue to challenge excessive digital search powers at borders, arguing for stronger protections and clearer procedures for confidential and privileged data. Some countries have implemented "privilege team" protocols, where sensitive data is reviewed by independent officials, but enforcement is inconsistent.

Best Practices for Traveling with Confidential Data

Step	Implementation Tips	Authority/Guidance
1. Data Minimization	Carry only what you cannot access remotely via a secure channel. Use a fresh "travel laptop" with no client archives.	NSA Mobile Device Best Practices (September 2021) recommends wiping and reinstalling the operating system before and after travel.
2. Strong Encryption at Rest	Use full-disk encryption (FDE) with a long passphrase; enable "travel mode" on password managers to purge vaults.	The Regulation of Investigatory Powers Act 2000 (RIPA) § 49 and similar laws target refusal to disclose keys—if the data are absent, there is nothing to decrypt.

3. Defensible KeyManagement	Do not memorize the decryption key; store it in a secure cloud HSM (hardware security module) accessible only once you clear customs.	ABA Formal Opinion 477R endorses off-device key storage for cross-border travel.
4. Zero-Trust Cloud Access	To reach a U.S.-hosted document repository from abroad, use security assertion markup language (SAML, a protocol for exchanging authentication and authorization data between an identity provider and a service provider) and one-time password (OTP, a security mechanism that provides a unique, time-sensitive password for authentication, often used as a second factor in multifactor authentication).	Many privilege rules treat documents stored abroad as subject to foreign subpoena; keep servers domestic.
5. Hardened Mobile Phones	Remove SIM; disable Bluetooth, NFC, and autoconnect WiFi; reboot daily.	National Security Agency (NSA) travel bulletins advise weekly reboot; daily is better abroad.
6. Incident-Response "Go Kit"	Include point-of-contact cards for firm IT, breach counsel, and insurer; carry tamper-evident bags to seal seized devices.	ABA Model Rule 1.1 extends to incident-response planning.
7. Privilege Labels and Claw-Back Agreements	Mark files "ATTORNEY-CLIENT PRIVILEGED/NOT FOR BORDER SEARCH"; bring a copy of CBP Directive 3340-049A and the jurisdiction's privilege statute.	Practical experience shows officers are more likely to summon a filter team when privilege claims are clear.
8. Training and Documentation	Brief every traveling lawyer and staffer; record that training for later malpractice defense.	Failure to train is cited in recent disciplinary actions under ABA Model Rule 5.3.

Protect Your Data

Traveling internationally with confidential data exposes professionals and organizations to significant risks, including invasive border searches, legal conflicts, and ethical challenges. Careful planning, use of technology, and awareness of both legal obligations and foreign laws can dramatically reduce exposure. By following the practical steps outlined above, travelers can better protect their own interests, as well

as those of clients, employers, and stakeholders, when crossing international borders.

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...

ABA American Bar Association | https://www.americanbar.org/groups/gpsolo/resources/magazine/2025-sep-oct/perils-crossing-borders-confidential-data/?utm_source=chatgpt.com

TAPAs: Mobile Apps Every Solo Should Us

Jeffrey M Allen and Ashley Hallene

Dec 10, 2025 7 min read

Summary

- **T**echnological **A**nd **P**ractice **A**dvice to help you become more efficient and effective. This tips to transform your phone into a paralegal while adhering to the highest ethical stand
- Standard text messaging (SMS) is rarely secure enough for privileged dialogue. Instead, u secure client portals or encrypted messaging apps.
- Your smartphone camera, paired with the right software, is a scanner replacement.
- Mobile time capture apps help ensure you are paid for all the work you do on behalf of y clients.

Thai Liang Lim via G

Jump to:

The modern law office is no longer defined by mahogany desks or floor-to-ceiling bookshelves. It fits in a pocket. For the solo or small firm lawyer, the smartphone has evolved far beyond a mere communication device. It has become an on-the-go assistant, always available and always working. While large firms rely on armies of

support staff, the solo lawyer must maximize personal productivity. Solos and small firms stand to gain the most from embracing mobile productivity.

We must, however, begin with a brief caution. Mobility increases convenience but also increases cybersecurity risk. The following guide outlines how to transform your phone into a paralegal while adhering to the highest ethical standards.

Secure Communication: Keeping Client Conversations Confidential

The foundation of the attorney-client relationship is confidentiality. When you leave the secure perimeter of your office, that foundation becomes vulnerable to threats. You must prioritize encrypted messaging and calling for client communications.

Standard text messaging (SMS) is rarely secure enough for privileged dialogue. Instead, use secure client portals (e.g., Clio Manage) or encrypted messaging apps (e.g., Signal). These tools create a walled garden that keeps sensitive information protected from prying eyes.

When evaluating communication tools, certain features are non-negotiable. Look for end-to-end encryption. This ensures that only the sender and the recipient can read the message. You also need multifactor authentication (MFA) to prevent unauthorized access, along with audit trails to document who accessed what information and when.

Implementing mobile communication ethically requires practice. Secure file-sharing tools (e.g., ShareFile) and e-signature tools (e.g., Docusign) allow you to move cases forward without compromising data integrity. Do not rely on standard email for sensitive attachments. Use a secure link. This practice protects the client and demonstrates your commitment to data security.

Scanner Replacements: Paperwork on the Go

Paper is the enemy of mobility. Fortunately, we can now easily convert paper to digital images almost anywhere. Your smartphone camera, paired with the right software, can serve as a scanner replacement.

The camera alone won't suffice. You need recommended features that transform a photograph into a usable legal document. Optical character recognition (OCR) is essential. OCR converts a picture of text into searchable, editable digital content, turning a snapshot into a working document. Without it, your digital file remains merely a picture, not a document. Adobe Scan can assist you in that regard.

Good scanning apps also provide automatic cropping and de-skewing. These features straighten the image and remove the background, making a photo taken on a coffee shop table look like it came from a flatbed scanner. Crucially, the app must offer secure cloud backup. A scan trapped on a lost phone is worse than useless; it's a liability.

The use cases for the mobile lawyer are extensive. You can immediately capture exhibits in court. You can sign documents on the fly. You can save receipts for expense reports before you lose the paper slip.

Adhere to best practices for storing, naming, and securing scanned documents. A file named "Image_001.jpg" is impossible to find six months later. Name the file immediately upon scanning. File it in the correct client folder in the cloud. Do this instantly, and you will never face a huge backlog of mystery documents, and you will greatly reduce the number of misplaced documents as well as the time required to find the one you need.

Mobile Timekeeping: Never Lose a Billable Minute Again

For the solo practitioner, time is inventory. If you fail to record it, you cannot sell it. Mobile time capture reduces revenue leakage for solos. The "leakage" occurs when you answer a client call in the car or answer an email in line at the grocery store, then forget to log the 0.1 or 0.2 hours.

Key capabilities in timekeeping apps make this process effortless. Look for one-tap timers. Complexity discourages use, resulting in lost revenue. If you can start a timer with a single tap, you will. Voice-activated time entries are also valuable. You can dictate the billing narrative immediately after a meeting ends, ensuring accuracy.

Some advanced apps offer automatic prompts or even entirely passive tracking based on calls, texts, emails, documents, and other work activity, which can be a real boon for attorneys often away from the office. Clio, for example, includes AI-supported activity tracking that flags when you've spent time communicating with a client (on calls, emails, etc.) and prompts you to create a time entry. This passive detection helps capture billable time you might otherwise forget.

Two particular apps in this space take automation a step further by minimizing or even eliminating the need for manual timers or memory-based logging:

- Billables AI runs in the background across the tools you already use (e.g., email, calendar, document-editing, video, and conference tools) and automatically captures your billable activity as you work. It doesn't rely on you remembering to "start the timer." Instead, every meaningful interaction (drafting documents, sending emails, attending calls or meetings) can be transformed into a time entry automatically. Billables AI then matches the activity to the correct client and matter, generates narrative descriptions consistent with your billing style or outside-counsel guidelines, and produces a time report ready for review.
- Time Miner provides another powerful option, offering a retroactive, communication-driven approach. Instead of needing you to remember to hit "start/stop," Time Miner scans your past calls, texts, and emails (from phone, mobile, or work systems), identifies client-related interactions, and automatically generates billable entries tied to the correct client/matter. Because Time Miner syncs with major case-management systems, the captured entries can be reviewed and exported for billing without additional manual work.

A mobile timer that does not sync with your primary billing software creates double-entry work. Avoid this. The data must flow seamlessly from phone to invoice.

The goal is to turn mobile timekeeping into a consistent habit. Capture the time when the work happens. Do not reconstruct your day from memory. Memory is fallible. Contemporaneous time entry is profitable.

AI Summarizers and Research Assistants: Quick Insights at Your Fingertips

Artificial Intelligence has moved from science fiction to the app store. AI tools now accelerate note review, meeting summaries, and email drafting (tasks that traditionally fell to junior associates or support staff). For the solo lawyer without a junior associate to lean on, AI can be a powerful force multiplier.

AI shines when you need to quickly digest large volumes of information. Traveling with a 50-page transcript? Let AI produce the first-pass summary so you can focus on the issues that matter. Instead of scrolling through a deposition on a small screen, use an AI tool to generate a synopsis of key points. This allows you to prepare quick client updates or spot issues before deeper research.

Several AI platforms are especially helpful for creating summaries, synthesizing notes, and extracting insights from legal materials. The two below are among the most notable:

- NotebookLM, Google's AI-powered "research assistant, allows you to upload your own sources (PDFs, transcripts, memos, exhibits, discovery documents, etc.) and ask questions directly about them. NotebookLM generates concise summaries, outlines, and issue-spotting notes tailored to the documents you provide. For a lawyer reviewing a lengthy deposition or expert report, this means instant access to key testimony, contradictions, or thematic summaries without manually sifting through pages. Its new mobile app lets you upload documents and receive summaries from your phone while traveling, in court hallways, or during client meetings. Because it limits outputs strictly to the materials you upload, it reduces hallucination risk and offers a more controlled, evidence-based workflow.

- Notigo is a purpose-built application for professionals who need meeting intelligence. For lawyers dealing with back-to-back client calls, strategy discussions, mediations, Zoom hearings, or witness interviews, Notigo provides real-time transcription and generates structured meeting summaries. Its legal-focused workflows help preserve accurate records for client communications

and file documentation. Notigo also integrates with calendars and conferencing platforms, making it easy to create clean, compliant summaries even from your mobile device.

A word of warning about ethics is critical here: You must verify all AI outputs. AI can hallucinate cases or misinterpret statutes. You remain the attorney; the AI should work as a drafter and assistant only. Furthermore, you must protect client data. Avoid uploading privileged documents without safeguards. Public AI models may train on your data, breaching your duty of confidentiality.

Look for features that indicate a tool is safe for legal use. These include local processing, where data stays on your device, or encrypted storage within lawyer-centric platforms. If the platform does not explicitly state it protects privilege, assume it does not.

Safety and Privacy Concerns: Protecting Your Practice on Mobile Devices

A mobile device containing client data presents as a target to cybercriminals. You face mobile-specific threats: lost devices, public WiFi, insecure apps, and permissions creep. “Permissions creep” refers to apps requesting access to data they do not need, such as a flashlight app requesting access to your contact list. Like they say about using illegal drugs: “Just say no!”

You must implement non-negotiable protections. A biometric lock combined with MFA represents a good place to start. Face ID or a fingerprint scanner offers convenience as well as a strong barrier against thieves.

Use a virtual private network (VPN) such as NordVPN. Public WiFi offers no protection. If you connect to WiFi at a hotel or airport without a VPN, you put your communications at risk for interception. A VPN encrypts your communications, protecting them.

Conduct app permission audits regularly. Review what access your apps have. Revoke unnecessary permissions. Ensure you have secure backups so that a lost phone does

not mean a lost practice.

Before you install an app, you should check the developer's reputation, read the privacy policy, and pay for the product. "Free" apps often monetize your data. In the legal profession, paying for privacy is a cost of doing business. This principle aligns squarely with your ethical obligations concerning competence and mobile device security. You have a duty of competence that extends to the technology you use.

Build a Mobile Toolkit That Works as Hard as You Do

The smartphone is a deliberate part of your tech stack. It is not a toy. It is not a distraction. When curated intentionally, it becomes a powerful business engine.

Small improvements add up to significant productivity gains. Better time capture increases revenue. Safer communication builds trust. Quick AI support saves time. These marginal gains compound, giving the solo lawyer the agility to compete with larger firms.

We encourage you to test, secure, and customize mobile tools to support a modern, agile solo practice. Your phone lives in your pocket. Put it to work.

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),...

ABA American Bar Association | https://www.americanbar.org/groups/gpsolo/resources/ereport/2026-january/tapas-mobile-apps-every-solo-should-use/

TAPAs: Passkeys and Passwordless Securi for Solo and Small Firm Lawyers

Jeffrey M Allen and Ashley Hallene

Jul 07, 2026 8 min read

Summary

- **T**echnological **A**nd **P**ractice **A**dvice to help you become more efficient and effective. This month: modern cybersecurity techniques that can succeed where passwords fail.
- Instead of the fragile cybersecurity model of secret passwords, passwordless security rel cryptographic proof of possession.
- A passkey is a cryptographic credential created for a specific website or service and store securely on your device. The service stores a public key, while your device holds the priva
- Passwordless authentication reduces your susceptibility to phishing and other social engineering attacks—it depends less on you being perfectly attentive, perfectly skeptical, perfectly awake during a long workday.

iStock.com/vc

Jump to:

Every solo and small firm lawyer should understand risk management. We live with unmissable deadlines, client confidences we must protect, and professional obligations that leave little margin for error. Yet, many law practices continue to rely on a security model that should make us uncomfortable, as it has passed its "sell-by" date: the traditional password.

We have come to like passwords. They feel familiar and controllable. But they have significant fragilities. The most common ways malefactors gain access to law firm systems remain phishing, vendor data breaches, reused passwords, social engineering, and credential stuffing (a type of cyberattack in which attackers use usernames and passwords stolen from one breach to try logging into many other accounts, exploiting the fact that people often reuse the same credentials). Even "strong" passwords often fail, not because attackers have cracked them, but because they have tricked users into disclosing them.

For years, the standard advice has been predictable: use stronger passwords, use a password manager, and enable multifactor authentication (MFA). That advice still matters, but it no longer serves as the endgame. The security industry has started moving toward a new default: *passwordless authentication*, led by *passkeys* and phishing-resistant MFA.

What "Passwordless" Actually Means (and What It Does Not)

"Passwordless" does not mean you will never authenticate again. It does not eliminate identity verification. Instead, it means eliminating *shared secrets*—information that can be stolen, guessed, reused, or tricked out of you.

Traditional passwords constitute shared secrets. You know them, and the service knows them (or a version of them). If an attacker convinces you to disclose a password, the system has no reliable way to distinguish you from the attacker.

Passwordless security replaces that fragile model with *cryptographic proof of possession*. Rather than typing something you know, you prove that you possess something—typically a secure device such as your phone, laptop, or a hardware security key—and often also verify something you are, such as a fingerprint or facial scan, resulting in authentication that is dramatically more resistant to phishing and account takeover.

Passwordless authentication relies on a combination of:

- Passkeys
- Hardware security keys
- Biometrics used locally on a device
- Device-based authentication tied cryptographically to a specific service

Passkeys Explained in Plain English

A passkey is a cryptographic credential created for a specific website or service and stored securely on your device. It uses public-key cryptography: The service stores a public key, while your device holds the private key. The private key never leaves your device.

When you sign in, the service issues a challenge. Your device responds with cryptographic proof using the private key after you unlock it locally with a biometric (such as a fingerprint or facial scan) or a device PIN. The service never sees your biometric data, and there is no password to steal.

Passkeys are designed to be:

- Phishing-resistant
- Site-specific
- Non-reusable across services
- Immune to credential-stuffing attacks

Many passkeys can also sync securely across devices within a platform ecosystem, allowing you to authenticate on a new device by approving the login on a device you already trust.

Why Passkeys Matter to Lawyers

Passkeys do not simply represent a technology trend. They directly address problems lawyers face every day.

- **Lawyers serve as prime phishing targets.** Law firm email accounts provide significant value to malefactors. They offer access to client data, billing, trust accounting, document repositories, and client communications. Passkeys are inherently resistant to phishing because they only work on the legitimate site that created them. A convincing fake login page cannot use your passkey. Picture this: You are boarding a plane, juggling your phone and briefcase, when an authentication prompt pops up asking you to approve a sign-in you did not initiate. You pause—just long enough to realize that if you tap “approve” out of habit, you may grant an attacker full access to your email, client communications, and cloud systems before the boarding door even closes. Passwordless authentication, done correctly, reduces how often lawyers find themselves in that position.
- **Law practices are cloud-dependent.** Email, practice management platforms, document storage, e-filing systems, and client portals are overwhelmingly cloud-based. Identity security now represents the first and most critical line of

defense.

- **Solos and small firms generally lack a dedicated IT staff.** Anything that increases security while reducing daily friction is a win. Once configured, passkeys make logging in faster and easier—not harder.
- **Professional responsibility still applies.** Ethics rules rarely mandate specific technologies, but they require reasonable efforts to safeguard client information. What qualifies as "reasonable" evolves, and phishing-resistant authentication has increasingly evolved into a significant part of the baseline.

Practical Steps You Can Implement Now

Note: This topic is so important that we will provide several more tips than usual.

Tip 1: Start With Your "Crown Jewel" Accounts

You need not move every account to passwordless authentication at once. A phased approach works well. Start with the accounts that control access to everything else—your crown jewels:

- Primary business email
- Cloud identity providers
- Practice management systems
- Document management or storage platforms
- Financial and billing systems

Securing these accounts delivers disproportionate risk reduction.

TAPAs takeaway: If a service supports passkeys, enable them. If it does not, enable

strong MFA using an authenticator app or hardware key—not SMS/text messages. An **authenticator app**—such as Microsoft Authenticator, Google Authenticator, Duo Mobile, or Authy—is an app on your phone or computer that helps verify your identity by generating short-lived codes or sending push approvals during sign-in.

Tip 2: Use the Practical "Ladder"

Passwordless security is not all-or-nothing. Real-world environments require flexibility. Think in terms of a ladder:

- **Best:** Passkeys (no shared secret, phishing-resistant)
- **Excellent:** Hardware security keys (phishing-resistant MFA)
- **Good:** Authenticator app codes or push approvals
- **Avoid when possible:** SMS/text message codes

You should actively move away from SMS-based MFA for your most important accounts. Think of SMS as one of those miniature spare tires: better than nothing, but not how you want to drive every day. You take an unnecessary risk if you continue to rely on SMS text messages for email MFA in 2026.

Tip 3: Treat Passkeys as the Default, Not an "Extra"

A useful mindset shift treats passkeys as the default login method rather than an added layer.

Passkeys remove two common failure points:

- You no longer need to remember or type passwords.
- You are far less likely to be tricked into authenticating on a fake site.

Use passkeys whenever you can. When you cannot, fall back to a hardware key or authenticator app.

Tip 4: Add Hardware Security Keys for Redundancy

Hardware security keys remain one of the strongest authentication tools available. They do not depend on phone access, cellular service, or battery life. A hardware security key is a small physical device—usually USB-C, USB-A, or NFC-enabled—that verifies your identity by cryptographically proving you have the trusted key, making it far more phishing-resistant than passwords or text-message codes. Most look like tiny USB dongles or key fob tokens; common brands include Yubico, Google Titan, FEITIAN, and Kensington, and prices typically range from about $30 for basic keys to $100 or more for biometric models.

Tip 5: Follow the Two-Device Rule

Some users or potential users worry about self-inflicted lockout with passwordless security. Yes, it poses that risk; good planning provides the response.

Ensure that at least two independent authentication methods can access each critical account. For example:

- Phone passkey + laptop passkey
- Phone/laptop passkey + hardware security key
- Primary authenticator app + backup method (preferably a hardware key, second trusted device, or offline recovery codes—not SMS if avoidable)

Before disabling passwords, test recovery options whenever possible. Store recovery codes offline in secure locations. You want redundancy for your protection. Document your process the way you document trust accounting procedures.

TAPAs takeaway: Passwordless security does not come as a “set it and forget it”

package. You need to set it and back it up.

Tip 6: Clean Up Password Habits During the Transition

Passwordless does not eliminate passwords overnight. While transitioning:

- Use a password manager for your remaining password-based accounts.
- Eliminate password reuse completely.
- Use long, unique passwords (not less than 12 characters including upper- and lower-case letters, numbers, and symbols).
- Remove old, saved browser passwords.
- Close unused or dormant accounts.

You may think of this work as boring. You need to think of it as essential.

Tip 7: Do Not Forget Client Portals and Intake Systems

Lawyers often lock down internal systems while overlooking outward-facing tools:

- Client portals
- Intake forms
- Secure messaging platforms

These systems often contain sensitive information and may provide entry points into broader systems. Where available:

- Require MFA.
- Use role-based permissions.
- Eliminate shared logins.
- Periodically review access logs.

Stronger authentication improves security for clients and lawyers.

Tip 8: Write a Simple Identity Incident Plan

Even good systems fail. Phones and other devices, keys, and other things get lost or stolen. Such events can cause a failure of your systems.

Every practice should have a simple identity incident plan that addresses:

- What happens if a device gets lost or stolen?
- How do you revoke access immediately?
- How do you restore access securely?
- How do you review recent account activity?

Write the plan down. Test it regularly and often (at least every six months). You will sleep better knowing that you have it in place.

A practical plan includes:

- Immediate containment (remote lock/wipe if available)
- Revoking active sessions
- Removing compromised devices or passkeys

- Resetting remaining credentials where passwords still exist
- Reviewing activity logs
- Notifying as appropriate
- Documenting what happened and what changed

Tip 9: Train for "Approval" Phishing

Passwordless security reduces many risks, but it does not eliminate human judgment.

Train yourself and any staff to:

- Question unexpected login approval requests.
- Slow down when messages feel urgent.
- Deny and investigate when context does not make sense.

Modern phishing often tries to trick users into approving a login rather than surrendering a password.

TAPAs takeaway: One of the most dangerous phrases in security today is, "I just hit approve because I was busy."

Tip 10: Make It Stick with a Quarterly Authentication Checkup

Security improvements decay without maintenance. Vendors change settings. Devices get replaced. Staff roles evolve. Personnel changes.

Put a recurring quarterly "authentication checkup" on your calendar. During that checkup, work through this integrated checklist:

- Enable passkeys for business email.
- Enable passkeys for your Microsoft or Google identity account.
- Replace SMS MFA with authenticator apps or hardware keys.
- Apply the two-device rule to all crown-jewel accounts.
- Store recovery codes offline.
- Require MFA for client portals where possible.
- Eliminate shared logins.
- Maintain a current identity incident plan.
- Train yourself and staff to deny unexpected approvals.
- Confirm that you have scheduled a recurring quarterly checkup.

That checklist is the bridge between good intentions and operational security. Don't just look at the checklist and say to yourself, "yep, we did that. . . ." Test each part to ensure that it still works. If not, make the necessary adjustments to ensure that it does.

Ethical and Professional Responsibility Considerations

Rules of professional conduct require lawyers to make reasonable efforts to safeguard client information. Although no rule yet mandates passkeys, law firms that knowingly rely on weaker methods despite readily available alternatives may find that position harder to defend after an incident.

Adopting phishing-resistant authentication aligns with confidentiality duties, technological competence obligations, and sound risk management.

This is not about being perfect. It is about being prudent.

Final Thoughts: Security That Works *with* You

Passwords fail because they require users to be perfect—never rushed, never distracted, never fooled. Passwordless authentication succeeds because it reduces temptation and error—and if security depends less on you being perfectly attentive, perfectly skeptical, and perfectly awake during a long workday, we will happily call it a design feature.

Passkeys and related technologies have no magic, but they represent meaningful progress. For solo and small firm lawyers endeavoring to balance efficiency with professional responsibility, they are worth adopting now—on your terms, at your pace, with a plan.

Now, that gives you some Technological And Practice Advice worth following!

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/gpsolo/resources/ereport/2026-july/tapas-passkeys-passwordless-security-solo-small-firm-lawyers/

A True Story of a Grandparent "Kidnappi Scam

Jeffrey M Allen

Mar 14, 2026 7 min read

Summary

- Scammers exploit fear and technology, using AI to convincingly impersonate loved ones a pressure victims into sending money.
- Always verify emergency claims independently before acting—never let panic dictate you response.
- Protect yourself by limiting the personal information you share online, establishing famil words, and staying informed about evolving scam tactics.

istock.com/

Jump to:

Scam of the Month Column

On an otherwise ordinary day, the phone rang, and on the other end was a voice so filled with panic—crying, shaking, and barely able to speak—that it immediately evoked a sense of dread.

Abruptly, a second voice interjected: deep, composed, and menacing. "If you ever wish to see your daughter again, you will comply with my instructions. Do not contact law enforcement. Do not reach out to anyone else. Secure the funds immediately." This scenario did not originate from a cinematic script or a literary work; instead, it transpired in reality, exemplifying a pernicious scam that has become increasingly prevalent in contemporary society. Although anyone may fall victim, these schemes disproportionately target older adults, particularly grandparents.

These fraudulent operations, commonly called "grandparent scams" or "virtual kidnapping scams," do not involve an actual abduction. Instead, they exploit the victim's emotional vulnerability, instilling a profound sense of fear through sophisticated psychological manipulation. The potency of this fear frequently compels individuals to deplete their savings, remit substantial sums to perpetrators, and act precipitously—often foregoing the critical step of verifying the threat's authenticity.

A Terrifying Call That Sounded All Too Real

One of the most thoroughly documented and unsettling instances occurred in Arizona in 2023. Jennifer DeStefano received a call from an unfamiliar number at her residence. Upon answering, she heard her fifteen-year-old daughter, Briana, speak. The voice,

consumed by hysteria, cried out, "Mom, I messed up." The palpable panic and distress in each utterance sent Jennifer's heart racing. Before she could inquire further, the caller's voice shifted, and a man asserted that he had kidnapped her daughter, threatening harm should Jennifer contact authorities or anyone else.

The extortion commenced with a demand for an exorbitant $1 million ransom. When Jennifer expressed shock, the perpetrator reduced the amount to $50,000—a sum still considerable, yet now presented as "reasonable" by comparison. The caller maintained continuous pressure, issuing threats and insisting upon immediate action. What rendered the situation particularly convincing was the initial voice, which Jennifer was certain belonged to her daughter.

In reality, nobody had abducted Briana. The scammer had employed artificial intelligence to fabricate a voice indistinguishable from Briana's. By acquiring audio samples—potentially from social media or video recordings—the perpetrator utilized advanced AI voice cloning technology to simulate Briana's voice in a state of distress, producing an alarmingly authentic effect. Fortunately, Jennifer had her family nearby, and they promptly contacted Briana directly, confirming within minutes that she remained safe at school and that no one had kidnapped her. No abduction had occurred—only a highly sophisticated scam

Jennifer subsequently shared her ordeal publicly, seeking to alert others to the increasing realism and persuasiveness of such schemes.

Mechanisms Underlying "Kidnapping" Scams

These scams rely upon emotional manipulation—leveraging fear, urgency, and familial affection to coerce victims. Scammers typically begin by identifying older adults with children or grandchildren, gathering information from public records, social media platforms, or commercial data brokers. Even innocuous Facebook posts can divulge critical details regarding family relationships, names, educational institutions, and travel itineraries.

Once the scammers have identified a target, they initiate the fraudulent call. Earlier iterations of the scam involved the caller impersonating a grandchild and making vague statements such as, "Grandma, I'm in trouble," relying on the victim to infer which

grandchild had called. However, technological advancements have now rendered these deceptions far more convincing

After the scammers set the emotional hook, they use manipulative tactics to reel in the victim.

Modern scammers possess the capability to:

- Spoof telephone numbers to appear local or familiar
- Utilize AI-generated voices that precisely mimic loved ones
- Transmit fabricated photographs or videos as "proof" of a kidnapping
- Research family specifics to enhance credibility

The scammers' overarching objective: to overwhelm the victim's logical faculties, preventing them from verifying the claims.

Enduring Emotional Consequences

Monetary losses can have devastating consequences for victims. Some individuals have forfeited thousands—or even tens of thousands—of dollars in a single incident. For retirees dependent on fixed incomes, such losses may deplete emergency reserves or life savings. The Federal Bureau of Investigation has documented billions of dollars lost annually to scams targeting older adults, with family-emergency schemes ranking among the most emotionally impactful.

Leah Foley, U.S. Attorney for Massachusetts, described how many victims not only lost their savings but also their sense of safety, judgment, and trust in the world around them. She also stated that: “These scams are not just financially devastating; they are emotionally traumatizing.” For seniors living on fixed incomes, losing thousands of dollars can be devastating, and many are too ashamed to report being duped, meaning the true toll may be even higher.

Recent Data and Trends

Virtual kidnapping scams have surged in recent years, evolving alongside technological advancements. According to the FBI's Internet Crime Complaint Center (IC3), extortion-related complaints—including virtual kidnappings—increased significantly between 2022 and 2023. In 2023 alone, IC3 received 880,418 complaints, with losses exceeding $12.5 billion—a 22% rise in financial losses compared to the previous year. The sophistication of these scams has grown, with perpetrators leveraging AI technology to simulate the voice of a victim's loved one, making the scam even more believable and harder to detect.

Law Enforcement's Perspective

The FBI and other agencies have issued numerous advisories regarding virtual kidnapping scams. Frequently, they have no tangible crime scene to investigate, no missing person to locate, and no actual hostage, all of which complicate the investigative process. The proliferation of technology among scammers has heightened official concern, with tools such as AI voice cloning, manipulated imagery and video, and real-time pressure tactics now commonplace.

According to FBI alerts, scammers increasingly employ altered "proof of life" media—photos, audio clips, and videos that purport to depict an individual in jeopardy. In reality, these fabricated materials render the scams far more plausible than their predecessors. Authorities urge individuals to remain vigilant, verify claims independently, and report all attempts, regardless of the financial outcome.

Legal and Regulatory Information

Victims of scams have several avenues for recourse. If you suspect a scam, immediately contact your local police or sheriff's office, your state attorney general, and report the fraud to the Federal Trade Commission (FTC). For older adults, Adult Protective Services can provide additional support. Legal aid offices and pro bono initiatives, such as the Scam Justice Legal Clinic, offer free legal assistance to victims of online scams, helping them understand their rights and options for recovery. The Consumer Financial

Protection Bureau and the FTC provide resources for reporting and recovering from scams, including steps to reverse fraudulent transactions and protect personal information.

Technology Deep Dive: How AI Voice Cloning Works

AI voice cloning scams involve criminals using artificial intelligence to clone a real person's voice and make fake calls that sound real. Scammers comb through social media, voicemail greetings, and videos to find audio clips of a person's voice, then use AI to make it say whatever they want. Even a few seconds of audio can enable the AI to generate convincing speech. Scammers can use synthesized voices to create fake messages or live calls, often paired with spoofed caller IDs to make the calls appear legitimate. Experts recommend limiting public access to recordings of family members' voices and establishing a family code word for emergencies

Expert Commentary

Federal investigators and cybersecurity experts warn that criminals now use artificial intelligence to create fake "proof-of-life" photos and videos, pressuring panicked families into paying ransoms for loved ones not actually in danger. FBI Special Agent Matt Horton explains, "With a combination of fear and stress and pressure, it just has to be enough to make the family believe." Cybersecurity professionals emphasize that knowledge has become the first line of defense, and urge families to be cautious about what they share online and to verify any emergency claims independently.

Global Perspective

Virtual kidnapping scams have become a global phenomenon, with cases reported from Hong Kong to Mexico City, Vietnam, and beyond. In Latin America, Mexico serves as a hub for virtual kidnappings, with organized gangs and opportunistic criminals targeting both locals and foreign nationals. In Asia, Vietnamese authorities have warned of a rising wave of sophisticated online scams targeting students and young

people living away from home. The tactics and prevalence of these scams vary by region, but the underlying psychological manipulation and use of technology are consistent worldwide.

Victim Support and Recovery

If scammers have targeted you or someone you know in a grandparent or virtual kidnapping scam, seek support. Organizations such as the FBI's Internet Crime Complaint Center (IC3), the Federal Trade Commission (FTC), and local law enforcement agencies can provide guidance on reporting and recovering from scams. Additionally, groups like AARP offer resources for emotional and financial recovery, helping victims navigate the aftermath of these traumatic events.

Report scams through SLD's Reporting page.

Practical Strategies for Safeguarding Against Scams

Fortunately, several straightforward practices can effectively thwart most of these fraudulent schemes:

Checklist for Preventing Virtual Kidnapping Scams

- Limit what you share on social media, especially travel plans, family details, and voice recordings.
- Turn on built-in message filters on your phone to block scam texts and calls.
- Use strong passwords and enable two-factor authentication for online accounts.
- Establish a family code word known only to trusted relatives for emergencies.
- Always verify claims independently by contacting the purported victim or another family member.

- Never send money, gift cards, or wire transfers after a phone call.
- Report all scam attempts to the FBI's Internet Crime Complaint Center (IC3) and the FTC.
- Stay informed about the latest scams by signing up for alerts from organizations like AARP Fraud Watch Network.

Personal Reflection and Call to Action

The rise of virtual kidnapping scams underscores the urgent need for vigilance, education, and community support. Share this information with your loved ones, especially older family members, and encourage open conversations about scam prevention. By staying informed, verifying claims, and utilizing available resources, we can protect ourselves and our families from these emotionally devastating crimes.

Conclusion

The cruelty inherent in grandparent "kidnapping" scams stems from the weaponization of love. Rather than appealing to greed, these schemes exploit the profound fear for the safety of cherished individuals. As technological capabilities advance, the realism and efficacy of such scams will likely intensify. The ordeal Jennifer DeStefano endured illustrates the remarkable persuasiveness of these tactics—even among intelligent and cautious individuals—but also demonstrates the efficacy of verification. A single, timely phone call spared her family from financial loss and terminated the scam. The paramount lesson: pause, ascertain the facts, and never allow panic to dictate financial decisions.

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...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-march/grandparent-kidnapping-scam/?utm_source=chatgpt.com

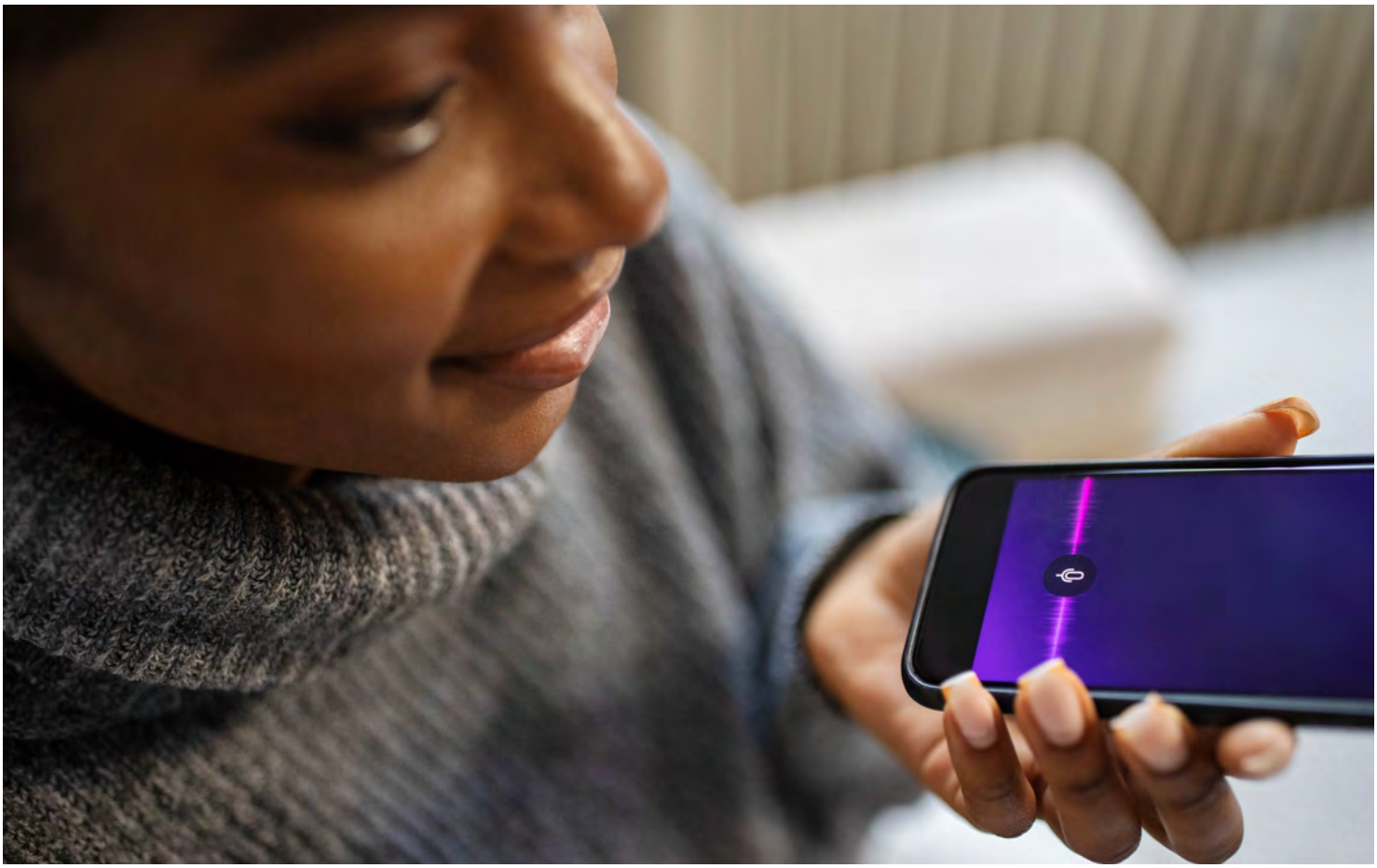
The Rise of the AI-Cloned Voice Scam

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

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...

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 bai steal identities and bill for unnecessary services.
- Victims face financial, medical, and long-term identity risks—even if they don’t pay direct 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 G

Jump to:

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 of skepticism, older adults can protect themselves and avoid becoming the next victim of

a “free” genetic test that costs far more than the price.

For lawyers counseling seniors or handling elder-law matters, this scam underscores the need to educate clients about:

- Protecting their Medicare identity.
- Understanding legitimate medical testing pathways.
- Recognizing high-risk fraud patterns tied to health technology.

This is a Medicare scam that every practitioner should be aware of—and every senior should be warned about.

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...

ABA American Bar Association | https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-january/medicare-scam/

The Benjamin Wood Scam After Hurricane Harvey

Jeffrey M Allen

Oct 15, 2025 5 min read

Summary

- Always verify the credentials of contractors before hiring them, especially after a disaster.
- If you suspect fraud, report it to the authorities immediately.
- Offer support and resources to those affected by contractor scams.

istock.com/shaunl

Perhaps we should call this month's installment the "scammer of the month" instead of the "scam of the month." It depends on your perspective and how you view assembly line scamming.

Hurricane Harvey wasn't just one of the costliest natural disasters in U.S. history—it was also one of the most devastating for the Houston area's sense of normalcy. In late August 2017, the storm stalled over southeast Texas, dumping over 50 inches of rain in some areas. It flooded entire neighborhoods. Families lost homes, cars, and decades of accumulated possessions. When the floodwaters finally drained, the hard part began: rebuilding. As Hurricane Harvey's floodwaters receded, Houston's contractor market underwent a dramatic transformation overnight. What was once a competitive landscape became a desperate scramble for resources.

That's when the scammers came.

Amidst the chaos, Benjamin Andrew Wood, a local contractor, saw an opportunity—not to help, but to take. He created a textbook example of post-disaster contractor fraud on an assembly line: high-pressure pitches, upfront deposits, promises of quick repairs,

and then… nothing. By the time prosecutors caught up with him, Wood had left behind a long trail of unfinished jobs, bad checks, unpaid suppliers, and disillusioned victims.

In February 2020, Wood pleaded guilty to aggregate theft in Harris County, Texas. The scope of the fraud? $180,000 stolen from 26 victims, mostly Harvey survivors struggling to rebuild. The court sentenced him to 10 years in prison, requiring that he serve that term concurrently with another 10-year sentence from neighboring Montgomery County for similar conduct. This wasn't a one-off dispute over shoddy work; it represented a deliberate, repeated scheme that preyed on people at their most vulnerable.

In the immediate aftermath of Harvey, Houston's contractor market flipped overnight from competitive to desperate. Tens of thousands of homes needed gutting, mold remediation, and rebuilding—often all at once. Licensed, reputable contractors get booked out for months. Many homeowners with children, elderly relatives, or medical needs felt they could not wait.

Scammers count on that sense of desperation and urgency. Wood advertised himself as a local, "veteran-owned" business, labels that carried powerful trust signals in a community that respected military service. For many people, that alone proved sufficient for them to assume honesty.

According to prosecutors, Wood didn't just take on one or two jobs he couldn't handle. He systematically lined up dozens of projects across Harris and Montgomery counties, collecting large upfront payments on the promise of fast mobilization. Some homeowners reported he showed up once or twice with small crews to create the appearance of progress. Others said he never returned after the deposit cleared.

While homeowners waited for work to begin, Wood allegedly wrote worthless checks to suppliers—checks drawn on closed accounts. That meant even when ordered, materials did not get delivered, or they arrived only after suppliers threatened to file liens against the victims' homes.

Wood's scheme lasted so long, in part, due to the fragmentation of victims in a post-disaster environment. Harvey displaced people across multiple neighborhoods and counties. Each family was juggling insurance claims, FEMA applications, and temporary housing arrangements. It was easy to assume you just got "unlucky" with your

contractor—until someone connected the dots.

Prosecutors eventually did just that. The Harris County District Attorney's Office consolidated over two dozen cases into one prosecution. This aggregation was critical; in Texas, reaching certain monetary thresholds can elevate theft to higher felony levels, which carry stiffer penalties and increase the likelihood of prison time.

While the $180,000 in financial loss was the primary claim, the real damage extended beyond dollars.

Lost Time and Secondary Damage – Delays meant homes remained exposed to Houston's humid climate. Mold spread, drywall warped, and wooden framing deteriorated. Insurers can—and sometimes do—argue that coverage does not extend to such secondary damage, if it could have been mitigated. The scam deepened victims' losses and jeopardized their insurance claims.

Liens and Legal Headaches – Because Wood's checks to suppliers bounced, some homeowners faced the threat of mechanics' liens for unpaid materials, even though they had already paid the contractor. Clearing these liens often requires additional legal expense.

The Emotional Toll – For people who had endured displacement and loss, realizing they had been defrauded proved emotionally crushing. Prosecutors described Wood's actions as targeting people in their "darkest hour." That sense of betrayal—especially from someone presenting as a trusted veteran—left emotional scars long after the legal case ended.

Wood's case illustrates a broader truth: *disasters don't just destroy homes; they warp markets and shortcut trust.*

Supply Shock – Demand for skilled labor surges overnight, outpacing legitimate supply. Homeowners feel lucky to find anyone available.

Liquidity Influx – Insurance checks and FEMA grants put large sums into the hands of people who likely never managed a construction project before.

Information Gaps – With government offices overwhelmed, licensing checks and

complaint records may prove harder to access.

Trust Shortcuts – Signals like “local,” “church-connected,” or “veteran-owned” bypass the skepticism that normally protects consumers.

If you’re an attorney advising clients after a disaster—or managing your own post-disaster repairs—the Wood case offers clear takeaways:

Paper First, Payment Second – Never let urgency override documentation. Get the license number, insurance certificates (from the carrier, not the contractor), and written scope of work before paying a cent.

Control the Cash Flow – Keep deposits small (10–30%), tie payments to verified milestones, and use joint checks to suppliers to prevent diversion of funds.

Watch the Lien Clock – Know when suppliers must be paid to avoid lien rights, and demand lien waivers with every progress payment.

Keep Communication Discoverable – Email is often more effective than text for key approvals. If litigation becomes necessary, you’ll want an easy-to-produce record.

Treat Credibility Signals Neutrally – Military service, religious affiliation, or neighbor recommendations don’t replace license verification.

Escalate Early – At the first sign of delay without explanation, freeze payments and involve your insurer or legal counsel. Early reporting can help prosecutors build a comprehensive case, such as the one that ultimately led to Wood's conviction.

Remain Vigilant- The aftermath of Hurricane Harvey left many victims in its wake. A key takeaway from any post-disaster situation is the importance of remaining vigilant and informed to avoid falling prey to scams during times of crisis.

When Harris County prosecutors announced Wood’s sentence, they framed it as a warning to would-be scammers: exploiting disaster victims isn’t “just a civil matter.” It’s a criminal act that can carry serious prison time.

That message is essential for prevention. Many scam victims assume law enforcement can’t—or won’t—intervene in contractor disputes. But as Wood’s 10-year sentence

shows, when there's a pattern of fraudulent conduct, criminal prosecution is not only possible, it's the right tool to protect the public.

Benjamin Wood offers more than a local crime story—it's a cautionary tale that will repeat after the next hurricane, wildfire, or flood, unless homeowners and their advisors act differently. In disaster recovery, urgency is the scammer's greatest weapon. The more you feel pressured to sign now, pay now, or skip steps "just this once," the more you should slow down.

Attorneys hold a unique position to help clients guard against that urgency trap—by insisting on verification, controlling payments, and keeping a clean, contemporaneous paper trail. Wood's victims didn't get those safeguards in time, but their persistence in coming forward ensured he was held accountable. And their story can help others avoid becoming the next chapter in a long, sad pattern.

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...

American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-october/benjamin-wood-scam/

GPSolo Magazine GPSolo, May/June 2026 (43:3): What to Do When . . .

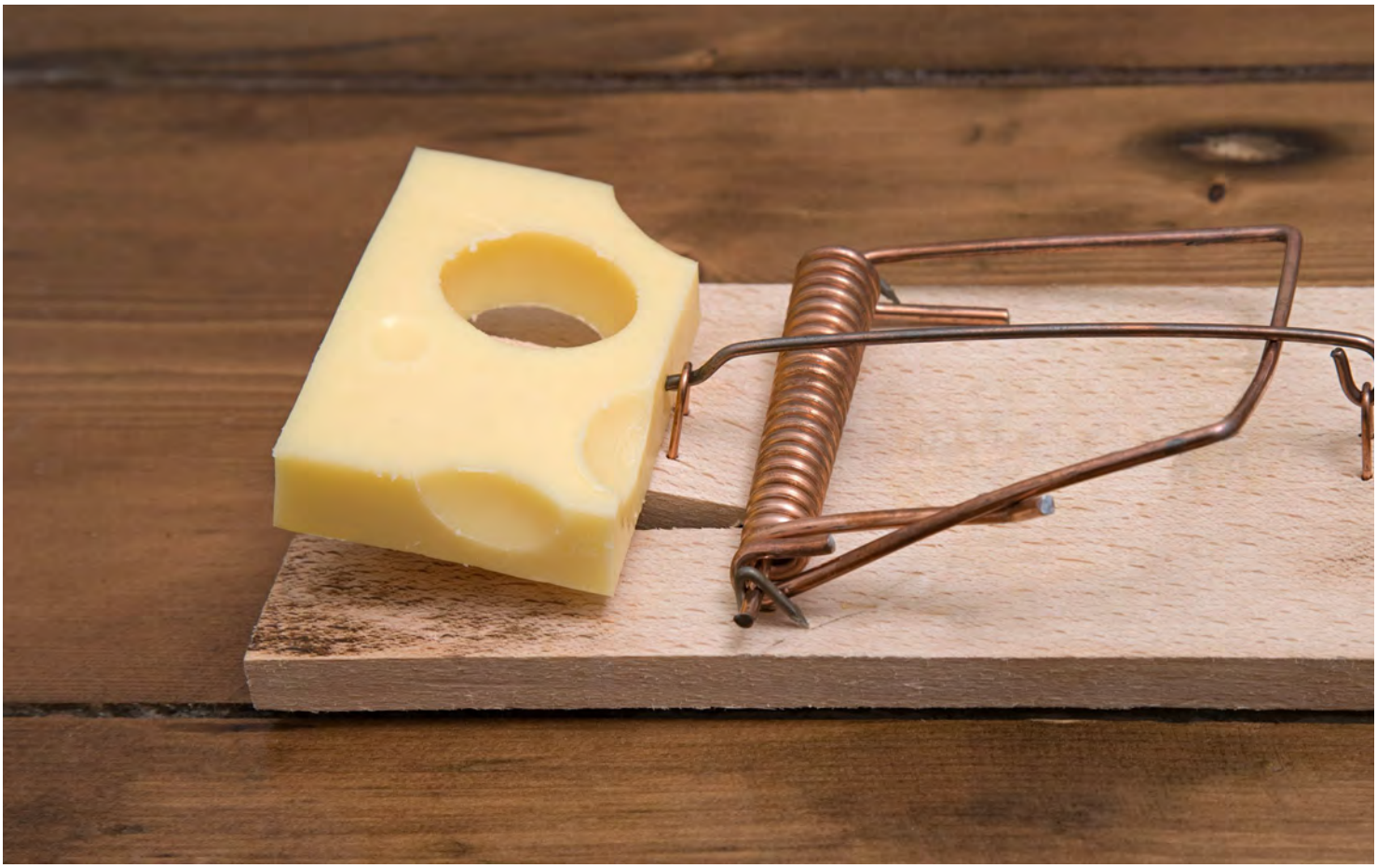
How AI Is Reengineering Scams Aimed at Lawyers

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:

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...

American Bar Association |
https://www.americanbar.org/groups/gpsolo/resources/magazine/2026-may-jun/how-ai-reengineering-scams-aimed-lawyers/?utm_source=chatgpt.com

GPSolo Magazine GPSolo, May/June 2026 (43:3): What to Do When . . .

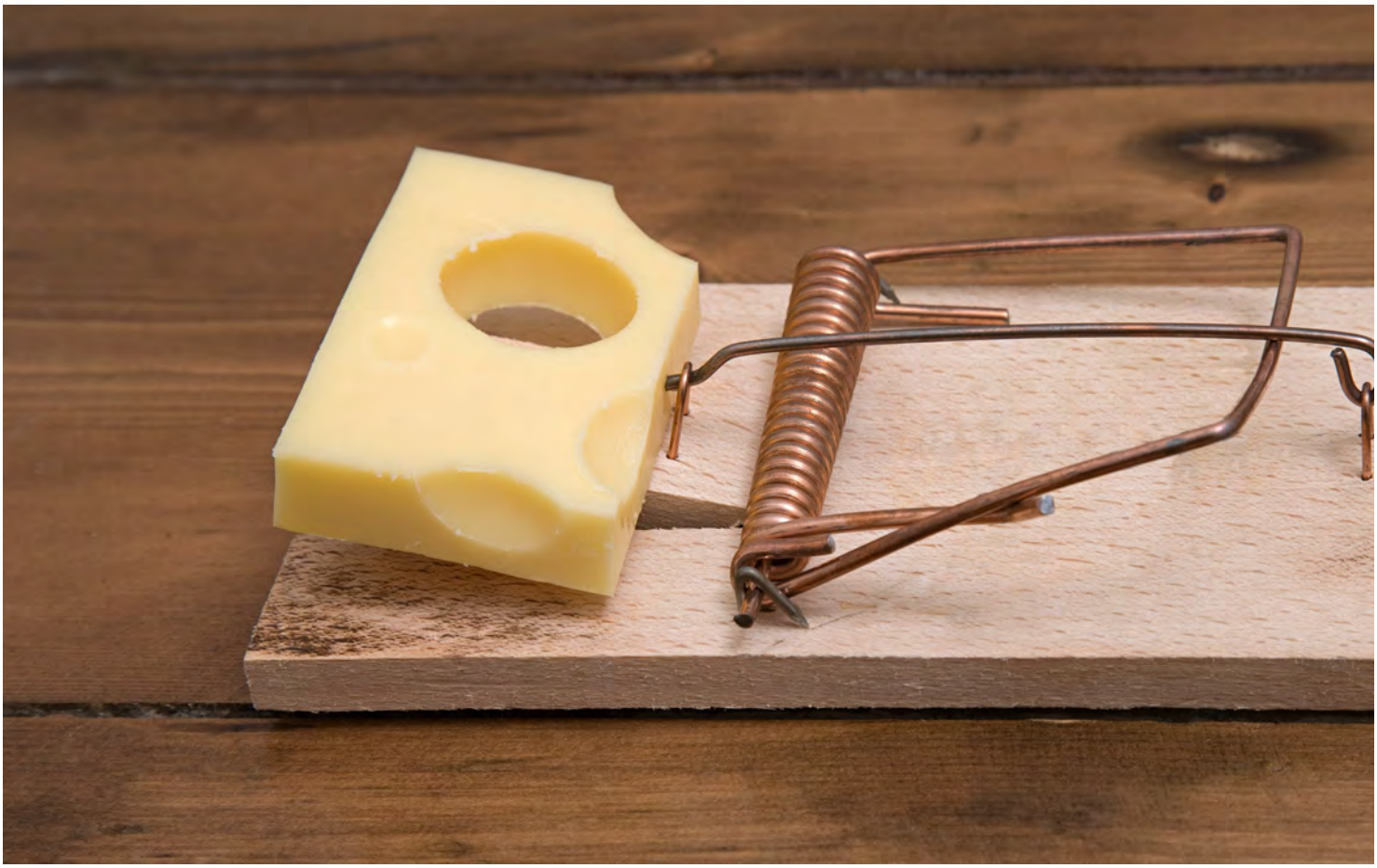
How AI Is Reengineering Scams Aimed at Lawyers

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:

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...

American Bar Association | https://www.americanbar.org/groups/gpsolo/resources/magazine/2026-may-jun/how-ai-reengineering-scams-aimed-lawyers/?utm_source=chatgpt.com

What Scams are Supported by AI?

Jeffrey M Allen and Ashley Hallene

Sep 22, 2024 7 min read

Summary

- AI has caused many changes in the world, and it will continue to impact us in many ways and have a ripple effect that will reach virtually every aspect of our personal and professional lives.
- The Senior Lawyers Division has identified scams as a major concern and will emphasize that concern in its activities during the current bar year.

iStock.com/Tess_Trunk

You have undoubtedly heard of the Industrial Revolution, the first of the more recent technological revolutions. When we started to write this article, we did a bit of research about the technological revolutions that have occurred in the last 300 years as a lead into this column. To our surprise, we learned that some writers say we have had three and now find ourselves in the fourth, while others say we find ourselves in the sixth. Exploring those differences and the full history of technology revolutions exceed the scope of this article.

If you prefer to think in terms of “Ages” rather than “Revolutions,” think of AI as the latest evolution of the Information Age, which has converted information into a commodity capable of rapid and wide distribution, usually using computers and related technology.

Whether you like to think in terms of “Ages” or “Revolutions,” the increasingly rapid development of artificial intelligence has created the latest. AI has caused many changes in the world, and it will continue to impact us in many ways and have a ripple effect that will reach virtually every aspect of our personal and professional lives.

In previous columns, we talked about the duality of technology in general and AI in particular. By “duality,” we refer to the fact that technology and AI are present as a double-edged sword. Cutting one way can benefit us in untold ways; cutting the other can cause damage ranging from minor to catastrophic in its impact. These benefits and detriments exist at all levels, including personal, professional, business, and, ultimately, societal. In this column, we will focus on AI and its ability to fuel or support scams, particularly since the release of ChatGPT and the expansion of generative AI (GenAI).

AI currently comes without a moral compass and does the work assigned to it by humans. Unfortunately, humanity includes many bad actors. Many have acquired technological proficiency that enables them to capitalize on the AI’s functionality in ways that facilitate taking advantage of others using one of many techniques we refer to collectively as “Scams.”

A recent article in the *San Francisco Chronicle* (February 11, 2024, Section A, Page 7) discusses one example of this problem. That article, “Feds Targeting AI Scam Calls” by Chase DiFeliciantonio, identifies robocalls using AI technology to generate voices as the number one consumer complaint. The calls sometimes sound like a famous or familiar person. The technology uses both audio and text messaging. A Truecaller/Harris Poll cited in the article found that “[t]he number of phone scam victims in the U.S. nearly tripled between 2017 and 2022.” The article also notes that the FCC revealed that in 2022, fraudulent calls and texts generated $1.13 billion in known losses.

The bad guys have used the technology to fool voters, to try to collect utility bills falsely claimed as “unpaid,” to imitate the voices of other family members and friends in pleas for financial assistance for innumerable reasons, and a myriad of other schemes. This scam, often called the “grandparents’ scam” because it has proven successful when used to contact grandparents pretending to be a troubled grandchild, preys, particularly on the elderly, trying to convince grandparents that a grandchild needs their help for a variety of reasons running the gamut from transportation issues to needing bail money. It does not limit itself to grandparents and the elderly, however, and one does not need to have reached a minimum age to acquire vulnerability or to become a target.

Respecting billing issues, we have seen calls purporting to come from utility companies,

insurance providers, and government agencies respecting allegedly unpaid bills.

The Senior Lawyers Division has identified scams as a major concern and will emphasize that concern in its activities during the current bar year. It recently approved a book on scams that should be available early next calendar year. In the interest of full disclosure, we will edit that book, which will be a compilation of contributions from several authors. We will also contribute to it as authors.

In the bad old days, most of these scams existed but ran using a human making a call and trying to sell themselves as whatever the fraud required. Some people have an acquired ability to mimic the voices of others. Many entertainers support themselves by imitating famous people. As good as some have been, AI does it much better. AI can produce an almost perfect replication of the voice of another. Unlike humans, who require time and practice to mimic a voice well, AI can take a few voice samples and instantly create its version. Some of these scams can and do still work without AI. For example, it does not take an AI voice imitation to present as a representative of a government agency or a utility company. They can sound like anybody and make the play. Selling oneself as a close friend or relative poses a far more difficult proposition as the victim will be familiar with this voice. However, the availability and evolution of AI made those scams more common by creating the ability to use an AI representation to make many calls in a short time frame, far more than one or a handful of people could make on their own.

Some scams would never have worked well before the recent evolution of AI. For example, a recent scam used an excellent AI-generated imitation of President Biden's voice to call voters and discourage them from voting in the New Hampshire Primary.

The voter scam tipped the balance, and now, the Attorneys General of 26 states have asked the FCC to clamp down on this abuse. The FCC responded by outlawing robocalls using AI-generated voices. We support the FCC's action, but we do so, tongue in cheek. While this seems like a step in the right direction, outlawing AI-generated robocalls does not mean they will stop. It only means the government can prosecute those who do it and get caught.

Efforts to stop or limit robocalls, scam telephone calls, and even calls by live people trying to sell you a product or service that may or may not be legitimate have generally

and regularly failed. How many of you used the “Do Not Call” system to prevent calls from telemarketers? How many of you stopped getting them? You can get software to help you reduce such calls on your mobile phone, but the technique has not stopped them. The situation has reached the point that we get multiple calls of this nature every day. We have reached the point that we will not answer the phone unless the caller has a caller ID and is a person or is calling from a number we recognize. If we miss a call we need to get, the caller will likely leave a message, and we can call back, if appropriate.

Given that you will likely continue to get such calls and texts, you should protect yourself as much as possible. While you cannot stop the calls from coming, you can act to reduce your exposure to them and your susceptibility. We do not intend the following as a comprehensive list of everything you can do to protect yourself. An exhaustive list would require more space than we have available. We do, however, recommend that, at a minimum, you follow these suggestions and remember that avoiding scams always involves vigilance, work, and a healthy dose of skepticism and that the use of AI, particularly GenAI, makes that even more imperative:

1. Learn about and keep current with common AI scams and deceptive practices. The scams change over time, and new scams come out, so this is not a once-and-done situation. You protect yourself much better by remaining current in your knowledge. In a shameless plug, we recommend you read the Scams book that the SLD will publish, as it will help you learn about, understand, and keep current in this area to enable you to protect yourself better.

2. Learn the capabilities and limitations of AI technology to help you recognize a possible fraudulent claim or other scam.

3. Carefully examine claims and offers respecting products and services, particularly those related to AI technology, products, or services. Verify credentials, qualifications, and the reputation of individuals and organizations making such claims. Look for and check out independent reviews, testimonials, and expert opinions respecting the legitimacy of the claims and products. Be cautious about such reviews and limit your search to trusted reviewers. Anyone can generate a review or a YouTube video about a product. Not all such reviewers have much by way of qualifications or expertise; some may have AI as their authors. Be cautious of AI-related offers promising unrealistic

outcomes or guaranteed results. Remember that if an offer seems too good to be true, it probably is.

4 Research the entity offering the products or services; again, exercise extreme caution when dealing with products or services provided using AI technology. Check their website, social media profiles, and online presence. Assess their credibility. Review customer feedback; take that with a grain of salt, as vendors can fake customer reviews or publish a carefully curated group of mostly favorable reviews (a clever approach is to include a few negative reviews to make the rest look credible). We look at customer feedback but rely more on independent reviews. Look for red flags such as lack of contact information, negative reviews, or suspicious business practices.

5 High-pressure sales tactics and aggressive marketing techniques commonly occur in scams. View attempts to pressure you to make immediate decisions or investments without providing adequate time for research or due diligence as a red flag. Consult independent experts, professionals, and trusted advisors before deciding on AI investments, purchases, or partnerships. Obtain objective opinions and advice from individuals knowledgeable about AI technology and its application. Look for certifications, accreditations, and industry affiliations that validate the legitimacy of AI-related products or services. Verify whether the company or individual offering AI solutions has received recognition from reputable organizations or industry associations.

6 Avoid sharing personal information, such as Social Security numbers, bank account details, or passwords, unless you have verified the offer's legitimacy and trust the entity requesting the information. Remember, once the bad guys get your information, they will likely use it themselves and monetize it by selling it to others on the Dark Web.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2024-september/what-scams-are-supported-by-ai/?utm_source=chatgpt.com

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:

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...

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

GPSolo Magazine GPSolo March/April 2025 (42:2): AI for Lawyers

Ethics in AI-Assisted Lawyering: Whose C It Anyway?

Ashley Hallene

Apr 01, 2025 9 min read

Summary

- Artificial intelligence (AI) systems introduce numerous ethical challenges for lawyers, mos notably regarding confidentiality, accountability, and bias.
- The lawyer's duty to supervise AI tools is firmly rooted in ethical rules, such as the Ameri Association (ABA) Model Rules of Professional Conduct governing the oversight of nonlav assistants.
- While technology can offer valuable support, it is the lawyer who must make the final cal matters of strategy, ethics, and client advocacy.
- Clear policies for oversight, transparency, and accountability reinforce the principle that technology supports but does not replace the human element of lawyering.

filo/E+ via G

Jump to:

Artificial intelligence (AI) is reshaping the practice of law, providing tools for data analysis, outcome prediction, and task automation. From AI-driven legal research

platforms to automated contract review systems, technology is enabling lawyers to focus more on strategic thinking and less on time-consuming administrative work. This transformation holds the potential to revolutionize the legal profession, making it more efficient and accessible.

Yet, with this power comes a heightened sense of responsibility. As AI tools become more integrated into legal practice, they introduce ethical challenges that demand careful navigation. Lawyers face challenges related to confidentiality, accountability, and bias in AI systems. The boundaries between human judgment and machine guidance blur, creating new dilemmas for legal professionals committed to upholding their ethical obligations.

The Promise of AI in Law

AI has already begun to redefine how lawyers approach their work, providing tools that enhance efficiency and support more informed decision-making.

AI tools allow lawyers to spend less time on repetitive tasks and more on strategic thinking, advocacy, and client relationships. Legal research platforms such as Westlaw Edge, for example, provide quick access to case law and statutes, enabling lawyers to focus on crafting arguments and strategies. The benefits extend beyond efficiency. AI tools for contract review, due diligence, and data-heavy tasks such as e-discovery reduce the likelihood of human error. AI predictive analytics drawn from patterns in historical data can improve lawyers' decision-making, empowering them to advise clients with greater confidence.

Success stories in the legal field demonstrate the impact of AI when thoughtfully applied. Law firms have reported significant time savings in contract review processes, reducing hours of manual work to minutes. International courts in jurisdictions such as Estonia have piloted AI tools to streamline administrative tasks, improving access to justice. In the corporate sector, AI-driven compliance tools have helped companies identify and address risks more effectively, safeguarding against potential liabilities.

These examples underscore the transformative potential of AI in the practice of law. AI offers lawyers new ways to deliver value, serving clients more effectively while improving the overall quality of their work. However, this promise does not come

without its challenges. As AI tools become more sophisticated, lawyers must remain vigilant regarding the ethical implications of their use.

Ethical Challenges in AI-Assisted Lawyering

With regard to AI, lawyers must navigate a landscape where innovation meets responsibility, ensuring that the adoption of AI enhances rather than undermines their professional duties. At the core of these challenges are issues of confidentiality, accountability, and bias.

Client Confidentiality and Data Privacy

AI systems analyze, categorize, and store data, sometimes using cloud-based servers or third-party platforms. This reliance on external systems introduces risks, including the possibility of data breaches, hacking, or inadvertent sharing of confidential details. Lawyers must remain vigilant—the duty to protect client information does not diminish when technology is involved.

Accountability and Responsibility

The lawyer's duty to supervise AI tools is firmly rooted in ethical rules, such as the American Bar Association (ABA) Model Rule of Professional Conduct 5.3, which governs the oversight of nonlawyer assistants. AI, though sophisticated, is ultimately a tool that lawyers must monitor and manage. Blind reliance on AI outputs can lead to mistakes, and lawyers remain accountable for the consequences. Lawyers must remain the ultimate arbiters of legal strategy, exercising professional judgment at every stage.

Bias in AI

AI systems are only as unbiased as the data used to train them. Algorithms developed with flawed or incomplete datasets may perpetuate systemic biases. In legal practice, AI tools for sentencing predictions may recommend harsher penalties for certain demographic groups. Similarly, bias in hiring algorithms has raised concerns about fairness and equity. Lawyers must be proactive in identifying and mitigating bias in the

AI tools they use. This begins with understanding the sources of training data and seeking tools designed with fairness and inclusivity in mind.

Who's Calling the Shots?

The integration of AI into legal practice introduces a complex question: Who is ultimately in control? As AI tools become more capable, they can provide insights and recommendations that influence legal strategy. This blurring of lines between human judgment and machine-generated advice raises concerns about maintaining the lawyer's role as the ultimate decision-maker.

Lawyers must take care not to abdicate their professional responsibilities to AI. While technology can offer valuable support, it is the lawyer who must make the final call on matters of strategy, ethics, and client advocacy. This includes taking responsibility when AI-generated recommendations lead to flawed or harmful outcomes. The legal profession is based on trust, which relies on the assurance that lawyers, rather than machines, are navigating clients through the complexities of the law. As the use of AI in law continues to grow, these ethical challenges will remain at the forefront.

Practical Scenarios: Ethical Dilemmas in Action

The ethical challenges of AI in law move from theoretical to tangible when lawyers encounter them in real-world situations. Understanding these dilemmas and how to address them is important for maintaining professionalism and trust. The following scenarios illustrate some of the most pressing issues lawyers may face when incorporating AI into their practice.

Scenario 1: The Biased Algorithm

A law firm adopts a case prediction tool to help assess the likelihood of success for potential litigation. Over time, one of the firm's lawyers notices a troubling pattern. The tool consistently predicts lower chances of success for cases involving certain demographic groups, raising questions about algorithmic bias.

This situation demands immediate ethical scrutiny. The lawyer must consider the

implications of relying on a tool that may perpetuate inequities. Ignoring the issue could lead to unfair treatment of clients and harm the firm's reputation.

To address the problem, the lawyer should first investigate the source of the bias. This involves reviewing the training data and algorithms used by the tool, possibly with the assistance of a technical expert. If the firm cannot mitigate the bias, the firm should discontinue its use and explore alternatives. Transparency with clients is also critical. The lawyer should explain the decision-making process and ensure that the AI tool does not replace sound legal judgment.

Scenario 2: The Confidential Data Breach

A lawyer uses an AI platform to manage document review for a large-scale litigation case. Without warning, the platform experiences a security breach, exposing sensitive client information. The breach, though unintentional, results in the potential compromise of privileged data.

In this scenario, the lawyer's ethical obligations are clear. First, they must promptly inform the affected client about the breach, adhering to rules of professional conduct that mandate disclosure of material information. Next, they should work with the AI provider to determine the cause of the breach and steps to prevent future incidents.

Determining fault can be complex. While the AI vendor may bear responsibility for technical failures, the lawyer is ultimately accountable for ensuring that the tools they use meet adequate security standards. Regular audits of AI systems and careful vetting of vendors are essential safeguards. Moving forward, the lawyer must reassess their reliance on the compromised platform and consider additional security measures.

Scenario 3: The Over-Reliance on AI

During a critical trial, a lawyer relies heavily on an AI tool to shape the closing argument. The tool suggests a particular angle based on its analysis of similar cases, but the strategy fails to resonate with the jury. The unfavorable outcome leaves the client dissatisfied and questioning the lawyer's judgment.

This scenario highlights the risks of over-reliance on AI. While AI can provide valuable

insights, it cannot account for the nuances of human behavior or the unique dynamics of a courtroom. The lawyer's duty is to balance AI-generated recommendations with their own expertise and intuition.

These scenarios illustrate the ethical dilemmas that can arise when integrating AI into legal practice. By understanding these challenges and responding thoughtfully, lawyers can navigate the complexities of AI while upholding their professional obligations.

Best Practices for Ethical AI Integration

The challenges and dilemmas presented by AI in law make clear that a thoughtful approach is essential. Lawyers must adopt best practices to ensure that the integration of AI into their work aligns with ethical standards. By combining vigilance, education, transparency, and oversight, they can maximize AI's benefits while minimizing risks.

Due Diligence

The first step to ethical AI use is thorough vetting of the tools and vendors involved. Lawyers must ensure that AI providers prioritize data privacy and incorporate safeguards against bias. Evaluating a vendor's track record, compliance with regulations, and methods for securing data can help build trust in their technology. Organizations should investigate the algorithm's design and verify whether independent audits identified any potential flaws.

Regular reviews and audits of AI tools in use are equally important. As technology evolves, new vulnerabilities may arise. Ongoing assessments help ensure that the tools remain effective, accurate, and compliant with legal and ethical standards.

Education and Training

Training lawyers and staff on the ethics and limitations of AI is critical to its responsible use. Many ethical challenges stem from a lack of understanding of how AI works. By providing education on the potential pitfalls, such as algorithmic bias or data vulnerabilities, firms can equip their teams to make informed decisions.

Staying updated on emerging regulations and ethical guidelines related to AI is equally important. Technology and the law are advancing quickly. Lawyers must remain informed about changes that could impact how they use AI, including new rules addressing accountability and privacy.

Transparency and Client Communication

Transparency builds trust, both with clients and within the legal profession. Lawyers should inform clients about the use and limitations of AI tools in their cases. This disclosure helps manage expectations and reassures clients that AI is a tool, not a replacement for human judgment.

Oversight and Supervision

Active oversight of AI is essential. This includes reviewing the results of AI analysis, cross-checking them with independent sources, and applying legal expertise to evaluate their relevance and accuracy. Documenting decisions that rely on AI further ensures accountability. Detailed records of how AI tools contributed to a particular course of action provide transparency and protect against potential disputes. These steps ensure that AI serves as a powerful ally, enhancing legal practice without compromising professional values.

Regulatory Landscape: Current and Future

The integration of artificial intelligence into legal practice has created opportunities for innovation, but it also necessitates a clear understanding of the regulatory framework governing its use. As lawyers navigate the ethical challenges of AI, they must also stay informed about the existing rules and emerging legislation shaping the future of AI in law.

Existing Rules and Guidelines

The ABA and state bar associations have begun addressing the ethical implications of AI in law. While no AI-specific rules currently exist, established ethical standards

provide guidance. For example, ABA Model Rule 1.1 emphasizes the need for competence, which now includes understanding the technology lawyers use. ABA Model Rule 1.6 underscores the importance of protecting client confidentiality, a critical concern when using AI tools that process sensitive data.

State bar associations have also weighed in. Some, such as California and New York, have issued formal opinions highlighting lawyers' responsibilities when using AI, including the duty to supervise the technology and its outputs. These opinions stress that lawyers must remain accountable for AI-generated recommendations, ensuring they align with professional standards.

Emerging Legislation Around AI in Legal Practice

The legislative landscape surrounding AI in legal practice is evolving rapidly. At the federal level, the United States has taken steps to establish guidelines for AI development and use. The National Artificial Intelligence Initiative Act aims to promote trustworthy AI, focusing on transparency, fairness, and accountability.

Several states have also introduced legislation addressing AI. For instance, Illinois passed the Artificial Intelligence Video Interview Act, which regulates the use of AI in employment decisions. While not specific to legal practice, such laws signal a growing awareness of the need for ethical oversight of AI technologies.

Legal-specific regulations are likely to emerge in the future. These may include requirements for AI transparency, mandatory bias testing, and clearer rules on accountability when AI tools are involved in legal matters. Lawyers must monitor these developments to ensure compliance and adapt their practices accordingly.

The Balanced Approach: AI as a Partner, Not a Replacement

As lawyers navigate the ethical challenges of AI and adapt to emerging regulations, the key to success lies in embracing a balanced approach. Encouraging a culture of responsibility is essential to achieving this balance.

Training programs that emphasize the limitations and ethical implications of AI can help lawyers and staff use these tools wisely. Clear policies for oversight, transparency, and accountability reinforce the principle that technology supports but does not replace the human element of lawyering.

By viewing AI as a partner rather than a replacement, lawyers can embrace innovation while staying true to their ethical obligations. AI can become a valuable ally in the pursuit of justice and the advancement of the legal profession.

Author

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),...

American Bar Association |
https://www.americanbar.org/groups/gpsolo/resources/magazine/2025-mar-apr/ethics-ai-assisted-lawyering-whose-call-it-anyway/?utm_source=chatgpt.com

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

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),...

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

Voice of Experience Voice of Experience: February 2026

The Warning Signs of AI Dependence in Legal Practice

Jeffrey M Allen and Ashley Hallene

Feb 07, 2026 5 min read

Summary

- Recognize AI over-reliance in legal practice by spotting warning signs like skipping primar source research, trusting “lawyerly” tone, and relying on unverified citations.
- Understand why AI errors are uniquely dangerous for lawyers because fluent, polished w can hide hallucinated cases, misapplied standards, and quiet mistakes that trigger sancti
- Adopt a professional AI review protocol that prioritizes verification, jurisdiction-specific a counterargument testing, and confidentiality checks before filing or advising clients.

istockphoto.com/Gorodenkoff Proc

Jump to:

AI Column

The law has always adapted to new tools. Lawyers once feared the photocopier and later the cloud. Today, generative AI can draft, summarize, and organize, but it can also mislead. The peril lies not in the existence of the tool, but in its confidence. AI writes in

clean, persuasive paragraphs that resemble legal work. If you allow the machine to do the thinking while you merely copy the results, you have surrendered your professional judgment.

The Hazard of Frictionless Work

AI tools save time and reduce the friction of the blank page. This convenience creates a mental hazard. In the traditional practice of law, the "blank page" acts as a necessary obstacle. It forces a lawyer to engage in the slow, often painful labor of organizing thoughts and selecting the precise language to serve a client's needs. This manual effort is not merely a chore; it is a diagnostic tool. Lawyers usually catch weak facts and missing elements during the active effort of drafting and outlining. The struggle to frame a sentence often reveals a flaw in the underlying legal theory.

When a machine produces a "good enough" draft instantly, the lawyer often skips the rigorous work that reveals cracks in an argument. This speed fundamentally alters the lawyer's relationship with the work. The practitioner shifts from an author, who must understand every brick in the foundation, to a proofreader, who merely checks the surface of a finished wall. Because the machine writes with a professional tone, the lawyer may feel a false sense of momentum. This ease creates a dangerous complacency. If you do not encounter the friction of building the argument yourself, you are less likely to notice when that argument rests on a fabricated citation or a misapplied standard. True advocacy requires the tension of creation; without it, the lawyer becomes a mere passenger to the machine's output.

Four Warning Signs of Over-Reliance

#1. You Stop Checking Primary Sources

AI predicts language; it does not know the law. It will cite non-existent cases and offer federal standards where state law applies. Consider a motion regarding the standard for summary judgment. An AI tool may generate a perfect recitation of the federal "plausibility" standard. However, if you are in a state court that retains a traditional "notice pleading" requirement, following the machine's lead will lead you into error.

The court will see a lawyer who has mastered a software prompt but failed to read the local rules. If the output becomes your authority before you pull the statute or the case, you have crossed the line into dependence.

#2. You Trust Tone Over Truth

AI writes with a professional, "lawyerly" voice that triggers unearned trust. A neat paragraph can hide false citations or shallow, "middle" answers that lack strategic edge. Never let a polished sound persuade you to skip the proof. The machine is designed to please the user with a fluent response, not to challenge the user with a difficult truth.

#3. You Cannot Explain the Reasoning

If you cannot explain an argument or justify a strategy without your notes, you do not own the work. Using AI to generate an argument you cannot reconstruct is like wearing someone else's suit. The garment may look fine while you stand still, but it will tear the moment you move. Imagine a judge asks, "How does this 1994 holding apply to the specific facts of the breach before us today?" If AI provided the citation without the underlying logic, you will find yourself stammering in open court. You must be able to defend the logic in a hearing or respond to a judge's questions directly. A lawyer who cannot explain the "why" behind a citation has ceased to be an advocate and has become a spokesperson for a black box.

#4. You Treat AI as a Liability Shield

Responsibility remains with the practitioner. A lawyer must supervise all assistance and ensure competence. Some believe they can point to the software as the culprit for a missed deadline or a fabricated quote. This is a fallacy. Thinking that you can blame the tool for an error is a sign that you are already off course. The court punishes the lawyer, not the software. Your signature on a filing is a personal guarantee of accuracy that no algorithm can share.

A Protocol for Professional Review

Before filing or sending any document, a practitioner must apply a strict standard of review. First, verify all authorities by reading every primary source and confirming every quote. Second, ensure the authority applies to your specific jurisdiction and remains good law. Third, test the reasoning by identifying the argument's logic and considering potential counterarguments. Finally, review the context for missing issues, "bad facts," and confidentiality breaches.

AI serves as a powerful assistant that helps lawyers move faster and manage complex information. However, as the tool becomes more fluent, the lawyer must become more disciplined. Over-reliance is not a single event; it is a gradual shift in habits that occurs when a lawyer stops thinking and stops owning the final product. Use AI to enhance your practice, but remember that clients and courts still demand what they always have: competence, candor, and accountable judgment.

Why AI Errors Are More Dangerous Than Ordinary Errors

Most legal mistakes are not dramatic. They are small and quiet: a wrong deadline, a misquoted holding, a missing element, or a standard that belongs to a different jurisdiction. In the past, these errors often signaled their own presence. A tired associate might produce a messy, disjointed memo that naturally invites skepticism from a senior partner. A poorly written wrong answer triggers an immediate instinct to verify.

AI makes these mistakes harder to see because it packages them in fluent language. A wrong answer written well triggers unearned trust. This is the "halo effect" of clean prose. When an algorithm generates a perfectly formatted brief, the lawyer’s critical defenses drop. The document looks right, feels right, and sounds right; therefore, the lawyer assumes it is right. AI is the best "wrong writer" lawyers have ever encountered because it replicates the professional polish of an expert while lacking the expert’s tether to reality.

The Erosion of Professional Intuition

Over-reliance is not a sudden catastrophe but a gradual shift in habits. It begins when a

lawyer stops doing the "heavy lifting" of research and drafting. Over time, this erodes the practitioner's legal instinct. A lawyer who does not engage with the raw material of the law loses the ability to sense when a conclusion feels "off."

This decay appears in predictable places: the research memo with citations you never verify, the contract draft that reads smoothly but misses the core business deal, and the summary that captures "main points" while smoothing over damaging details. In each case, the failure is identical: the lawyer treats the AI output as a completed work rather than a draft requiring professional review.

A Call for Accountable Judgement

AI is a powerful assistant. It helps lawyers move faster, write more clearly, and manage complex information. But the more fluent the tool becomes, the more disciplined the lawyer must be. Accountability cannot be delegated to a machine. Whether you use a fountain pen or a neural network, you remain the author of your filings and the guardian of your client's interests.

Use AI, but do not surrender to it. Clients and courts still demand what they always have: competence, candor, and accountable judgment. The mark of the modern lawyer is not the ability to use the tool, but the wisdom to know when the tool has reached its limit.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-february/warning-signs-of-ai-dependence-in-legal-practice/?utm_source=chatgpt.com

Voice of Experience Voice of Experience: September 2025

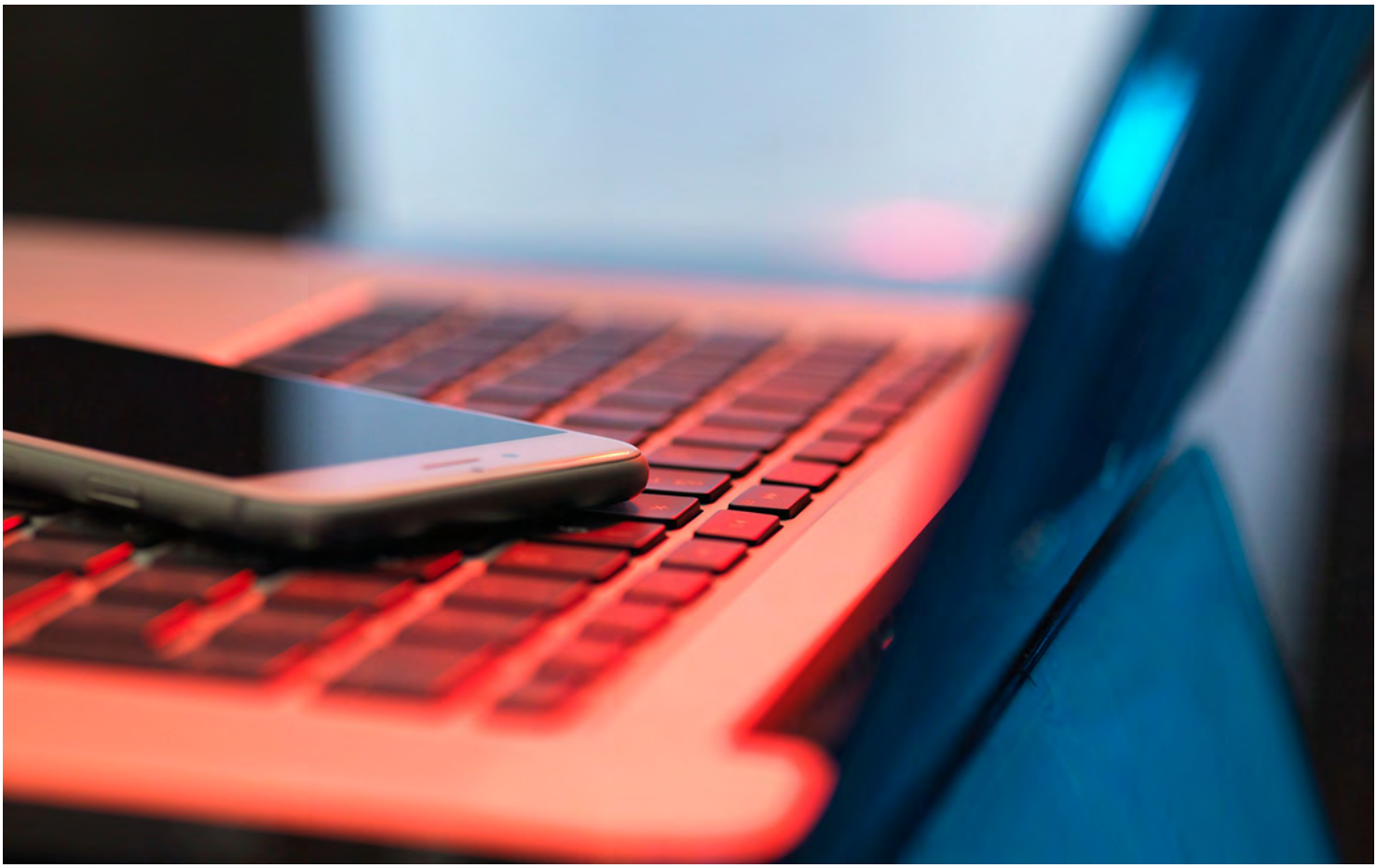
How to Navigate the New Frontier of Frau the Era of Generative AI

Jeffrey M Allen and Ashley Hallene

Sep 11, 2025 9 min read

Summary

- Generative AI has made scams more sophisticated, believable, and dangerous, significan impacting the legal profession.
- AI-generated phishing, deepfake audio/video, and fake legal documents are prevalent, ca significant financial and reputational damage.
- Lawyers must stay informed about AI advancements, implement layered verification, and upgrade security tools to protect themselves and their clients.



TEK IMAGE/SCIENCE PHOTO LIBRARY via G

Jump to:

Artificial intelligence (AI) is transforming the legal profession at a remarkable rate. It

offers tools that can streamline case research, help draft documents, and enhance client communications. These same advances are also accelerating the evolution of scams, making them more sophisticated, believable, and dangerous. The meteoric rise of generative AI (GenAI) has dramatically altered the landscape, empowering criminals to orchestrate scams once considered impossible. Scams have always adapted to new technologies. Generative artificial intelligence (GenAI) now represents a significant leap forward. Instead of crude or generic endeavors, fraud has become emotional, personal, and multiplied by the millions.

According to a July 2025 Pew survey, 73% of U.S. adults across all age groups report experiencing an online scam or cyberattack, while 21% have lost money to fraud in their lives . GenAI turbocharges these scams.

To protect themselves and their clients, lawyers must understand both the promise and the peril of this technology.

How Artificial Intelligence Has Transformed Scams

Traditional fraud tactics, clumsy phishing emails, poorly forged documents, or simple social engineering have given way to a new generation of AI-enhanced scams. Scammers now use GenAI to create hyper-realistic messages, invent synthetic voices and faces, and manipulate data at scale. These capabilities significantly raise the stakes for legal professionals, who must remain vigilant not only for themselves but for their clients and firms.

GenAI: The Double-Edged Sword

Generative AI models excel at mimicking human communication. They can draft emails, generate convincing legal documents, and even create audio or video indistinguishable from genuine sources. While these tools can be invaluable for lawyers, they also provide fraudsters with the means to deceive on an unprecedented level.

AI-Driven Scams: Real-World Cases and Escalating Tactics

- **Hyper-Personalized Phishing:** In 2023, Abnormal Security identified a wave of AI-generated phishing attacks tailored to law firms. Scammers used GenAI to reference real court cases, recent verdicts, and even ongoing negotiations to make fraudulent requests appear legitimate. Several firms reported falling victim to information leaks and, sometimes, unauthorized fund transfers. AI bots sift through social media to learn your interests or network, then generate emails or messages impersonating someone known to you. These messages look polished, include relevant details, and often bypass spam filters. Recent reports warn that users of Gmail, Outlook, and Apple Mail are particularly vulnerable to such attacks in 2025.

- **Deepfake Audio and Video:** Scammers clone human voices or create synthetic videos to impersonate people, ranging from celebrities to coworkers and family members. The 2020 UK CEO fraud case, where an executive transferred €220,000 based on a convincing deepfake call, serves as a prime example. In 2023, scammers duped an employee at a Hong Kong multinational firm into transferring $25 million after joining a video call where every participant was a deepfake mimicking company executives. In another 2023 case, an Arizona attorney received a video call "from a client" requesting confidential case files, only later to discover the entire interaction was AI-generated. Other examples include:

    - An energy firm employee was tricked into transferring $243K via a voice clone of the parent company's CEO.

    - In early 2024, Arup employees sent nearly $26 million after attending a video call with deepfake avatars of their coworkers and the CFO.

    - In Florida in 2025, a woman lost $15,000 after scammers used a cloned voice of her daughter claiming she'd had an emergency, then pressured her for another $30,000 with fake legal threats. Fortunately, her family intervened in time.

    - Another case involved a fake kidnapping of someone's son using voice clone tech to extort money.

- **Fake Legal Documents and Court Orders**: In Texas, a law firm nearly released escrow funds based on an AI-generated phony court order, complete with forged credentials and signatures. In the UK, a 2022 national legal regulator issued a warning after several firms received AI-generated "urgent" injunctions, prompting hasty actions that nearly led to significant financial losses.

- **Invoice and Vendor Fraud:** In 2023, a scammer using GenAI to send emails that mimicked a longstanding vendor, down to the writing style, reference numbers, and formatting, targeted a New York law firm. The scam was detected only after the accounting team noticed a subtle difference in the bank account details. In Australia, a mid-sized law firm narrowly avoided transferring $800,000 to a scam account after an AI-generated invoice appeared to come directly from the firm's IT provider.

- **Fake Law Firms and Synthetic Identities:** In 2021, the Law Society of England and Wales reported an increase in AI-created law firm websites, complete with phony lawyer profiles and credentials, duping clients out of both sensitive documents and retainer fees. In Canada in 2022, an AI-generated website and matching LinkedIn profiles convinced several small businesses they were engaging with a reputable firm, only to lose significant retainers.

- "**Grandparent" Deepfake Scam:** In 2022, an elderly Canadian couple lost $21,000 after receiving a phone call from a voice matching their grandson, created with deepfake technology. The callers impersonated both the grandson and a lawyer, urging an immediate wire transfer for a supposed legal emergency.

- **AI-Generated Court Filings:** In 2023, a New York attorney submitted a legal brief containing fictitious case citations created by ChatGPT. Although unintentional, this incident revealed how easily GenAI can introduce mistakes and plausible-sounding but fraudulent legal content into court filings or discovery processes.

- **Impersonation of Colleagues:** In 2022, a senior partner at a London firm received what appeared to be urgent emails from a trusted associate, requesting sensitive client information. The emails were written in a style

nearly identical to that of the associate, but forensic analysis later revealed they were crafted by GenAI and sent from a spoofed domain.

- **Fake Settlement Offers**: In California in 2023, an insurance defense firm received a detailed settlement proposal for a complex civil case. The proposal included AI-generated signatures and referenced real case law, but the investigation revealed it was a fraudulent attempt to redirect funds to a criminal account.

- **AI-Driven Social Engineering on Social Media:** In the U.S., legal professionals have reported incidents where AI bots, posing as potential clients, extracted detailed information about legal strategy or billing before vanishing, leaving the real clients and firms exposed to future fraud attempts.

- **AI-Generated Romance and Investment Scams:** Romance scammers have long relied on emotional manipulation, but now GenAI can create synthetic personas, complete with fabricated photos, stories, and social histories, to build trust over time before requesting money. These networks, often based in West Africa and Southeast Asia, are industrializing romance fraud.

- **Fake celebrity deepfakes**: One "Jennifer Aniston" romance scam victim was conned into sending £200 in Apple gift cards, another lost nearly £700,000 trusting a fake Brad Pitt.

- **Phantom Travel and Fake Business Scams:** There are cases of people traveling long distances expecting fictional attractions shown in AI-generated marketing, only to find the place doesn't exist. It's not just misleading; it's a financial loss and emotional blow.

- **Small businesses also face impersonation**: fake job listings, cloned store sites, or deepfake ads using public figures to lure customers. These "deepfake economy" tactics disrupt commerce & trust.

Why Generative AI Changes the Game

Scale & Accessibility: Tools like GhostGPT (a jailbreak model) allow anyone to craft phishing scripts, clone voices, and build intelligent chatbots—even without technical expertise. Scam pages created via GenAI quadrupled globally from May 2024 to April 2025— over 38,000 new scam pages per day.

Emotional Persuasion & Automation: GenAI enables scammers to imitate tone, timing, and personal details. A scam message doesn't feel like an attack; it feels like someone you trust asking for help.

Synthetic Identities: Fraudsters using AI are building entire fake personas, from identity documents to selfies, to fool banking verifications. These aren't random bots—they're sophisticated "users" capable of loan fraud, money laundering, or even phishing executives.

Impersonation Scams: As businesses leverage AI to enhance customer service, cybercriminals are also exploiting this technology, launching sophisticated impersonation scams. These scams are spreading fast. A report from the Identity Theft Resource Center shows a 148% spike in impersonation scams between April 2024 and March 2025 as scammers spin up fake business websites, create lifelike AI chatbots, and build voice agents that sound like real company reps. In 2024 alone, the Federal Trade Commission reported $2.95 billion in losses due to impersonation scams.

Real-World Impacts

- CEO-level scams (e.g., WPP's CEO impersonated via voice on WhatsApp in 2024) show how advanced fraud can penetrate corporate levels.
- Financial losses continue to mount: globally, deepfake-related fraud exceeded $200 million in Q1 2025; losses are projected to hit $40 billion by 2027.
- GenAI phishing and voice scams have even duped trained teams in multi-million-dollar organizations.

Legal and Regulatory Landscape

The rapid evolution of AI-generated scams has spurred governments and regulatory bodies worldwide to introduce and strengthen laws aimed at the detection, prevention, and prosecution of scams. Here are some key developments and their implications for legal practitioners:

- **The EU Artificial Intelligence Act (AI Act):** Adopted in 2024, the AI Act is the world's first comprehensive law regulating AI. It prohibits certain AI practices (such as manipulative deepfakes for fraud) and imposes transparency obligations on high-risk AI systems, including those used in financial and legal services. Lawyers practicing in Europe, or those with EU clients, must understand their responsibilities, including disclosure and risk management protocols.

- **U.S. Deepfake and Digital Impersonation Laws**: Several U.S. states, including Texas, California, and Virginia, have enacted laws criminalizing malicious deepfakes, especially those used for fraud, election interference, or reputational damage. The federal "DEEP FAKES Accountability Act" has been proposed to mandate watermarks on AI-generated media and criminal penalties for malicious use.

- **Federal Trade Commission (FTC) Guidance**: In the U.S., the FTC has issued guidelines warning businesses and professionals about AI-driven fraud. The guidelines recommend robust verification procedures, regular employee training, and heightened scrutiny of unusual transactions.

- **Data Protection and Cybersecurity Laws**: The General Data Protection Regulation (GDPR) in Europe and similar laws in Canada and the U.S. mandate strict controls over data handling. These laws require law firms to implement reasonable security measures to protect client data from AI-driven breaches or manipulations and to report violations promptly.

- **Bar Association Ethics Opinions**: Many national and state bar associations have issued ethics opinions reminding lawyers of their duty to stay competent with emerging technologies and to protect client confidentiality against AI-generated threats.

Regulations will likely evolve as GenAI becomes more prevalent in creating and enhancing scams and digital deception. Legal professionals must stay aware of developments relevant to their practice areas and jurisdictions, because non-compliance can have serious professional and financial consequences.

Why Older Lawyers Face Unique Risks

Attorneys with decades of experience hold trust and authority but may be less acclimated to the latest technological threats. Scammers take advantage of this unfamiliarity with technology and exploit this trust and understanding, crafting attacks that leverage long-held relationships and established communication channels. Since older lawyers often manage high-value transactions and sensitive client matters, they are especially attractive targets for AI-enhanced scams.

How to Protect Yourself and Spot AI Scams

Generative AI scams can feel indistinguishable from reality. The following practices, however, can reduce your exposure:

Preventive Protective Measures

1. **Continuous Education**: Stay up to date on cybersecurity and AI as they relate to fraud by attending technology-focused CLEs, reading reputable legal technology publications, and discussing trends with IT specialists.

2. **Layered Verification**: Always confirm any instructions involving sensitive data or funds by using a secondary, secure channel. Verify requests for information or changes to payment details directly with the person or organization making the request.

3. **Upgrade Security Tools**: Adopt advanced security tools capable of detecting AI-generated content, and ensure that you keep your systems up to date. Multi-factor authentication and regular audits of legacy systems can help you minimize vulnerabilities.

4 **Regular Staff Training**: Organize regular staff-wide educational sessions with real-world simulations of AI-driven scams to reinforce best practices in spotting suspicious activity and teach about new technology that helps detect fraud and defend against scams.

5 **Partner with Experts**: Engage outside cybersecurity professionals for regular audits and advice on the latest AI-driven protections, tailored to legal practices.

6 **Set Alerts:** Set up bank alerts, credit freezes, and dark-web monitoring where feasible.

7 **Establish "Safe Words" for Families and Firms:** A pre-shared word or phrase can confirm identity in emergencies.

8 **Monitor Accounts and Credit Use Technical Defenses:**

- Enable multi-factor authentication and password managers.
- Keep devices and apps updated to patch vulnerabilities.
- Consider email filtering and anti-deepfake detection tools.

In the Moment:

1. Pause Before You React
Scammers rely on urgency. If someone claims you must act immediately, especially with money, stop and verify.

2. Verify Through a Second Channel
Use a known phone number, video call, or in-person check. Do not trust the channel through which the request came.

3. Scrutinize Media

Look for subtle cues in voice and video:

- Slight timing mismatches in lip sync
- Unnatural pauses or tonal glitches
- Overly generic or “too perfect” backgrounds

4. Report and Share

Reporting scams to the FTC, IC3 (FBI), or local law enforcement helps disrupt networks and warn others.

Conclusion

Generative AI has moved scams from clumsy and obvious to sophisticated and subtle, personalized, emotional, and scalable. Legal systems are catching up with watermarking rules, deepfake bans, and fraud updates, but the most reliable defense today remains human skepticism, verification, and community awareness.

Generative AI offers immense opportunities but also brings new forms of risk that require a proactive, informed approach to defend against them. By building awareness, adopting advanced security strategies, and staying abreast of evolving regulations, lawyers can remain pillars of trust and protection for their clients in an increasingly complex digital world.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-september/navigate-the-new-frontier-of-fraud-in-the-era-gen-ai/?utm_source=chatgpt.com

Voice of Experience Voice of Experience: December 2025

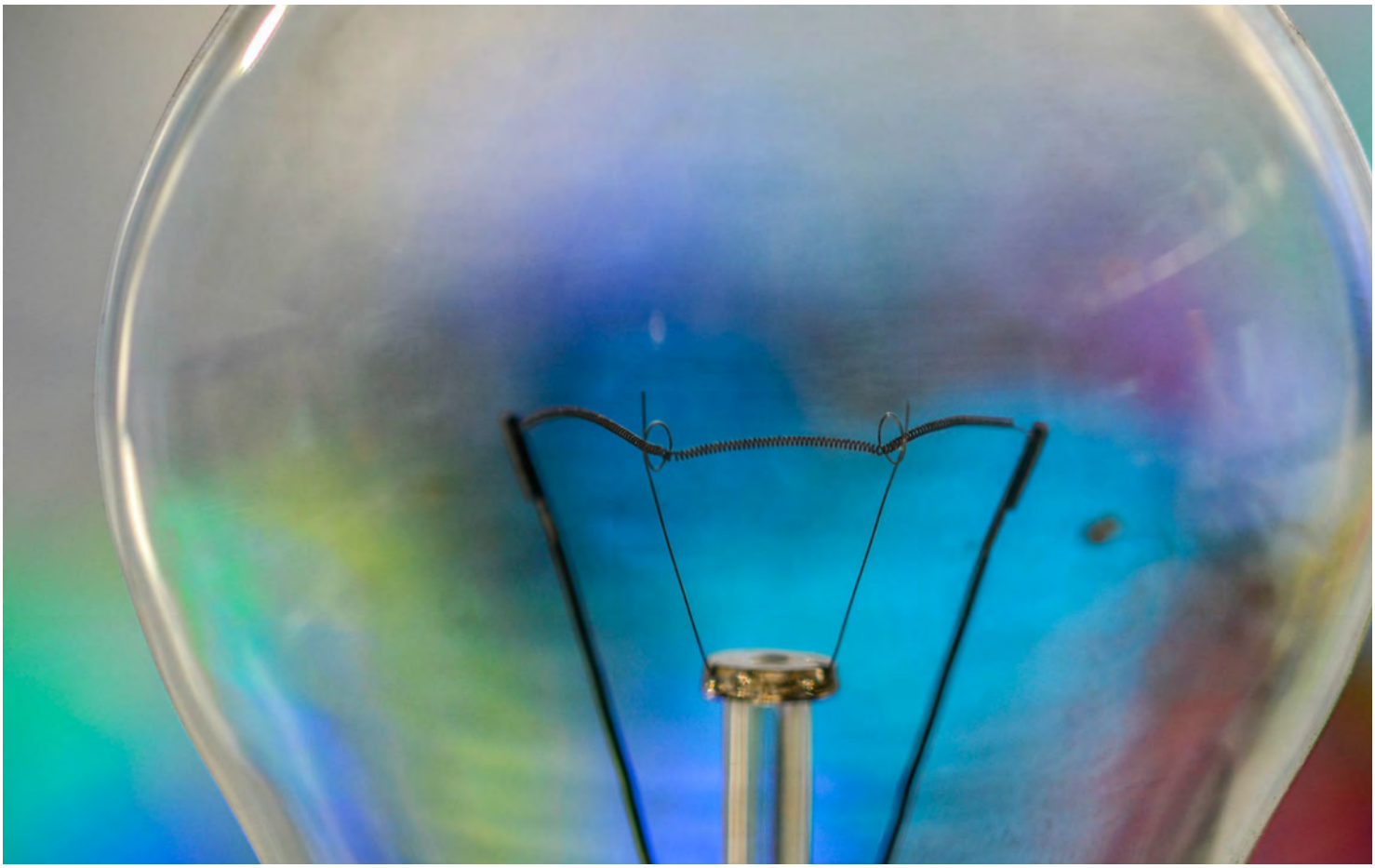
It Is Risky Business When AI Starts Practi Judgment

Jeffrey M Allen and Ashley Hallene

Dec 04, 2025 8 min read

Summary

- Legal judgment has always required a blend of law, fact, and human insight.
- AI advances promise speed, consistency, and cost savings. Yet, they also invite a quiet sh control from lawyer to machine.
- Lawyers now stand at a moment where technology can expand their reach or quietly nar



iStock.cor

Jump to:

Artificial intelligence (AI) has already reshaped how lawyers research, draft, and manage their practices. What once took hours can now be done in minutes with the

help of innovative tools that predict, summarize, and suggest. The next frontier, however, is more unsettling. AI is beginning to move from helping with tasks to guiding the very judgments that define legal work.

Across firms, algorithms are assessing risk, scoring contracts, and advising on settlement strategy. These systems learn from patterns in vast data sets. Yet, they do not think, reason, or understand. They calculate. When lawyers start relying on those calculations without question, the profession enters uncertain ground.

Legal judgment has always required a blend of law, fact, and human insight. It weighs ethics, emotion, and nuance in ways no program can reproduce. The danger lies not in the use of AI, but in its quiet promotion from assistant to decision-maker. Many lawyers see the efficiency. Few see the erosion of professional responsibility that can follow when technology begins to imitate judgment itself. The question is no longer whether lawyers should use AI, but how far they are willing to let it think for them.

The Expanding Reach of AI in Legal Decision-Making

Once confined to research tools and document review, AI is now venturing into the realm of analysis and advice. Programs that once highlighted keywords are beginning to recommend strategies. Software that once compared clauses now predicts litigation outcomes. These advances promise speed, consistency, and cost savings. Yet, they also invite a quiet shift in control from lawyer to machine.

Across the profession, new tools are being marketed as “decision support” systems. They score contracts for risk, analyze evidence for persuasive value, and estimate the likelihood of winning a motion or settling a case. The results appear confident, often wrapped in the authority of data and algorithms. Many lawyers, pressed for time and dazzled by precision, treat those outputs as reliable guidance. Few stop to ask what the machine actually knows, or how it reached its conclusion.

Clients demand speed, and firms seek advantage. AI delivers both, but at a cost that few recognize. When software begins to suggest what “should” be done rather than simply presenting what “could” be done, it blurs the line between information and

judgment. The profession's reliance on reason and ethics begins to thin, replaced by a confidence built on probability rather than principle.

The growing presence of AI in decision-making does not just change how lawyers work. It changes what it means to be a lawyer.

What Makes Judgment "Legal Judgment"?

To understand what is at stake, it helps to ask what makes legal judgment different from analysis. Judgment is not only the application of law to fact. It is the art of weighing circumstance, consequence, and character. It requires both intellect and experience, a sense of what is fair as well as what is lawful. No program, however advanced, can feel the hesitation that comes before a hard choice or the empathy that guides a wise one.

AI can find patterns in data, compare cases, summarize opinions, and even predict outcomes with impressive precision. What it cannot do is grasp why a client's story matters or how a single decision may alter a life. Machines can analyze nuance but never truly perceive it. When lawyers begin to treat machine logic as wisdom, they risk trading the human heart of their work for a digital imitation.

Law is more than a system of rules; it is a profession built on judgment. Every decision carries interpretation, values, and moral weight. A lawyer must consider not only what the law permits but what justice demands in the moment. AI may provide insight, yet it cannot accept responsibility. The challenge is not to resist technology but to keep it in its proper role.

The Ethical Edge: Oversight, Accountability, and Competence

If judgment defines the lawyer's craft, then oversight defines the lawyer's duty. The profession has long accepted that assistants, clerks, and even software can help carry the workload, but responsibility never leaves the lawyer's desk. AI does not change that rule. It makes it harder to follow.

The American Bar Association's Model Rule 1.1 requires competence in both law and technology. A lawyer who uses AI without understanding its limits risks falling short of that standard. Model Rule 5.3 extends the obligation to supervise nonlawyers and technology. Together, these rules mean that even when AI produces a flawless draft or analysis, the lawyer must still review, verify, and stand behind it.

The problem grows more subtle when the output looks persuasive. A brief written with AI assistance may appear authoritative, complete with citations that sound credible but lead nowhere. A risk report may read as precise while hiding flawed data or missing context. The danger lies in complacency, not malice. Lawyers who trust without testing give away the very oversight they are sworn to provide.

Ethical practice in an AI-driven world requires new habits of verification and humility. It is vital to learn not only how to use these tools but also how to question them. They must treat AI as a partner that requires supervision, not as an oracle that delivers truth. The line between help and delegation is thin, and the cost of crossing it can be measured in both reputation and responsibility. No program can be allowed to act as an unsupervised advisor.

When the Algorithm Becomes the Advisor

As lawyers grow more comfortable with AI, the line between assistance and advice begins to blur. What starts as a convenient shortcut can become a quiet dependency. Each time an algorithm provides a polished answer, the lawyer's instinct to question weakens. Over time, the tool that once served as a helper begins to shape how decisions are made.

In many offices, AI now drafts correspondence, evaluates risk, and proposes negotiation strategies. It suggests arguments with a tone of authority that feels hard to doubt. When a system presents data as certainty, it becomes easy to confuse probability with truth. The risk is not that the software makes mistakes, but that the human mind stops noticing them. Lawyers who accept algorithmic advice without reflection trade experience for efficiency.

Consider a contract review platform that rates clauses on a color-coded scale. Green feels safe, red feels risky. The lawyer who relies on those signals may never ask what

assumptions created them. Or imagine a litigation analytics tool that predicts a judge's tendencies based on prior rulings. The lawyer who follows that prediction without context may misread both the judge and the case. What looks like an informed strategy can become obedience to code.

The profession's strength has always rested on discernment. More than deciding what is correct, lawyers must also decide what is right. When the algorithm begins to offer advice, that discernment must grow sharper, not weaker.

Redefining the Lawyer's Role in an Automated Era

The profession now faces a choice: resist, over-rely, or adapt. The lawyer who adapts with discernment will lead. The profession has never been only about knowledge. It has been about judgment, empathy, and communication. Machines can analyze precedent and suggest strategies, but they cannot reassure a nervous client or sense when a deal feels wrong. The rise of automation gives lawyers a chance to reclaim what only humans can offer.

The shift requires a new kind of skill. Lawyers must learn how to interpret AI outputs rather than simply accept them. They need to understand enough about how these systems work to spot errors, bias, or gaps in reasoning. The lawyer of the future will not compete with technology but will guide it, applying context and conscience where code cannot. This kind of "augmented judgment" combines the speed of the machine with the wisdom of experience.

The change also calls for humility. Many lawyers entered the field believing expertise alone would keep them relevant. Now value depends on adaptability. Those who embrace technology with discernment will thrive. Those who resist or rely too heavily on automation will risk being left behind.

The profession stands at a turning point. The lawyer's role is no longer to outthink the machine but to ensure that thinking still serves justice. The most successful lawyers will be those who keep the human element alive in a system increasingly driven by code.

Building Guardrails for Responsible Use

AI can serve justice only when its use is transparent, accountable, and ethical. Without guardrails, even good intentions can lead to misuse. Firms that adopt AI should begin with clear policies. Every lawyer should know what tools are approved, how data is handled, and what kinds of information must never be shared. Training should go beyond technical skills to include ethical awareness and critical thinking. A lawyer who knows how to prompt an AI system must also know how to question its results. Internal review processes can help catch errors before they reach clients or the court.

Vendors must also face scrutiny. Contracts with AI providers should define who is responsible for mistakes, data breaches, or misleading output. Lawyers should demand plain-language explanations of how systems make decisions and what data they rely on. Blind trust in a vendor's claims is no safer than blind trust in the algorithm itself.

Professional associations and regulators have a role to play as well. Bar organizations can issue guidance on best practices, disclosure requirements, and model policies. Courts can establish standards for how AI-generated work may be used in filings and discovery. The legal community has always evolved through precedent, and now it must set new precedents for technology that acts alongside the lawyer.

Guardrails will not limit creativity. They will preserve it. The goal is not to fear AI but to ensure that its power serves the public good, the integrity of the profession, and the client's trust.

Keeping the Human in the Loop

The story of AI in law is still being written. Each new tool promises efficiency and insight, yet each also raises questions about trust, responsibility, and the soul of professional judgment. Lawyers now stand at a moment where technology can expand their reach or quietly narrow it. The outcome depends on how they choose to use it.

The legal profession has always adapted to change. From typewriters to online research, every generation has faced a new challenge to its habits and values. What makes AI different is its appearance of thought. It does not just help draft or organize. It begins to reason. That illusion of intelligence tempts even skilled lawyers to surrender the slow, human process of judgment for the speed of prediction.

Keeping the human in the loop means more than reviewing a machine's output. It means insisting that technology serve people, not the other way around. AI can assist, advise, and even surprise, but it cannot care. It cannot weigh fairness or feel the pull of justice. Those are human tasks, and they remain the lawyer's highest calling. If lawyers remember that conscience, not code, defines their craft, they can let AI enhance their work without losing what makes it human.

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),...

American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-december/ai-practicing-judgment/?utm_source=chatgpt.com

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

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),...

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

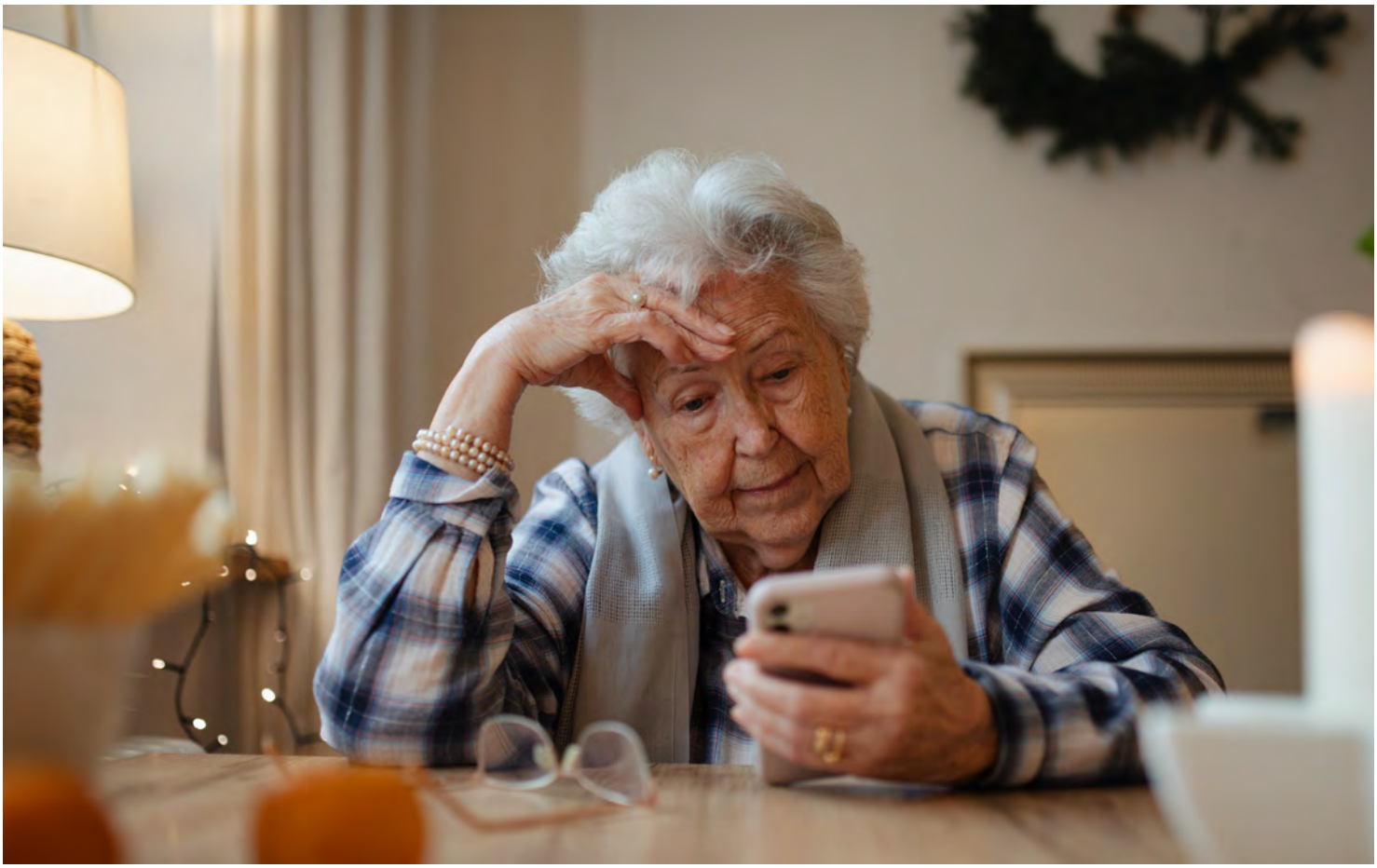
Lessons for Senior Lawyers on AI Mishap Legal Practice

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 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),...

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

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:

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),...

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: September 2025

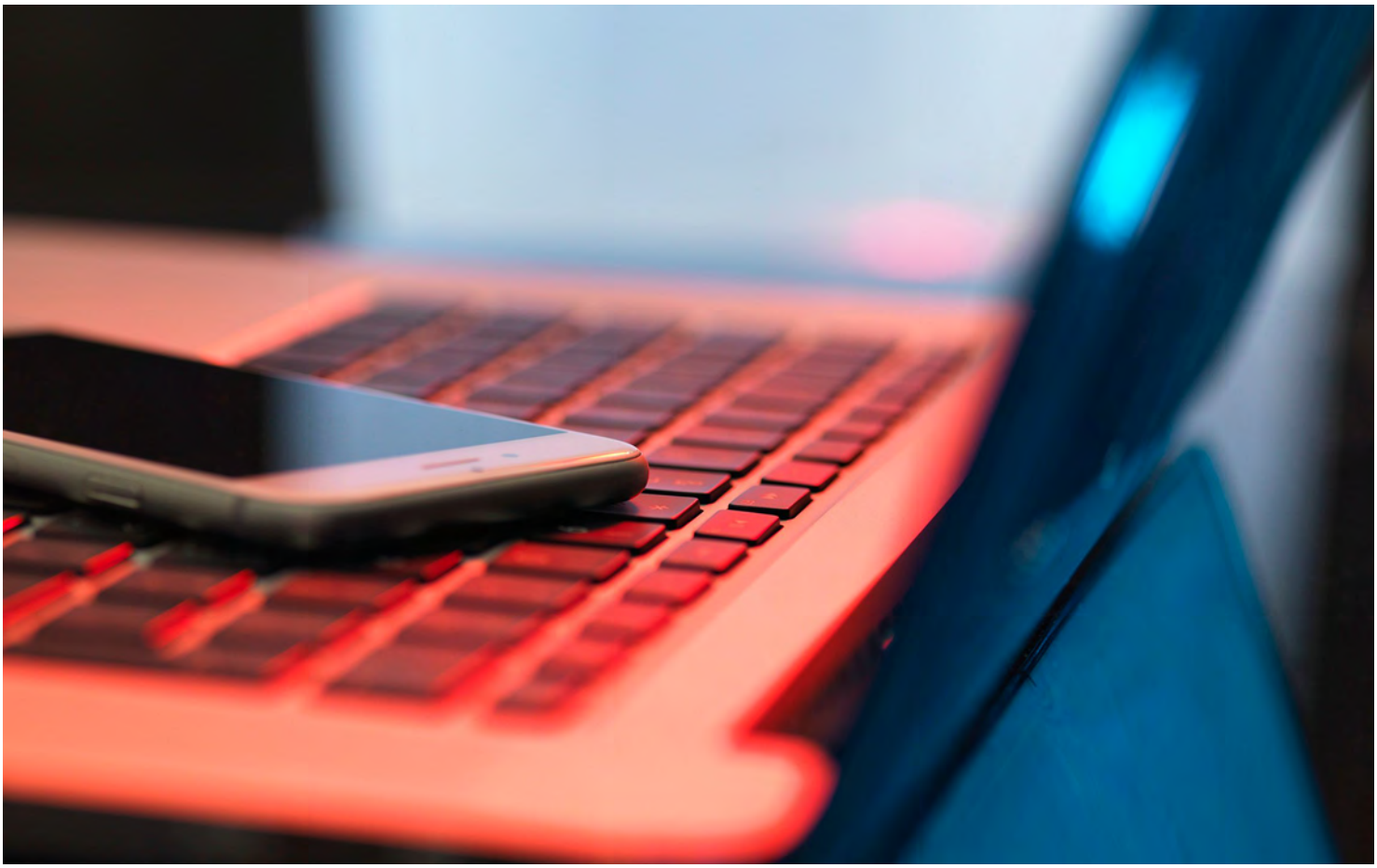
How to Navigate the New Frontier of Frau the Era of Generative AI

Jeffrey M Allen and Ashley Hallene

Sep 11, 2025 9 min read

Summary

- Generative AI has made scams more sophisticated, believable, and dangerous, significan impacting the legal profession.
- AI-generated phishing, deepfake audio/video, and fake legal documents are prevalent, ca significant financial and reputational damage.
- Lawyers must stay informed about AI advancements, implement layered verification, and upgrade security tools to protect themselves and their clients.



TEK IMAGE/SCIENCE PHOTO LIBRARY via G

Jump to:

Artificial intelligence (AI) is transforming the legal profession at a remarkable rate. It

offers tools that can streamline case research, help draft documents, and enhance client communications. These same advances are also accelerating the evolution of scams, making them more sophisticated, believable, and dangerous. The meteoric rise of generative AI (GenAI) has dramatically altered the landscape, empowering criminals to orchestrate scams once considered impossible. Scams have always adapted to new technologies. Generative artificial intelligence (GenAI) now represents a significant leap forward. Instead of crude or generic endeavors, fraud has become emotional, personal, and multiplied by the millions.

According to a July 2025 Pew survey, 73% of U.S. adults across all age groups report experiencing an online scam or cyberattack, while 21% have lost money to fraud in their lives . GenAI turbocharges these scams.

To protect themselves and their clients, lawyers must understand both the promise and the peril of this technology.

How Artificial Intelligence Has Transformed Scams

Traditional fraud tactics, clumsy phishing emails, poorly forged documents, or simple social engineering have given way to a new generation of AI-enhanced scams. Scammers now use GenAI to create hyper-realistic messages, invent synthetic voices and faces, and manipulate data at scale. These capabilities significantly raise the stakes for legal professionals, who must remain vigilant not only for themselves but for their clients and firms.

GenAI: The Double-Edged Sword

Generative AI models excel at mimicking human communication. They can draft emails, generate convincing legal documents, and even create audio or video indistinguishable from genuine sources. While these tools can be invaluable for lawyers, they also provide fraudsters with the means to deceive on an unprecedented level.

AI-Driven Scams: Real-World Cases and Escalating Tactics

- **Hyper-Personalized Phishing:** In 2023, Abnormal Security identified a wave of AI-generated phishing attacks tailored to law firms. Scammers used GenAI to reference real court cases, recent verdicts, and even ongoing negotiations to make fraudulent requests appear legitimate. Several firms reported falling victim to information leaks and, sometimes, unauthorized fund transfers. AI bots sift through social media to learn your interests or network, then generate emails or messages impersonating someone known to you. These messages look polished, include relevant details, and often bypass spam filters. Recent reports warn that users of Gmail, Outlook, and Apple Mail are particularly vulnerable to such attacks in 2025.

- **Deepfake Audio and Video:** Scammers clone human voices or create synthetic videos to impersonate people, ranging from celebrities to coworkers and family members. The 2020 UK CEO fraud case, where an executive transferred €220,000 based on a convincing deepfake call, serves as a prime example. In 2023, scammers duped an employee at a Hong Kong multinational firm into transferring $25 million after joining a video call where every participant was a deepfake mimicking company executives. In another 2023 case, an Arizona attorney received a video call "from a client" requesting confidential case files, only later to discover the entire interaction was AI-generated. Other examples include:

    - An energy firm employee was tricked into transferring $243K via a voice clone of the parent company's CEO.

    - In early 2024, Arup employees sent nearly $26 million after attending a video call with deepfake avatars of their coworkers and the CFO.

    - In Florida in 2025, a woman lost $15,000 after scammers used a cloned voice of her daughter claiming she'd had an emergency, then pressured her for another $30,000 with fake legal threats. Fortunately, her family intervened in time.

    - Another case involved a fake kidnapping of someone's son using voice clone tech to extort money.

- **Fake Legal Documents and Court Orders**: In Texas, a law firm nearly released escrow funds based on an AI-generated phony court order, complete with forged credentials and signatures. In the UK, a 2022 national legal regulator issued a warning after several firms received AI-generated "urgent" injunctions, prompting hasty actions that nearly led to significant financial losses.

- **Invoice and Vendor Fraud:** In 2023, a scammer using GenAI to send emails that mimicked a longstanding vendor, down to the writing style, reference numbers, and formatting, targeted a New York law firm. The scam was detected only after the accounting team noticed a subtle difference in the bank account details. In Australia, a mid-sized law firm narrowly avoided transferring $800,000 to a scam account after an AI-generated invoice appeared to come directly from the firm's IT provider.

- **Fake Law Firms and Synthetic Identities:** In 2021, the Law Society of England and Wales reported an increase in AI-created law firm websites, complete with phony lawyer profiles and credentials, duping clients out of both sensitive documents and retainer fees. In Canada in 2022, an AI-generated website and matching LinkedIn profiles convinced several small businesses they were engaging with a reputable firm, only to lose significant retainers.

- "**Grandparent" Deepfake Scam:** In 2022, an elderly Canadian couple lost $21,000 after receiving a phone call from a voice matching their grandson, created with deepfake technology. The callers impersonated both the grandson and a lawyer, urging an immediate wire transfer for a supposed legal emergency.

- **AI-Generated Court Filings:** In 2023, a New York attorney submitted a legal brief containing fictitious case citations created by ChatGPT. Although unintentional, this incident revealed how easily GenAI can introduce mistakes and plausible-sounding but fraudulent legal content into court filings or discovery processes.

- **Impersonation of Colleagues:** In 2022, a senior partner at a London firm received what appeared to be urgent emails from a trusted associate, requesting sensitive client information. The emails were written in a style

nearly identical to that of the associate, but forensic analysis later revealed they were crafted by GenAI and sent from a spoofed domain.

- **Fake Settlement Offers**: In California in 2023, an insurance defense firm received a detailed settlement proposal for a complex civil case. The proposal included AI-generated signatures and referenced real case law, but the investigation revealed it was a fraudulent attempt to redirect funds to a criminal account.

- **AI-Driven Social Engineering on Social Media:** In the U.S., legal professionals have reported incidents where AI bots, posing as potential clients, extracted detailed information about legal strategy or billing before vanishing, leaving the real clients and firms exposed to future fraud attempts.

- **AI-Generated Romance and Investment Scams:** Romance scammers have long relied on emotional manipulation, but now GenAI can create synthetic personas, complete with fabricated photos, stories, and social histories, to build trust over time before requesting money. These networks, often based in West Africa and Southeast Asia, are industrializing romance fraud.

- **Fake celebrity deepfakes**: One "Jennifer Aniston" romance scam victim was conned into sending £200 in Apple gift cards, another lost nearly £700,000 trusting a fake Brad Pitt.

- **Phantom Travel and Fake Business Scams:** There are cases of people traveling long distances expecting fictional attractions shown in AI-generated marketing, only to find the place doesn't exist. It's not just misleading; it's a financial loss and emotional blow.

- **Small businesses also face impersonation**: fake job listings, cloned store sites, or deepfake ads using public figures to lure customers. These "deepfake economy" tactics disrupt commerce & trust.

Why Generative AI Changes the Game

Scale & Accessibility: Tools like GhostGPT (a jailbreak model) allow anyone to craft phishing scripts, clone voices, and build intelligent chatbots—even without technical expertise. Scam pages created via GenAI quadrupled globally from May 2024 to April 2025— over 38,000 new scam pages per day.

Emotional Persuasion & Automation: GenAI enables scammers to imitate tone, timing, and personal details. A scam message doesn't feel like an attack; it feels like someone you trust asking for help.

Synthetic Identities: Fraudsters using AI are building entire fake personas, from identity documents to selfies, to fool banking verifications. These aren't random bots—they're sophisticated "users" capable of loan fraud, money laundering, or even phishing executives.

Impersonation Scams: As businesses leverage AI to enhance customer service, cybercriminals are also exploiting this technology, launching sophisticated impersonation scams. These scams are spreading fast. A report from the Identity Theft Resource Center shows a 148% spike in impersonation scams between April 2024 and March 2025 as scammers spin up fake business websites, create lifelike AI chatbots, and build voice agents that sound like real company reps. In 2024 alone, the Federal Trade Commission reported $2.95 billion in losses due to impersonation scams.

Real-World Impacts

- CEO-level scams (e.g., WPP's CEO impersonated via voice on WhatsApp in 2024) show how advanced fraud can penetrate corporate levels.
- Financial losses continue to mount: globally, deepfake-related fraud exceeded $200 million in Q1 2025; losses are projected to hit $40 billion by 2027.
- GenAI phishing and voice scams have even duped trained teams in multi-million-dollar organizations.

Legal and Regulatory Landscape

The rapid evolution of AI-generated scams has spurred governments and regulatory bodies worldwide to introduce and strengthen laws aimed at the detection, prevention, and prosecution of scams. Here are some key developments and their implications for legal practitioners:

- **The EU Artificial Intelligence Act (AI Act):** Adopted in 2024, the AI Act is the world's first comprehensive law regulating AI. It prohibits certain AI practices (such as manipulative deepfakes for fraud) and imposes transparency obligations on high-risk AI systems, including those used in financial and legal services. Lawyers practicing in Europe, or those with EU clients, must understand their responsibilities, including disclosure and risk management protocols.

- **U.S. Deepfake and Digital Impersonation Laws**: Several U.S. states, including Texas, California, and Virginia, have enacted laws criminalizing malicious deepfakes, especially those used for fraud, election interference, or reputational damage. The federal "DEEP FAKES Accountability Act" has been proposed to mandate watermarks on AI-generated media and criminal penalties for malicious use.

- **Federal Trade Commission (FTC) Guidance**: In the U.S., the FTC has issued guidelines warning businesses and professionals about AI-driven fraud. The guidelines recommend robust verification procedures, regular employee training, and heightened scrutiny of unusual transactions.

- **Data Protection and Cybersecurity Laws**: The General Data Protection Regulation (GDPR) in Europe and similar laws in Canada and the U.S. mandate strict controls over data handling. These laws require law firms to implement reasonable security measures to protect client data from AI-driven breaches or manipulations and to report violations promptly.

- **Bar Association Ethics Opinions**: Many national and state bar associations have issued ethics opinions reminding lawyers of their duty to stay competent with emerging technologies and to protect client confidentiality against AI-generated threats.

Regulations will likely evolve as GenAI becomes more prevalent in creating and enhancing scams and digital deception. Legal professionals must stay aware of developments relevant to their practice areas and jurisdictions, because non-compliance can have serious professional and financial consequences.

Why Older Lawyers Face Unique Risks

Attorneys with decades of experience hold trust and authority but may be less acclimated to the latest technological threats. Scammers take advantage of this unfamiliarity with technology and exploit this trust and understanding, crafting attacks that leverage long-held relationships and established communication channels. Since older lawyers often manage high-value transactions and sensitive client matters, they are especially attractive targets for AI-enhanced scams.

How to Protect Yourself and Spot AI Scams

Generative AI scams can feel indistinguishable from reality. The following practices, however, can reduce your exposure:

Preventive Protective Measures

1. **Continuous Education**: Stay up to date on cybersecurity and AI as they relate to fraud by attending technology-focused CLEs, reading reputable legal technology publications, and discussing trends with IT specialists.

2. **Layered Verification**: Always confirm any instructions involving sensitive data or funds by using a secondary, secure channel. Verify requests for information or changes to payment details directly with the person or organization making the request.

3. **Upgrade Security Tools**: Adopt advanced security tools capable of detecting AI-generated content, and ensure that you keep your systems up to date. Multi-factor authentication and regular audits of legacy systems can help you minimize vulnerabilities.

4. **Regular Staff Training**: Organize regular staff-wide educational sessions with real-world simulations of AI-driven scams to reinforce best practices in spotting suspicious activity and teach about new technology that helps detect fraud and defend against scams.

5. **Partner with Experts**: Engage outside cybersecurity professionals for regular audits and advice on the latest AI-driven protections, tailored to legal practices.

6. **Set Alerts:** Set up bank alerts, credit freezes, and dark-web monitoring where feasible.

7. **Establish "Safe Words" for Families and Firms:** A pre-shared word or phrase can confirm identity in emergencies.

8. **Monitor Accounts and Credit Use Technical Defenses:**

- Enable multi-factor authentication and password managers.
- Keep devices and apps updated to patch vulnerabilities.
- Consider email filtering and anti-deepfake detection tools.

In the Moment:

1. Pause Before You React
Scammers rely on urgency. If someone claims you must act immediately, especially with money, stop and verify.

2. Verify Through a Second Channel
Use a known phone number, video call, or in-person check. Do not trust the channel through which the request came.

3. Scrutinize Media

Look for subtle cues in voice and video:

- Slight timing mismatches in lip sync
- Unnatural pauses or tonal glitches
- Overly generic or “too perfect” backgrounds

4. Report and Share

Reporting scams to the FTC, IC3 (FBI), or local law enforcement helps disrupt networks and warn others.

Conclusion

Generative AI has moved scams from clumsy and obvious to sophisticated and subtle, personalized, emotional, and scalable. Legal systems are catching up with watermarking rules, deepfake bans, and fraud updates, but the most reliable defense today remains human skepticism, verification, and community awareness.

Generative AI offers immense opportunities but also brings new forms of risk that require a proactive, informed approach to defend against them. By building awareness, adopting advanced security strategies, and staying abreast of evolving regulations, lawyers can remain pillars of trust and protection for their clients in an increasingly complex digital world.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-september/navigate-the-new-frontier-of-fraud-in-the-era-gen-ai/?utm_source=chatgpt.com

Voice of Experience Voice of Experience: February 2026

The Warning Signs of AI Dependence in Legal Practice

Jeffrey M Allen and Ashley Hallene

Feb 07, 2026 5 min read

Summary

- Recognize AI over-reliance in legal practice by spotting warning signs like skipping primar source research, trusting “lawyerly” tone, and relying on unverified citations.
- Understand why AI errors are uniquely dangerous for lawyers because fluent, polished w can hide hallucinated cases, misapplied standards, and quiet mistakes that trigger sancti
- Adopt a professional AI review protocol that prioritizes verification, jurisdiction-specific a counterargument testing, and confidentiality checks before filing or advising clients.

istockphoto.com/Gorodenkoff Proc

Jump to:

AI Column

The law has always adapted to new tools. Lawyers once feared the photocopier and later the cloud. Today, generative AI can draft, summarize, and organize, but it can also mislead. The peril lies not in the existence of the tool, but in its confidence. AI writes in

clean, persuasive paragraphs that resemble legal work. If you allow the machine to do the thinking while you merely copy the results, you have surrendered your professional judgment.

The Hazard of Frictionless Work

AI tools save time and reduce the friction of the blank page. This convenience creates a mental hazard. In the traditional practice of law, the "blank page" acts as a necessary obstacle. It forces a lawyer to engage in the slow, often painful labor of organizing thoughts and selecting the precise language to serve a client's needs. This manual effort is not merely a chore; it is a diagnostic tool. Lawyers usually catch weak facts and missing elements during the active effort of drafting and outlining. The struggle to frame a sentence often reveals a flaw in the underlying legal theory.

When a machine produces a "good enough" draft instantly, the lawyer often skips the rigorous work that reveals cracks in an argument. This speed fundamentally alters the lawyer's relationship with the work. The practitioner shifts from an author, who must understand every brick in the foundation, to a proofreader, who merely checks the surface of a finished wall. Because the machine writes with a professional tone, the lawyer may feel a false sense of momentum. This ease creates a dangerous complacency. If you do not encounter the friction of building the argument yourself, you are less likely to notice when that argument rests on a fabricated citation or a misapplied standard. True advocacy requires the tension of creation; without it, the lawyer becomes a mere passenger to the machine's output.

Four Warning Signs of Over-Reliance

#1. You Stop Checking Primary Sources

AI predicts language; it does not know the law. It will cite non-existent cases and offer federal standards where state law applies. Consider a motion regarding the standard for summary judgment. An AI tool may generate a perfect recitation of the federal "plausibility" standard. However, if you are in a state court that retains a traditional "notice pleading" requirement, following the machine's lead will lead you into error.

The court will see a lawyer who has mastered a software prompt but failed to read the local rules. If the output becomes your authority before you pull the statute or the case, you have crossed the line into dependence.

#2. You Trust Tone Over Truth

AI writes with a professional, "lawyerly" voice that triggers unearned trust. A neat paragraph can hide false citations or shallow, "middle" answers that lack strategic edge. Never let a polished sound persuade you to skip the proof. The machine is designed to please the user with a fluent response, not to challenge the user with a difficult truth.

#3. You Cannot Explain the Reasoning

If you cannot explain an argument or justify a strategy without your notes, you do not own the work. Using AI to generate an argument you cannot reconstruct is like wearing someone else's suit. The garment may look fine while you stand still, but it will tear the moment you move. Imagine a judge asks, "How does this 1994 holding apply to the specific facts of the breach before us today?" If AI provided the citation without the underlying logic, you will find yourself stammering in open court. You must be able to defend the logic in a hearing or respond to a judge's questions directly. A lawyer who cannot explain the "why" behind a citation has ceased to be an advocate and has become a spokesperson for a black box.

#4. You Treat AI as a Liability Shield

Responsibility remains with the practitioner. A lawyer must supervise all assistance and ensure competence. Some believe they can point to the software as the culprit for a missed deadline or a fabricated quote. This is a fallacy. Thinking that you can blame the tool for an error is a sign that you are already off course. The court punishes the lawyer, not the software. Your signature on a filing is a personal guarantee of accuracy that no algorithm can share.

A Protocol for Professional Review

Before filing or sending any document, a practitioner must apply a strict standard of review. First, verify all authorities by reading every primary source and confirming every quote. Second, ensure the authority applies to your specific jurisdiction and remains good law. Third, test the reasoning by identifying the argument's logic and considering potential counterarguments. Finally, review the context for missing issues, "bad facts," and confidentiality breaches.

AI serves as a powerful assistant that helps lawyers move faster and manage complex information. However, as the tool becomes more fluent, the lawyer must become more disciplined. Over-reliance is not a single event; it is a gradual shift in habits that occurs when a lawyer stops thinking and stops owning the final product. Use AI to enhance your practice, but remember that clients and courts still demand what they always have: competence, candor, and accountable judgment.

Why AI Errors Are More Dangerous Than Ordinary Errors

Most legal mistakes are not dramatic. They are small and quiet: a wrong deadline, a misquoted holding, a missing element, or a standard that belongs to a different jurisdiction. In the past, these errors often signaled their own presence. A tired associate might produce a messy, disjointed memo that naturally invites skepticism from a senior partner. A poorly written wrong answer triggers an immediate instinct to verify.

AI makes these mistakes harder to see because it packages them in fluent language. A wrong answer written well triggers unearned trust. This is the "halo effect" of clean prose. When an algorithm generates a perfectly formatted brief, the lawyer’s critical defenses drop. The document looks right, feels right, and sounds right; therefore, the lawyer assumes it is right. AI is the best "wrong writer" lawyers have ever encountered because it replicates the professional polish of an expert while lacking the expert’s tether to reality.

The Erosion of Professional Intuition

Over-reliance is not a sudden catastrophe but a gradual shift in habits. It begins when a

lawyer stops doing the "heavy lifting" of research and drafting. Over time, this erodes the practitioner's legal instinct. A lawyer who does not engage with the raw material of the law loses the ability to sense when a conclusion feels "off."

This decay appears in predictable places: the research memo with citations you never verify, the contract draft that reads smoothly but misses the core business deal, and the summary that captures "main points" while smoothing over damaging details. In each case, the failure is identical: the lawyer treats the AI output as a completed work rather than a draft requiring professional review.

A Call for Accountable Judgement

AI is a powerful assistant. It helps lawyers move faster, write more clearly, and manage complex information. But the more fluent the tool becomes, the more disciplined the lawyer must be. Accountability cannot be delegated to a machine. Whether you use a fountain pen or a neural network, you remain the author of your filings and the guardian of your client's interests.

Use AI, but do not surrender to it. Clients and courts still demand what they always have: competence, candor, and accountable judgment. The mark of the modern lawyer is not the ability to use the tool, but the wisdom to know when the tool has reached its limit.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-february/warning-signs-of-ai-dependence-in-legal-practice/?utm_source=chatgpt.com

Ask Techie: What's the Best Way to Manag Email Security in My Small Law Firm?

Ashley Hallene

Jul 01, 2025 1 min read

Summary

- This month's tech Q&A column answers your question about the best way to manage em security in a solo or small firm law practice.
- Email security is non-negotiable in legal practice. Strong encryption, vigilance against phi and secure providers help safeguard client confidentiality and uphold professional responsibility.

iStock.com/Viachesla

Jump to:

Q: What's the Best Way to Manage Email Security in My Small Law Firm?

A: To manage email security in a solo or small firm law practice, follow these key steps:

1. **Use a secure email provider.** Choose an email provider with strong security features. Providers such as ProtonMail, Microsoft Defender for Office 365,

or Google Workspace with security enhancements offer encryption, phishing protection, and compliance support.

2 **Encrypt sensitive emails.** Use end-to-end encryption for confidential communications. Services such as Virtru, Mimecast, or built-in encryption in Microsoft Outlook and Gmail add an extra layer of protection. Encrypt attachments separately when sending highly sensitive information.

3 **Guard against phishing attacks.** Train yourself and your staff to recognize phishing emails. Look for misspelled domains, urgent requests for information, and suspicious links. Enable multi-factor authentication (MFA) on all accounts to prevent unauthorized access, even if credentials are compromised.

4 **Protect client confidentiality.** Never send sensitive client data over unencrypted email. Use secure portals for document exchange. Limit email forwarding and use access controls to restrict sensitive information. Regularly review email security settings to ensure compliance with ethical obligations.

5 **Monitor and update security measures.** Keep software and email security settings up-to-date. Regularly review access logs and implement automated threat detection tools. Consider cybersecurity insurance for additional protection.

Email security is non-negotiable in legal practice. Strong encryption, vigilance against phishing, and secure providers help safeguard client confidentiality and uphold professional responsibility.

Techie: Ashley Hallene, JD, is *GPSolo eReport* Editor-in-Chief (hallenelaw@outlook.com).

What's YOUR question?

If you have a technology question, please forward it to Managing Editor Rob Salkin (robert.salkin@americanbar.org) at your earliest convenience. Our response team selects the questions for response and publication. Our regular response team

includes Jeffrey Allen, Wells H. Anderson, Ashley Hallene, Al Harrison, and Matthew Murrell. We publish submitted questions anonymously, just in case you do not want someone else to know you asked the question.

Please send in your questions today!

Author

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),...

Using AI for Practice Management

Ashley Hallene and Jeffrey M Allen

Mar 26, 2025 6 min read

Summary

- Generative AI and Chat GPT can do more in the legal field, such as draft legal documents in case management, automate routine client correspondence, and analyze firm efficienc
- Implementing AI in law practice management has significant implications for human wor requiring them to learn how to use AI efficiently and having some of their repetitive tasks replaced by AI.
- Despite its advantages, using AI in law practice management carries potential risks such cybersecurity, bias in AI algorithms, and overreliance on automation.
- Attorneys and law firms must disclose the use of AI, especially when it impacts client interactions or financial transactions.

istock.com

Jump to:

Conclusion →

Introduction

The legal profession increasingly relies on technology to manage client and firm information and conduct daily operations. While technology offers numerous benefits, it also introduces significant cybersecurity risks that can present particularly challenging situations for solo and small firm attorneys. Safeguarding client confidentiality and maintaining the integrity of legal practices requires understanding these risks and implementing effective security measures.

Integrating artificial intelligence (AI) into law practice management has revolutionized law firms' operations, improving efficiency, organization, and client service. With the advent of generative AI (Gen AI) and advanced models like ChatGPT, legal professionals now have access to sophisticated tools that assist in managing workloads, automating administrative tasks, and optimizing business operations. These innovations have reshaped how legal professionals handle daily tasks, making managing workloads easier, automating admin work, and improving client interactions. However, adopting AI also introduces new risks that must be managed carefully to ensure compliance with ethical and professional standards.

AI has gradually evolved from simple automation tools to sophisticated systems capable of performing complex tasks. Initially, we used it for basic functions such as document automation and e-discovery. Over time, machine learning and natural language processing advancements enabled AI to handle more intricate tasks, including legal research, contract analysis, and predictive analytics.

The Impact of Generative AI and Chat GPT

Generative AI, including models like Chat GPT, has profoundly impacted the legal industry. These AI systems can generate human-like text, making them valuable for drafting documents, creating legal briefs, and even generating responses to client inquiries. Chat GPT, in particular, has revolutionized client communication by providing

instant, accurate responses to common legal questions, improving client satisfaction and efficiency. We anticipate seeing more use of AI, particularly Gen AI, in the law office for practice management and the actual practice of law.

Generative AI, including ChatGPT, has expanded the scope of what AI can do in law practice management. Unlike earlier rule-based AI systems, Gen AI can assist in:

- Quickly generating detailed summaries of lengthy documents and reports for transmittal to clients.
- Automating routine client correspondence and internal memoranda to expedite response time.
- Enhancing customer service through the use of AI-powered chatbots to handle client inquiries.
- Data analysis providing insights into business performance metrics.
- Improving the onboarding processes by automating training and knowledge-sharing tasks.

The Role of AI in Law Practice Management and Law Office Operations

Today, AI assists attorneys and firm administrators in several ways:

1. **Document Management and Organization**. AI-powered systems can efficiently categorize, store, and retrieve documents, making case file management seamless and providing reports and information that the attorney can share with the client.
2. **Timekeeping and Billing Automation**. AI-driven tools automate time tracking, invoice generation, and expense management, ensuring accuracy in financial transactions and relieving attorneys of some of the tedium associated with billing practices.

3. **Client Relationship Management (CRM)**. AI-enhanced CRM platforms can help firms manage client interactions, automate follow-ups, and personalize client communications.

4. **Scheduling and Workflow Optimization**. AI-driven tools can streamline scheduling for meetings, court dates, and deadlines, improving time management for the attorney and client.

5. **Task Automation and Administrative Support**. AI-powered virtual assistants can handle repetitive administrative tasks like data entry and email management, ensuring timely and efficient completion.

6. **Compliance and Risk Management**. AI can monitor compliance with regulatory requirements, flag potential compliance issues, and suggest remedial actions to mitigate risks.

The Benefits of AI in Law Practice Management

The adoption of AI in law firms offers several advantages:

- **Increased Efficiency**. AI minimizes time spent on repetitive administrative tasks, allowing attorneys and staff to focus on client service and cases.

- **Cost Savings**. Automation reduces operational costs, leading to higher profitability.

- **Enhanced Accuracy**. AI reduces human error in data management, billing, and scheduling, rendering the firm more efficient.

- **Improved Client Service**. AI-driven CRMs and chatbots enhance responsiveness and client engagement, improving client relations and satisfaction.

- **Better Resource Allocation**. AI insights help firms make data-driven decisions on staffing and resource distribution.

Potential Issues for Human Workers

Implementing AI in law practice management has significant implications for human workers, including:

- **Job Availability**. As AI automates administrative and routine tasks, the demand for certain support roles, such as legal secretaries, administrative assistants, and paralegals, will likely decrease.
- **Workforce Reskilling**. Employees will need to adapt by acquiring new skills to work effectively with AI systems. Law firms may need to invest in training programs to upskill staff in AI literacy and technology management.
- **Workplace Conditions**. AI-driven workflow optimization can increase efficiency but may also increase expectations for faster turnaround times and greater productivity, potentially increasing employee stress and workloads.
- **Employment Displacement Concerns**. As AI takes over more repetitive functions, firms must carefully consider how to balance automation with maintaining meaningful employment opportunities for human workers.
- **Ethical and Human Oversight Challenges**. While AI improves efficiency, it lacks human judgment and moral reasoning. AI has no internal moral compass or genuine concept of right and wrong. Maintaining a workforce capable of critical thinking and ethical decision-making remains essential.

Risks and Ethical Considerations

Despite its advantages, using AI in law practice management carries potential risks:

- **Data Privacy and Security**. AI systems handling sensitive firm and client information must adhere to strict security protocols to prevent data breaches. This may require human oversight and the training of humans to provide the necessary supervision.

- **Bias in AI Algorithms**. AI models trained on biased data may produce inaccurate or skewed results, affecting firm decision-making. We must take precautions to ensure such issues do not result in erroneous decisions.
- **Over-Reliance on Automation**. Excessive reliance on AI without human oversight can lead to errors in financial reporting and compliance issues.
- **Regulatory Compliance**. AI-powered systems must align with legal industry regulations to avoid potential liabilities.

Minimizing Risks and Compliance Measures

To mitigate these risks, law firms should adopt best practices, including:

1. **Human Oversight**. Always have a properly trained natural person review AI-generated outputs to ensure accuracy and compliance with ethical, legal, and regulatory requirements.
2. **Data Security Measures**. Only use AI tools that comply with data protection regulations and implement cybersecurity best practices, including robust access controls.
3. **Bias Auditing**. Regularly evaluate AI models for bias and inaccuracies.
4. **Regulatory Awareness**. Law firms must stay informed about evolving regulations governing AI use in legal and business operations. As the rules change, the firms must adjust their practices and retrain their employees to ensure compliance.
5. **Client Disclosure**. Attorneys must transparently share with their clients how they employ AI in practice management and the actual practice of law.
6. **Provide Training**. We must equip legal professionals with the skills to work alongside AI tools effectively. This does not mean one-and-done training; as the playing field changes, so must the training.

7 **Employee Transition Plans**. Law firms must develop strategies to support employees whose roles may change due to AI, including reskilling initiatives and career development opportunities.

Disclosure Obligations and Best Practices

Attorneys and law firms must disclose the use of AI, especially when it impacts client interactions or financial transactions. Best practices for disclosure include:

- **Explicit Client Communication**. Please start at the beginning and inform clients in engagement letters about AI usage and its role in firm operations. Report any significant changes to clients in writing.
- **Clear Explanation**. Ensure that you carefully, thoroughly, and clearly explain to your clients the nature and scope of your firm's AI implementation, its benefits, potential limitations, and associated risks.
- **Risk Mitigation Disclosures**. Highlight measures taken by the firm to ensure data security and compliance.
- **Ongoing Updates**. Inform clients of changes in AI implementation, related policies, and their implications for firm operations.
- **Obtain Consent**. Obtain explicit written consent from clients before using AI tools in their cases.

Future Prospects

Looking ahead, we should anticipate continuing enhancement of AI's capabilities and further expansion of its role in the legal field. Expect advancements that include:

- **Advanced Predictive Analytics**. More accurate predictions of case outcomes and litigation risks.

- **Enhanced Natural Language Processing**. Anticipate implementing AI structures with an improved understanding and heightened ability to generate legal language.
- **AI-Driven Legal Strategy**. The evolution of AI systems with the ability to develop and suggest legal strategies based on comprehensive data analysis.

Conclusion

AI has transformed law practice management by improving operational efficiency, client service, and business decision-making. Its capabilities will induce lawyers to rely on it increasingly. However, we must balance its use with ethical considerations, human oversight, and transparency. Additionally, firms must proactively address workforce challenges, ensuring they equip employees with the skills necessary to thrive in an AI-enhanced environment. As AI technology evolves, firms that integrate AI intelligently and proactively address its risks will better position themselves to succeed in the future legal landscape.

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...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2025-march/using-ai-for-practice-management/?utm_source=chatgpt.com

Voice of Experience Voice of Experience: October 2024

Using AI for Predictive Analytics in Litigat

Ashley Hallene and Jeffrey M Allen

Oct 16, 2024 6 min read

Summary

- Learn how AI-powered predictive analytics can forecast litigation outcomes, guide strateg offer insights into judicial behavior.
- See examples of ways lawyers can apply predictive analytics to various stages of a matte

iStock.cor

Jump to:

Picture this: your law firm is involved in a high-stakes contract dispute, and you are facing a critical decision: settle for millions or risk going to trial. Traditional legal intuition leaned towards settling, but an AI-powered predictive tool told a different story. By analyzing hundreds of similar cases, judge profiles, and court rulings, the AI predicted an 80% chance of winning if they took it to court. Armed with this insight, the firm confidently pursued litigation—and won. This case wasn't a gamble; it was a calculated risk made possible by AI, highlighting how predictive analytics is

revolutionizing legal strategy. You have likely heard the saying, “If you can’t know the law, know the judge.” This phrase emphasizes the strategic advantage of being familiar with how a particular judge interprets and applies the law, as judges can exercise significant discretion in legal decisions. In the context of AI, predictive analytics tools help lawyers "know the judge" by analyzing past rulings and behavioral patterns, offering valuable insights for litigation strategy.

Predictive analytics involves using AI and machine learning algorithms to analyze large datasets, including past case rulings, legal filings, judicial decisions, and even jury behavior. The goal is to predict future legal outcomes and guide strategy by identifying patterns and trends. AI platforms aggregate vast amounts of legal data, including case law, statutes, court rulings, and historical outcomes. These datasets can include both structured (e.g., case records) and unstructured data (e.g., written opinions). Algorithms can be applied to detect patterns in the data, such as how certain judges rule on specific types of cases or which arguments have historically succeeded in certain courts. Through this analysis, AI tools can predict the likely outcome of a case, considering factors like jurisdiction, judge behavior, precedent, and case specifics. This can include forecasts on whether a case is likely to settle, win, or lose. This can help you evaluate the risks associated with proceeding to trial versus settling. It can highlight potential weaknesses in a case and provide insights on likely timelines and costs. Let’s examine how you might use predictive analytics in your practice:

Initial Case Evaluation

Hopefully, you have gathered enough information in your initial consultation for a thoughtful review of the matter. Using that information, predictive analytics tools can then analyze historical data from similar cases to predict the likely outcome of the new case. This includes assessing the probability of winning or losing, potential settlement amounts, and the duration of the case. This helps the lawyer provide the client with a realistic expectation of the case’s prospects. It can also help the lawyer allocate resources efficiently, including determining the amount of time, personnel, and budget required to handle the case effectively.

Evolving Case Strategy

If the matter progresses and you have identified both the judge for your matter and opposing counsel, then predictive analytics can offer further insights into their past rulings and strategies that may shape your strategy. For example, let's say a lawyer is preparing to represent a client in a complex business contract dispute. The case has been assigned to Judge Smith, who has a reputation for favoring strict interpretations of contract law. The opposing counsel, Attorney Johnson, is known for aggressive litigation tactics and frequently pushes for early settlements.

Using a predictive analytics tool, the lawyer examines Judge Smith's past rulings in similar contract cases. The tool reveals that Judge Smith consistently sides with plaintiffs in cases where the contract language is ambiguous but favors defendants when the contract is clear and unambiguous. Additionally, the data shows that Judge Smith tends to issue summary judgments in cases with well-documented evidence, avoiding lengthy trials.

The lawyer then uses predictive analytics to analyze Attorney Johnson's litigation history. The data reveals that Johnson tends to propose settlement offers early in the litigation process but pushes cases to trial when facing weaker evidence. The tool also shows that Johnson has a pattern of using procedural motions to delay proceedings, often aimed at pushing the other party into settling out of frustration.

Armed with this information, how might the lawyer adjust his strategy? Based on Judge Smith's tendency to issue summary judgments, the lawyer decides to present a case with clear, well-documented evidence and highlights the contract's explicit terms. This strategy increases the likelihood of a favorable summary judgment, potentially avoiding a drawn-out trial. Since the lawyer is also armed with the knowledge of Attorney Johnson's usual tactics, the lawyer prepares to counter early settlement offers and procedural delay tactics. The lawyer also takes steps to expedite the filing process and remains firm on pursuing a trial, knowing that Johnson often pushes weaker cases to trial if procedural delays succeed.

Which Way Forward? Settlement vs. Trial Analysis

Another useful facet of predictive analytics is its ability to identify key factors that influence settlement outcomes, such as the nature of the dispute, the jurisdiction, the

judge, and the opposing counsel. Here is another example to consider. Let's say a client approaches a lawyer with an employment discrimination case. The client believes they were wrongfully terminated based on their age. The lawyer turns to predictive analytics to analyze thousands of similar employment discrimination cases. The results consider factors such as the nature of the claim, the jurisdiction, the judge's history, and the outcomes of past cases and conclude there is a 60% chance of winning if the case goes to trial. It also estimates potential damages, suggesting that if the client wins, they could receive between $100,000 and $300,000. The tool assesses past settlement trends in similar cases and predicts a 70% chance of reaching a settlement. It also estimates that the settlement amount would likely be between $80,000 and $150,000. This highlights the risks of proceeding to trial, such as the possibility of losing the case and incurring significant legal fees. The lawyer also considers the time and emotional toll on the client. Based on all this, the lawyer advises the client on the potential outcomes. The client understands that while there is a reasonable chance of winning at trial, the settlement offers a more certain and quicker resolution with less risk. The client decides to pursue a settlement.

Finding the Right Tool for You

When you are ready to get on board with predictive analytics, here are some considerations for choosing the right platform for your practice:

1. **Assess the Platform's Data Sources**. Ensure the platform draws from comprehensive, up-to-date legal databases. It should include case law, statutes, court rulings, and data on judges and opposing counsel. Verify that the platform covers the jurisdictions relevant to your practice, as legal rules and case outcomes can vary significantly between states, regions, or countries. In the early days, most platforms focused on Federal court, only recently expanding into state and local courts. Make sure the platform has access to long-term historical data for more accurate predictions. One way to test this is through a thorough demo of the application.

2. **Evaluate the Accuracy of Predictions**. Look for platforms that demonstrate a consistent track record of accurate predictions in real-world cases. Check for case studies, reviews, or testimonials from legal professionals who have used

the tool. You should look for a tool that provides reasoned predictions on aspects such as the likelihood of winning, judicial behavior, settlement probabilities, and expected timeframes.

3 **Consider Whether the Platform Is Customizable, Flexible, and User-Friendly.** You should look for a platform that allows customization based on the specific facts of your case, jurisdiction, or legal area. The ability to adjust variables and inputs will provide more tailored insights. The platform should have a user-friendly interface that allows for easy navigation, data entry, and analysis without requiring extensive technical expertise.

4 **Data Privacy and Security.** Ensure the platform adheres to strict data privacy and security standards, as it will likely involve sensitive client information. Check for compliance with legal data privacy laws, such as GDPR or CCPA.

As predictive analytics continues to evolve, it will become an increasingly important tool in legal practice, driving data-driven decision-making and enhancing strategic outcomes. As legal professionals embrace predictive analytics, its integration into daily practice will not only improve efficiency and reduce costs but also transform the way lawyers approach litigation and client service.

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...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2024-october/using-ai-for-predictive-analytics-in-litigation/

Voice of Experience Voice of Experience: June 2026

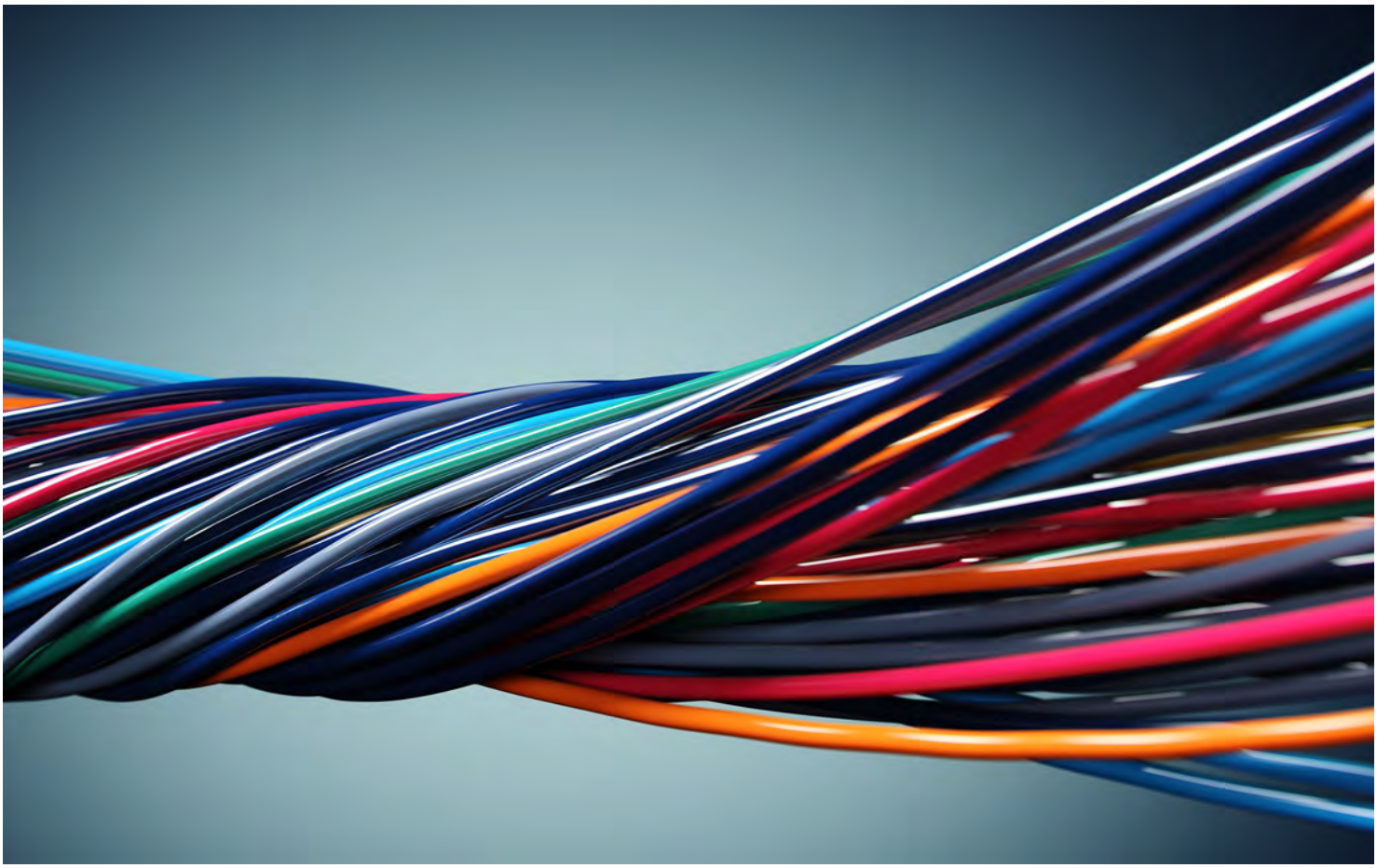
The New Digital Estate Issue for Lawyers, Businesses, Families, and Individuals

Jeffrey M Allen and Ashley Hallene

Jun 03, 2026 7 min read

Summary

- Lawyers need to have a digital estate plan for securing their own and their clients' digital (online accounts) in the event of incapacitation, death, or emergency, ensuring the fiduci not only have the authority but the ability to access them.
- Digital estate planning must address account recovery, not just asset disposition, becaus modern multi-factor authentication (MFA) and device-based security can leave fiduciaries authority but no practical access.
- Lawyers add value by building account-recovery inventories, redundancy, and tested wor that preserve continuity, confidentiality, and compliance during death, incapacity, or emergencies.
- Effective plans separate legal authority from access, rely on provider tools and trusted he and store recovery information securely without encouraging shared passwords.



iStoc

Jump to:

When people plan for the inevitable shuffling off of their mortal coil, they focus on wills, trusts, and tangible property. Increasingly, however, urgent—and disruptive—problems arise from locked digital accounts. Nearly everyone has digital accounts these days. While many digital accounts, such as social media, have little significance in the greater scheme of things, digital accounts often hold important information or allow control of significant assets. Modern security practices make "call customer service" an unreliable strategy. Lawyers can add value by incorporating account-recovery planning into client work and by addressing parallel law-office continuity needs before a crisis arises.

A common fact pattern: A surviving spouse calls with a death certificate and letters testamentary in hand, but the decedent's email account requires a phone-based approval prompt on a device no one can unlock. Another variation: a lawyer misplaces a phone while traveling, and a routine sign-in to an e-filing portal fails because the only multi-factor authentication (MFA) method required a connection to that lost device.

Account Recovery Belongs in Every Digital Estate Conversation

For many clients, "digital estate planning" sounds like a question of who gets the photo library, the domain name, or the cryptocurrency wallet. Those matter, but they assume the fiduciary can actually gain access to the accounts.

Account providers increasingly rely on MFA, device-based trust, and automated fraud detection. These tools protect users, but they also reduce the effectiveness of traditional recovery approaches (calling a help desk, presenting a death certificate, or producing a power of attorney). Add carrier SIM-swap fraud and email takeovers, and the modern result we increasingly see: a representative with authority but no access.

For lawyers, the issue cuts two ways. First, as a client-service problem: if a client loses their digital keys, even a well-drafted plan can stall while a representative fights through automated account defenses. Second, as a practice-management problem: MFA and trusted devices often protect law-office email, cloud files, billing, court e-filing credentials, and bank portals. When a lawyer becomes incapacitated—or loses a phone the day before a hearing—colleagues may have authority to act but lack access to the systems needed to keep the practice running.

For the Law Practice: Continuity, Confidentiality, and a "Keys Plan"

Most lawyers have rebuilt their practices around a handful of accounts: an email identity, a cloud storage system, a practice management and/or document management platform, an e-filing portal, and one or more financial accounts. Passwords rarely represent the weak point. The recovery chain does: who can receive reset codes, who has a trusted device, and who can approve an unfamiliar log-in when a provider's fraud controls are triggered.

Firms usually discover the recovery gap only in urgent situations. Deadlines do not pause while someone tries to locate a hardware key, find the owner account for a practice platform, or persuade a provider that a legitimate log-in attempt is not fraud. A firm-facing key plan helps to reliably and efficiently resolve the problem.

A practice-focused version of the inventory—kept separate from the personal/family list—can reduce delays and confusion during an emergency. It should identify:

- **Identity and email platform**, including who is an administrator and where administrative recovery information is stored.
- **Core practice systems**, including any owner accounts that can add or remove users.
- **E-filing and court portals** (and any mandated MFA method), including who may file if the responsible lawyer is unavailable.
- **Banking and trust account access** (including dual-control and approvals) and the process for emergency signers.
- **Website/domain registrar**, VoIP/phone provider and any client intake forms that route through email or a CRM.
- **Where client data lives** (shared drives, matter folders, encrypted archives) and how it is accessed if a key account is unavailable.

The office does not want attorneys to distribute a master password. In a law office, shared credentials present a compliance and malpractice hazard as they blur responsibility and can expose client confidences. Aim for role-based access (separate logins for each user), least-privilege permissions, and a documented method for an authorized colleague to obtain administrative control over a digital account when a disability, death, or emergency makes it necessary. Many platforms support delegated administration, emergency access features, or organizational recovery workflows far safer than “everyone knows the code.”

A Simple Workflow

1. **Build the inventory.** Identify the keys accounts and the high-impact accounts that depend on them.
2. **Choose the helper(s).** For clients, that may be an agent under a power of attorney, a spouse, or a successor trustee. Lawyers should use a designated assisting attorney, partner, trusted staff member, or IT administrator—depending on jurisdictional rules and your firm’s structure for law firm accounts.
3. **Pick secure storage.** Use a password manager’s emergency-access feature where appropriate, and store printed recovery codes and device-unlock instructions offline in a secure location, with copies in a second secure location outside of the office.
4. **Document the how.** Write down the steps a helper would need to take: the location of a trusted device, how to unlock it, what carrier to call, the required documents, and which accounts have the highest priority.
5. **Test annually or after a major change.** Recovery procedures change. A plan that worked last year may fail after a phone upgrade, a new authenticator app, or a provider’s switch to passkeys or a change of providers.

Client-Facing: How to Explain the Issue

In client meetings, normalization provides the most effective approach. The conversation should not focus on mistrust or sharing passwords. It should focus on building a recovery path that works under real-world conditions: missing devices, health emergencies, and accounts that treat every unfamiliar log-in as a potential takeover.

Separate (1) lawful authority, (2) practical access, and (3) security. The process should not encourage casual password sharing; it should create a structured plan that helps the right person recover the right account at the right time, with the least risk.

Client-Facing Tool: An "Account Recovery Inventory"

Although written for clients and families, the same inventory method can be duplicated by substituting practice keys accounts.

- **Primary email account(s)** used for logins and recovery (often the key to the kingdom).
- **Mobile carrier account** (carrier log-in, account PIN/passcode, and authorized individuals respecting the account).
- **Authenticator method** used for MFA: authenticator app, hardware key, text message, email code, or passkey.
- **Trusted devices**: which phones, tablets, and computers key accounts recognize.
- **Password manager** (if used): product name, where it has been installed, and how the emergency contact or recovery process works.
- **Recovery options on file**: backup email, backup phone, recovery codes, backup codes, and any trusted contacts.
- **High-impact accounts**: banking, credit cards, brokerage, retirement, tax portals, health portals, utilities, major retailers/subscriptions, and cloud

storage.

- **Where the plan is kept**: physical location and a second location for redundancy.

Use Redundancy to Mitigate Failure

Many lockouts happen because of security built around a single phone number, a single device, or a single email inbox. Single points of access lead to failure. Account recovery planning reduces the single points of failure. The plan should assume the loss of the phone, the client's inability to answer challenge questions, and the family or business partners' inability to access the client's email.

Passkeys deserve special attention. While phishing-resistant, they can make device access more important because the key often lives in a phone, tablet, or laptop (and may sync through a vendor ecosystem). If the only passkey (or approval prompt) lives on a missing phone, an executor may have impeccable paperwork but no access.

Storing Recovery Information—Without Creating New Risks

The best plans allow quick access by a trusted person. Prefer (a) a reputable password manager with an emergency-access workflow, (b) offline storage for recovery codes, and (c) redundancy across multiple locations. Many families use a sealed envelope in a home safe (with instructions and recovery codes), plus a second sealed copy stored elsewhere. Safe deposit boxes create problems as individuals may have difficulty gaining access to the box immediately after death or during incapacity.

For lawyers, the engagement requires advising on a recovery plan, but not taking custody of client credentials. A short statement in a client handout or engagement letter can clarify that the client retains responsibility for selecting the storage method and controlling who can access it. It should provide that the lawyer will not maintain passwords, recovery codes, or device-unlock information. That clarification protects the client (by reducing unnecessary disclosure) and protects the lawyer (by reducing breach

risk and later disputes about "who logged in").

1. **Lock down the mobile carrier.** Encourage a carrier account PIN/passcode, port-out protection where available, and limited "authorized users."
2. **Turn on (and print) recovery codes.** Many services provide one-time recovery codes—useless if stored inside the locked account, invaluable if stored offline.
3. **Use more than one recovery path.** Where the provider allows it, add a backup email and a backup phone number not dependent on the same device.
4. **Consider adding trusted contacts.** Some platforms allow a "trusted contact" or legacy contact to help with access or account memorialization.
5. **Plan for device access.** If an account depends on a trusted device, make sure the fiduciary can physically access and unlock at least one trusted device.
6. **Use a password manager with an emergency feature.** Many password managers offer emergency access, family sharing, or recovery workflows.

Authority, Privacy, and Provider Rules

Many states have enacted versions of the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA), which distinguishes between the *content* of communications and other digital assets, and often prioritizes an online tool (such as a provider's legacy contact feature) over a will or trust provision.

Provider tools—such as a legacy contact designation, trusted contact, or an account recovery contact—baked into the provider's process can provide the fastest path to lawful access. If the client has not set those tools up, the fiduciary may have to rely on a slower documentation-and-review process, inconsistent across providers and sometimes inconsistent across product lines with the same provider.

A power of attorney or letters testamentary may establish the right person, but they do not automatically satisfy a platform's technical controls. If the account requires a one-time code delivered to a phone no one can unlock, the fiduciary may have clear

authority but no ability to complete the recovery path. Lawyers can provide immediate, measurable value by planning for that gap.

Conclusion

Lawyers need to translate fast-changing technology into durable protection—both to properly serve clients' needs and to protect their own practices. Adding an "account recovery inventory" to estate and incapacity planning can reduce cost, delay, and stress. A parallel law-office "keys plan" can help avoid missed deadlines and continuity problems when a trusted device disappears or an automated fraud system blocks a login.

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),...

ABA American Bar Association |
https://www.americanbar.org/groups/senior_lawyers/resources/voice-of-experience/2026-june/new-digital-estate-issue-for-lawyers-businesses-families-indivduals/