



**BARCLAY DAMON** <sup>LLP</sup>

# The Ethics of **Cybersecurity**: Tips to Protect Your Practice

**Kevin Szczepanski**  
Co-Chair, Data Security & Technology Practice  
Barclay Damon LLP

# An Ethical Overview



# Rules Governing Lawyers

- » Competence  
RPC 1.1
- » Communication  
RPC 1.4
- » Confidentiality  
RPC 1.6
- » Conduct of Nonlawyers  
RPC 5.3

22 NYCRR pt. 1200

# Competence – RPC 1.1

- » A lawyer should provide competent representation to a client.”
- » “Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary to the representation.”
- » Comment [8]: “To maintain the requisite knowledge and skill, a lawyer should . . . **(ii) keep abreast of the benefits and risks associated with the technology the lawyer uses to provide services to clients or to store or transmit confidential information[] . . . .**”

## “The Technology The Lawyer Uses”

Microsoft Outlook

Use of VPN (for remote login and remote work)

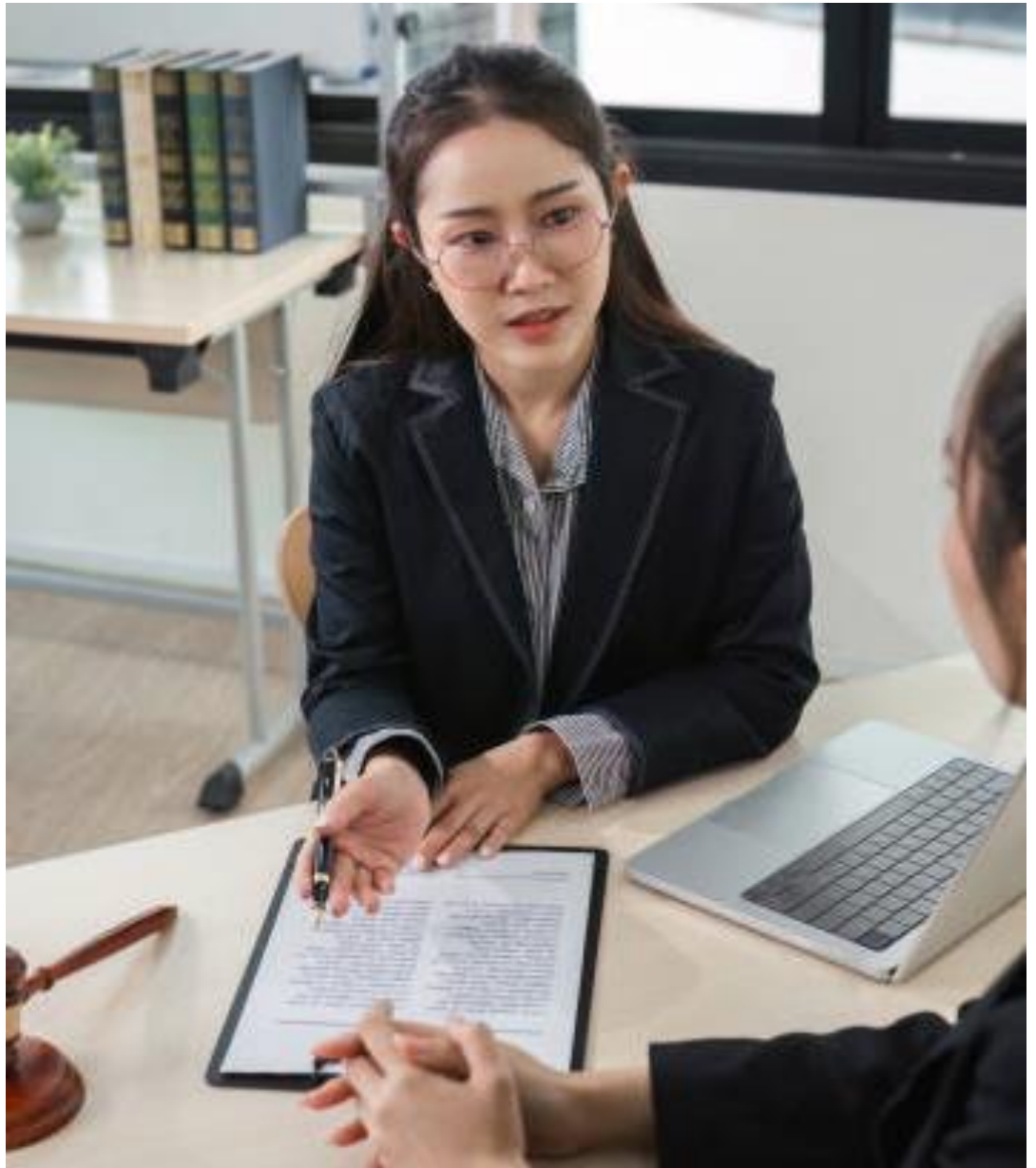
Video-conferencing software

Legal Research (LEXIS, Westlaw, Casetext)

File management

Smart phones

Generative AI



# Communication – RPC 1.4

- » “A lawyer shall . . . . Reasonably consult with the client about the means by which the client’s objectives are to be accomplished[.]”
- » “A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.”

# Confidentiality – RPC 1.6

- » “A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure or use of, or unauthorized access to, information protected by Rules 1.6, 1.9(c), or 1.18(b).”
  - 1.6 – Confidentiality
  - 1.9(c) – Confidential Information of a Former Client
  - 1.18(b) – Use of Information from a Prospective Client

# Confidentiality – RPC 1.6

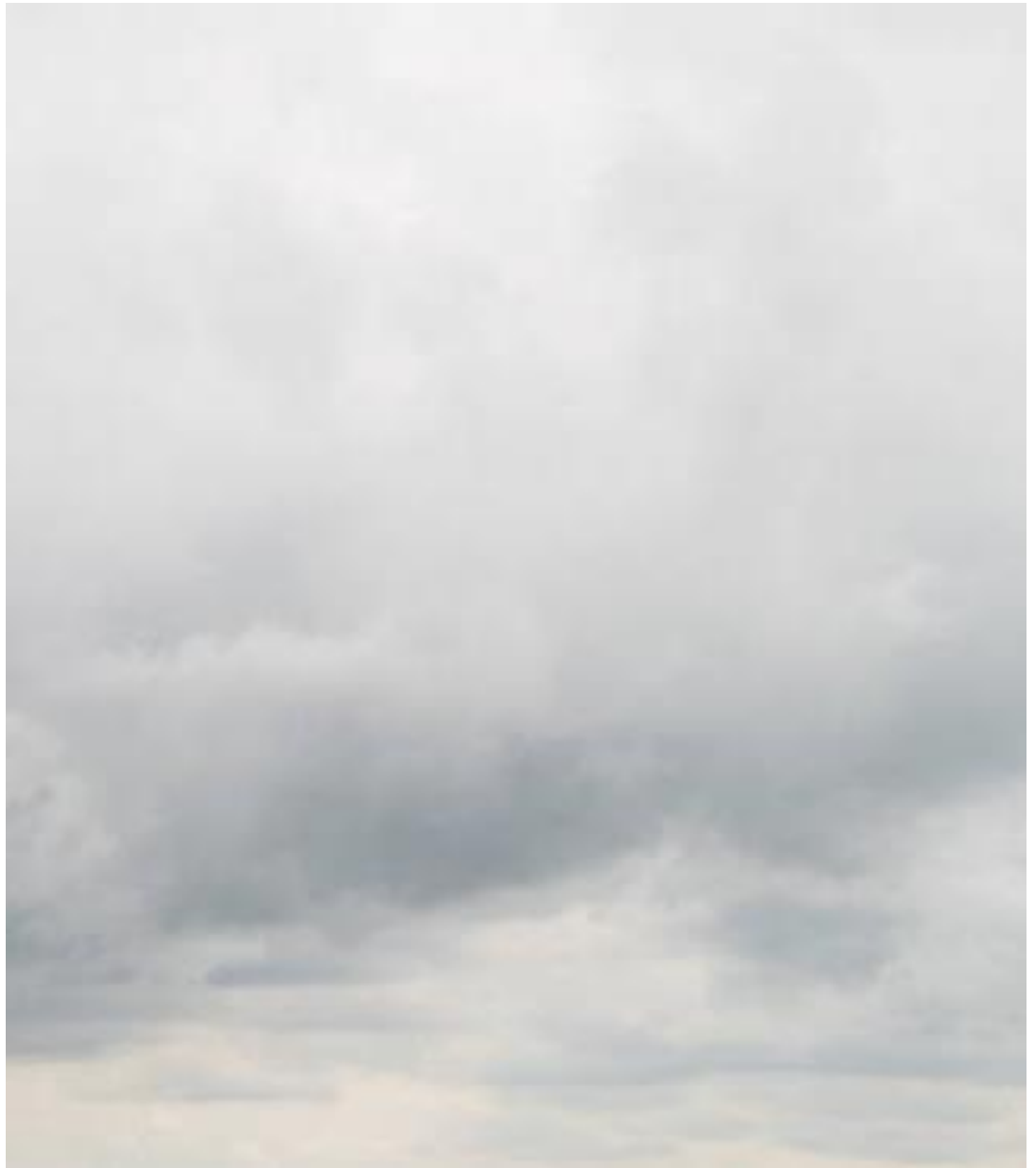
- » In determining what's reasonable, several factors are considered:
  - › The sensitivity of the information;
  - › The likelihood of disclosure if additional safeguards are not employed;
  - › The cost of employing additional safeguards;
  - › The difficulty of implementing the safeguards; and
  - › The extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or software excessively difficult to use).

## **Conduct of Nonlawyers – RPC 5.3**

“A law firm shall ensure that the work of nonlawyers who work for the firm is adequately supervised, as appropriate.... [T]he degree of supervision required is that which is reasonable under the circumstances, taking into account

“the experience of the person whose work is being supervised[] ...” and

“the likelihood that ethical problems might arise in the course of the working on the matter.”



# Takeaway: A Lawyer Must . . .

1. Understand the benefits and risks of technology.
2. Disclose them to the client.
3. Obtain the client's informed consent.

**When:** at the beginning of the engagement, or before using a technology.

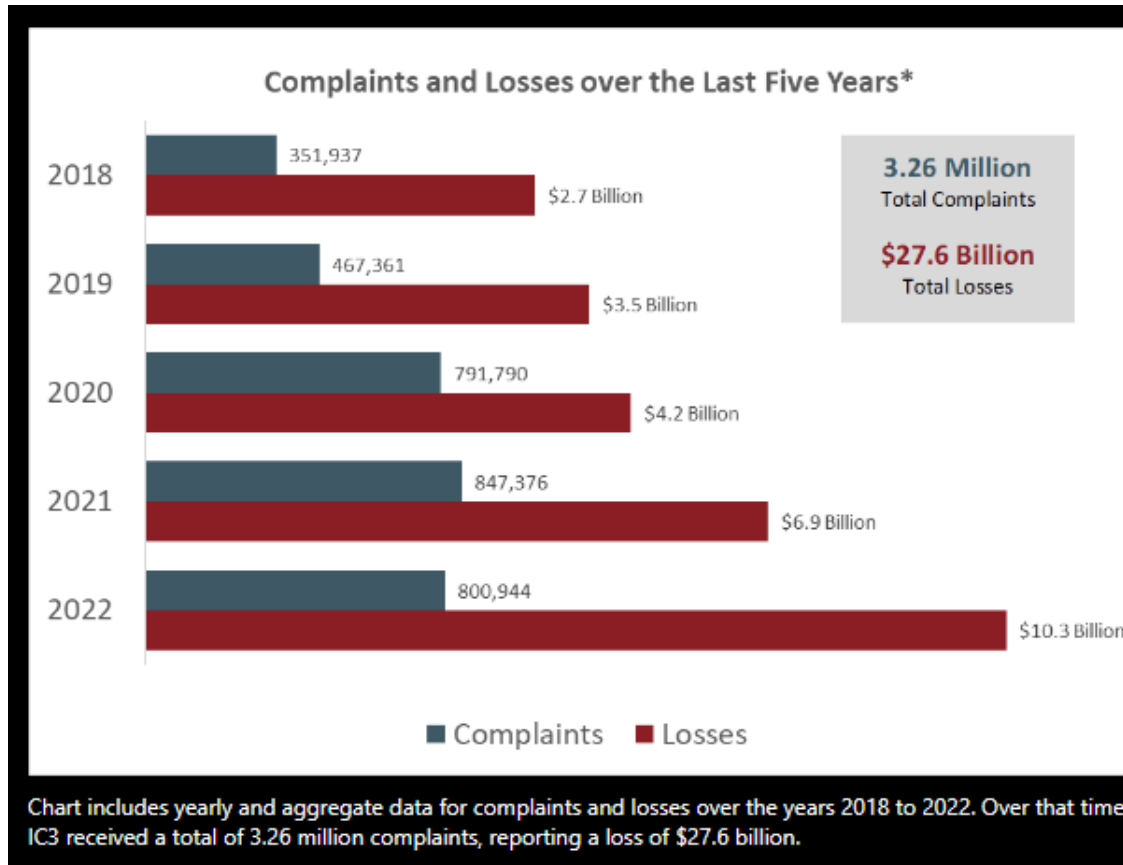
**How:** in writing (“If it’s not in writing, it didn’t happen.”)\*

\*Robert Barrer, Chief Ethics Officer, Barclay Damon LLP

# Pivoting to Funds-Transfer Fraud



# Rising Attacks on Digital Systems



» See <https://www.ic3.gov>.

# How Does It Happen?

Call or e-mail from a trusted source

Sense of urgency (e.g., fraud, theft)

Request for personal information (i.e., login credentials, password, MFA verification)

Threat actor obtains control, transfers funds from client's account to account(s) threat actor controls.

See, e.g.,  
<https://www.ic3.gov/Media/Y2024/PSA240411>.

# What Do You Do?

- » Immediately report to the FBI
  - <https://www.ic3.gov>
  - Client should report – easy to do
  - Include as much detail as possible
    - › Victim’s contact information
    - › Financial-transaction information (account information, transaction date(s) and amount(s))
    - › Subject’s contact information
    - › Specific details of how victimized

# Why Report to the FBI?

- » Financial Fraud Kill Chain (FFKC)
- » Criteria:
  - Wire transfer of \$50,000 or greater
  - International
  - SWIFT recall notice has been initiated
  - Transfer within last 72 hours

See “Fact Sheet on the Rapid Response Program,” Financial Crimes Enforcement Network (FinCEN), Feb. 11, 2022, at 1-3.

# »» Why Report to the FBI?

- » Even if the wire does not meet those criteria, the FBI may be able to
  - tie the fraud to another investigation; or
  - enlist the help of other law enforcement (e.g., the Department of Homeland Security or the U.S. Secret Service)

# Now: How Do You Recover the Stolen Funds?

- » Recovery from threat actor is highly unlikely
- » Recovery from “receiving bank” is likely limited
  - The transferred funds are typically gone before the client or its bank requests a freeze
  - UCC Article 4-A limits a receiving bank’s liability

# Receiving Bank's Limited Liability

- » Article 4-A of New York UCC governs procedures, rights, and liabilities arising out of commercial electronic funds transfers
- » The drafters of Article 4-A “use[d] precise and detailed rules to assign responsibility, . . . allocate risks and establish limits on liability . . . .”

*Grain Traders, Inc. v. Citibank, N.A.*, 160 F.3d 97, 100 (2d Cir. 1998); N.Y. U.C.C. §4-A-102, official cmt.



# Receiving Bank's Limited Liability

---

“If a receiving bank accepts a payment order issued in the name of its customer as sender which is . . . **not authorized and not effective** as the order of the customer under §4-A-202, the bank shall refund any payment of the payment order received from the customer.” N.Y. U.C.C. §4-A-204(1)(a).

---

So for a bank's refund obligations to be triggered under Article 4-A, the payment order must be **neither [1] authorized nor [2] effective**. In other words, if the payment order is *either* authorized *or* effective, the bank bears no refund obligation. *Jajati v. JPMorgan Chase Bank, N.A.*, 2024 U.S. Dist. LEXIS 4703, at \*9-\*10 (E.D.N.Y. Jan. 9, 2024).

# “Effective” = Commercially Reasonable

---

Even if the customer does not *authorize* it, a payment order is *effective* as long as there is a *commercially reasonable* security procedure in place, and the bank accepts the payment order in good faith and in compliance with that security procedure. N.Y. U.C.C. §4-A-202(2).

---

Therefore, if the bank follows commercially reasonable security procedures, a loss resulting from an unauthorized transaction falls on the customer. *See 123RF LLC v. HSBC Bank USA, N.A.*, 2023 U.S. Dist. LEXIS 49920, at \*17 (S.D.N.Y. Mar. 23, 2023).

## Were the Procedures Commercially Reasonable?

Ultimately, the question whether the security procedures are commercially reasonable is a question of law to be decided by a court.

In deciding this question, courts consider:

1. the wishes of the customer expressed to the bank;
2. the circumstances of the customer known to the bank, including the typical size, type and frequency of payment orders normally issued by the customer to the bank;
3. alternative security procedures offered to the customer, and
4. security procedures in general use by customers and receiving banks similarly situated.”

N.Y. U.C.C. §4-A-202(3); *123RF LLC*, 2023 U.S. Dist. LEXIS 49920, at \*17.





# Insurance is the Key Potential Source of Recovery



## Common Sources of Coverage:

Cybersecurity Policy

Crime Policy

Overlapping Coverage

Requires submission of detailed Proofs of Loss and diligent follow-up



Every Business Should Review Its Coverage with Counsel



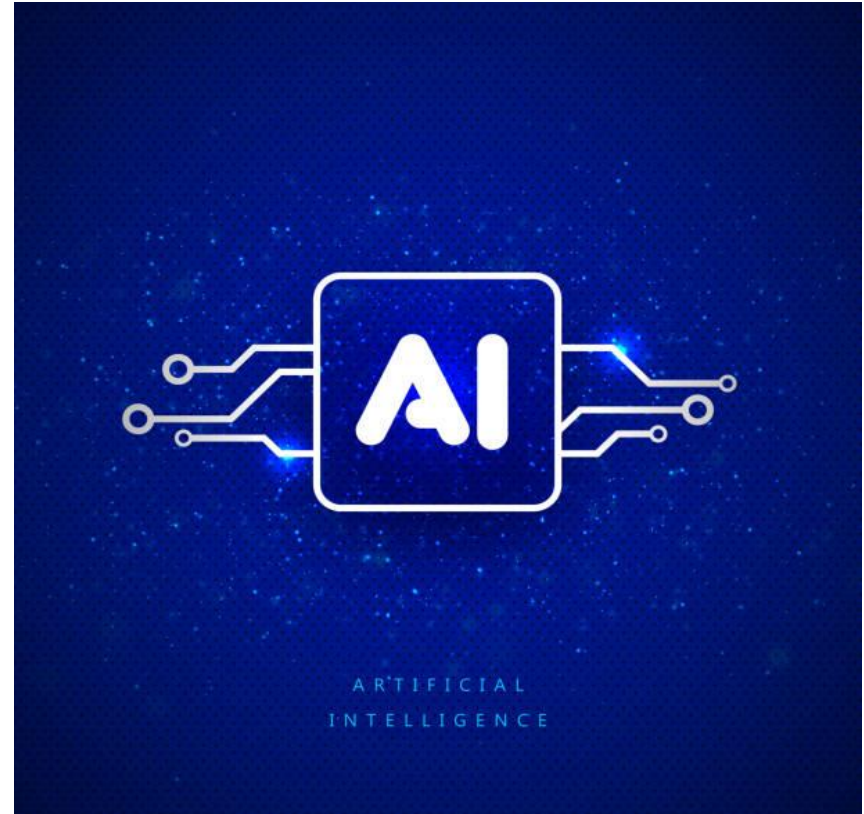
# Artificial Intelligence: The Emerging Compliance Landscape



# »» What is Artificial Intelligence?

- » “**AI**” – the term used to describe how computers can perform tasks normally viewed as requiring human intelligence.
  - Recognizing objects, speech, and word patterns
  - Making decisions based on data
- » “**Machine Learning**” – an application of AI in which computers use algorithms (“rules”) embodied in software to learn from data and adapt with experience.

See Report and Recommendations of the NYSBA Task Force on Artificial Intelligence, as approved by the House of Delegates, Apr. 6, 2024 (“Task Force Report”), at 12.



# »»» What is Generative AI?

## » OpenAI's "Chat**GPT**"

- "generative pretrained transformer"
- Large-language model
  - › Trained on enormous amounts of data (e.g., the Internet)
  - › Once transformer "learns" features of data it is fed, it can be prompted to create more.
  - › Data may be taken from Internet or a proprietary database
  - › Do not recreate the way human brains work; they are "next word prediction engines"

See Task Force Report, at 16-17.

# »» The Benefits of AI

- » Efficiently performs repetitive tasks
- » Reduces human error
- » Increases efficiency
- » Augments human intelligence

See Task Force Report,  
at 20-24.



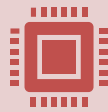
# »» The Risks of AI



- » Hallucinations: fake data, including caselaw
  - » Widening justice gap
  - » Data privacy & surveillance risks
  - » Security risks
  - » Amplification of social biases
  - » Misinformation: “deep fakes”
- See Task Force Report, at 24-28.



# AI Legislative Proposals: Three Main Categories



**Transparency-in-use bills** – covering both AI development and outputs



**Sector-specific bills** – focusing on “high risk” uses of AI to assist with employment, healthcare, and housing issues



**Consumer bills** – focusing on disclosure and opt-outs.

# AI Legislative Proposals: A Few Examples

**Connecticut** – Connecticut Privacy Act, effective 1/1/23, provides consumers the right to opt out of profiling if it is to be used in automated decision-making; HB 1147, introduced 1/29/24 to regulate use of “deep fakes” in communications about candidates for elective office; undisclosed, deceptive “deep fakes” would be prohibited

**District of Columbia** – B114, introduced 2/2/23 to prohibit organizations from using algorithms that make decision

**Massachusetts** – HD. 4788, introduced 1/11/24 to require that any generative AI system used to create audio, video, text or print AI-generated content must make “clear and conspicuous” disclosure

**New York City** – Local Law 144, effective 1/1/23, requires employers to conduct bias audits of AI-enabled tools used for employment decisions

See <https://www.bclplaw.com/en-US/events-insights-news/2023-state-by-state-artificial-intelligence-legislation-snapshot.html>.

# 7 Keys to Consider Before Implementing AI Solutions



- » What does your firm do best?
- » Can AI improve it?
- » What AI program should you implement?
- » How does it work, and what data will it train on?
- » How will you safeguard protected data?
- » Have you put in place a written policy or statement on the use of AI?
- » Have you trained your users?

# »» Misuse of AI for Legal Authority

- » ***Mata v. Avianca***, 2023 U.S. Dist. LEXIS 108263 (S.D.N.Y. June 22, 2023) – attorneys submitted non-existent judicial opinions with fake quotes and citations created by ChatGPT, then continued to stand by the fake opinions after judicial orders called their existence into question.



# Misuse of AI for Legal Authority

- » ***United States v. Cohen***, 2023 U.S. Dist. LEXIS 225233 (S.D.N.Y. Dec. 12, 2023) – attorney directed to provide copies of cited decisions to court or show cause why he should not be sanctioned under Fed. R. Civ. P. 11(b)(2) and (c), 28 U.S.C. §1927, and inherent power of court for citing non-existent cases.

# Misuse of AI for Legal Authority

» *Park v. Kim*, 91 F.4th 610 (2d Cir. 2024) – court refers to Grievance Panel\* attorney who generated citation to non-existent case and then cited case in reply brief.

\*See 2d Cir. L. R. 46.2.

## Wadsworth v. Walmart (D. Wyo.) – 2025



- » “Lead” plaintiff’s counsel used in-house, AI-powered data base to add caselaw to motions in limine
- » Cases were fake, but lead counsel did not catch error
- » “Trial” counsel signed motions without reviewing them
- » Court discovered the fake cases, ordered plaintiff to show cause why court should not impose sanction
- » “Trial” counsel blamed “lead” counsel, who took blame
- » One sanctioned \$1,000; the other sanctioned \$3,000

# Make Sure Your Cases are Real—and That They Stand for the Proposition You Cite Them For

- » Fed. R. Civ. P. 11 applies (*Park*):
  - Rule 11(b)(2) – “[T]he claims, defenses, and other legal contentions are warranted by existing law . . . .
  - Rule 11(c) – Empowering court to impose sanction
- » Courts have inherent power to sanction attorneys for citing non-existent case law to the court (*Cohen*).

# Do NOT Enter Confidential Information Into an Open AI Platform

- The data entered into an AI application is not necessarily confidential or private.
- In using such an application, a lawyer must comply with the RPC and affirmatively take steps to protect client confidential information and communications between the lawyer and the client.

# Wrapping Up . . . .

**Questions:**

[kszczepanski@barclaydamon.com](mailto:kszczepanski@barclaydamon.com)

(716) 858-3834



## Cyber Sip

### Barclay Damon LLP

★ 5.0 (6) · NEWS COMMENTARY · UPDATED BIWEEKLY

Cyber Sip™ is an award-winning biweekly Barclay Damon Live podcast offering practical tips on improving every organization's cybersecurity. We talk with industry thought leaders to keep you up to date on ... [MORE](#)

▶ [Latest Episode](#)

## Episodes >

FEB 18

### Recent Trends in Data Breach Class Actions

In this episode of Cyber Sip, Kevin Szczepanski welcomes plaintiff-side attorney David Lietz, a senior partner at Milberg. David and Kevin take a deep dive into the complexities of data breach class actions, including their evolution, the risks of identity theft, legal standing, and the settlement process. They note the many reasons people give to not join class actions, also pointing out new methods for uppin...

FEB 5

### Navigating the Cyber Insurance Landscape: Trends to Watch

Welcome back to Season 4! In this episode of Cyber Sip, Kevin Szczepanski and Kelly Geary, managing principal of Epic Insurance Brokers & Consultants and national practice leader of Professional, Executive & Cyber Solutions, discuss the current state of the cyber insurance market, the impact of AI on cybersecurity, and the challenges organizations face in implementing effective cybersecurity me...

JAN 22

### Your Laptop Goes Missing! What Do You Do?