

# **AI In Prime Time: New and Evolving AI Laws and Ethical Considerations for Financial Services Attorneys**

CCFL Conference Presentation - May 2025



Sponsored by:  
Conference on Consumer Finance Law

## Overview



- What is AI?
- Ethics & AI
- AI & Financial Services
- Applications & Examples

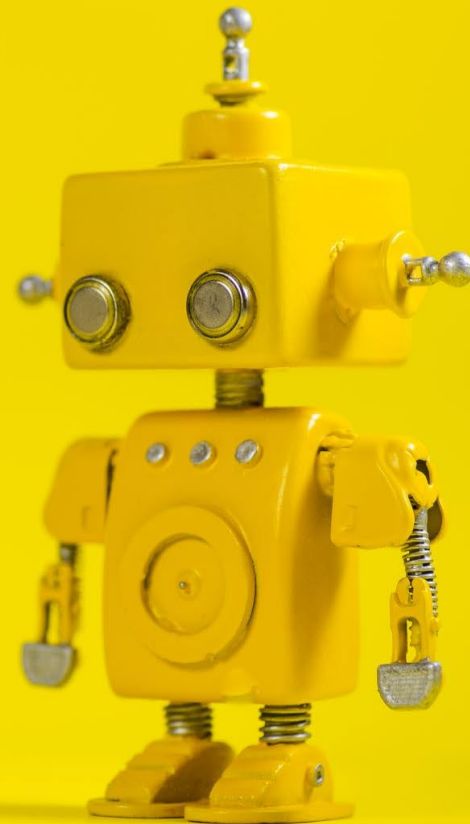
# Disclosure

This presentation is provided for informational purposes only. The presentation is not intended to be an exhaustive review of all laws on any subject. We have made every effort to ensure that the information in this presentation is complete and accurate with respect to the topic(s) addressed. The individual presenter(s) are not responsible for any errors in or omissions from the information provided.

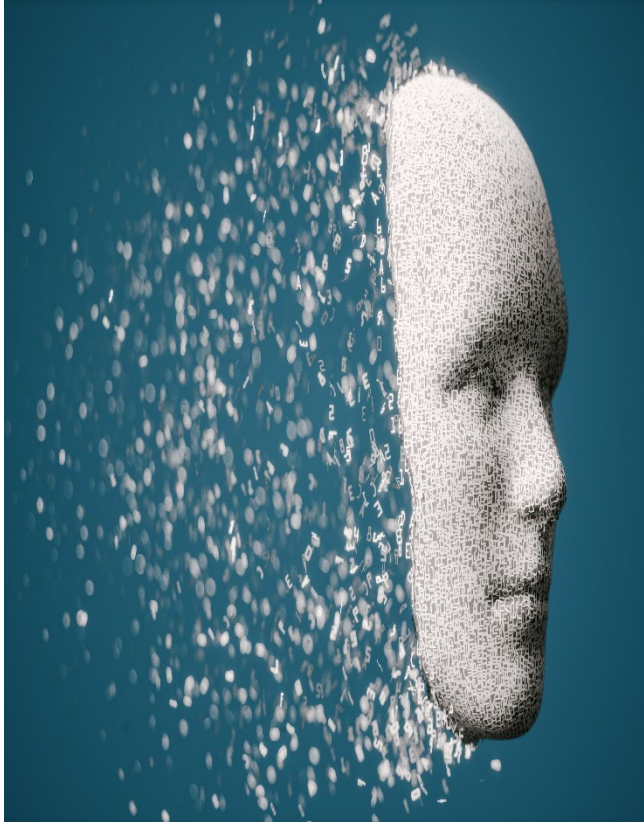
Nothing in this presentation should be construed as legal advice from the individual presenter or their employers, nor is the presentation a substitute for legal counsel on any matter. Legal advice must be tailored to specific facts and circumstances. No attendee of this presentation should act or refrain from acting solely on the basis of any information included in this presentation. Attendees should seek appropriate legal or other professional advice on legal matters specific to their business.

The views and opinions in this presentation are those of the presenter and do not necessarily represent official policy or positions of their employers or any of their employer's clients.

# WHAT IS AI?



# What is Artificial Intelligence?



**Artificial Intelligence (AI)** is a broad term used to describe technology that enables computers and machines to perform tasks that typically require human intelligence, such as learning, comprehension, problem solving, decision making, and creativity.

**Machine Learning** is a subset of AI that enables computers to learn and improve without being explicitly programmed. It focuses on developing computer programs that can learn trends and patterns from data to make predictions or optimizations. This form of “AI” has existed for many years.

**Generative AI** refers to deep-learning models that can generate high-quality text, images, and other content based on the data they were trained on.

**Large Language Models (LLMs)** are a specific type of Generative AI focusing on text generation (e.g., Chat GPT-4), trained on vast amounts of text data to predict and generate coherent text.

# Abbreviated History of AI

---

## Early Developments (1950s-1960s)

AI research begins with efforts to create systems that can mimic human decision-making, laying the groundwork for legal applications. John McCarthy coined the term "artificial intelligence" at the Dartmouth College workshop, marking the formal beginning of the field of AI.

## Expert Systems Conceptualized (1970s)

The concept of "expert systems" was developed in the 1970s by Edward Feigenbaum, a computer science professor at Stanford University and founder of Stanford's Knowledge Systems Laboratory. Expert systems are diagnostic or decision-making systems that ask a structured series of questions, similar to how a human expert might, and then provide a suggested diagnosis or outcome. These systems heavily rely on codified expert knowledge and aim to mimic the ability of a human expert to reach conclusions based on a subject's responses to a series of questions. In this series of questions, the subsequent question typically depends on the response provided to the previous ones.

## Expert Systems in Practice (1980s-1990s)

During the 1980s and 1990s, expert systems were considered the most promising field of AI research for application in the legal profession, partly because solving many legal problems relies on the application of codified knowledge, such as the complicated statutes and extensive case law, along with rule-based decision-making. Richard Susskind's expert system from the late 1980s was a computerized method for navigating the emerging Latent Damages Bill.

## Machine Learning (2000s)

Machine learning algorithms and analytics platforms (e.g., fraud detection platforms, underwriting) enable AI to analyze large volumes of legal data, improving contract analysis and case prediction.

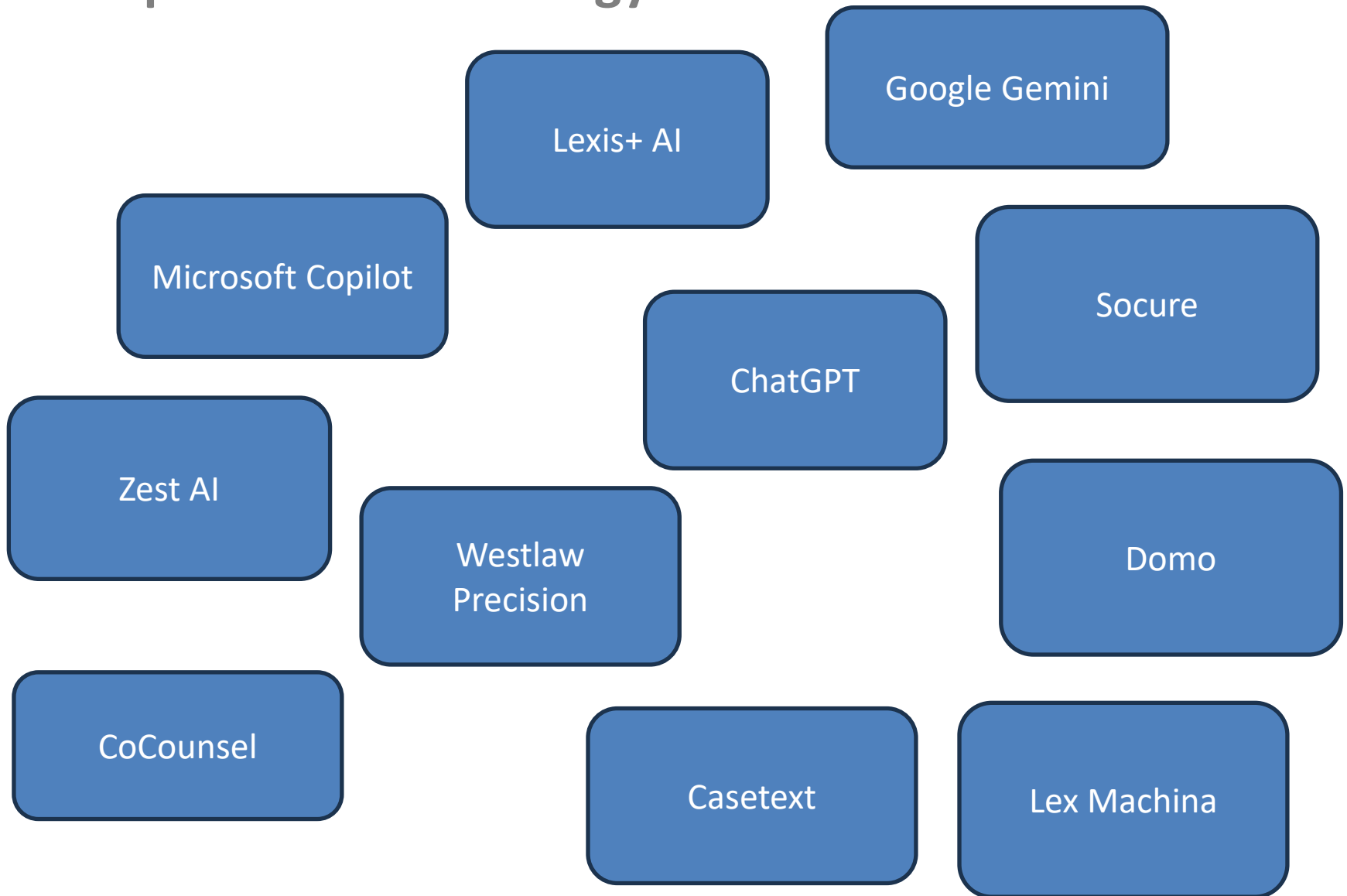
## Modern Applications (2010s-Present)

AI tools, such as natural language processing (NLP) and predictive analytics, are used for contract drafting, legal research, and case management. Machine learning tools (e.g., Kira) assist in contract review and due diligence. Generative AI (e.g., ChatGPT) uses deep learning to create content from large datasets. This allows the creation of new content.



[This Photo](#) by Unknown Author is licensed under [CC BY-SA-NC](#)

## Examples of AI Technology







## AI Use Cases for Legal Departments



**Attorneys are increasingly using AI tools to perform certain legal tasks more efficiently and reduce costs :**

- Drafting/templating communications (e.g., memos, emails, correspondence to opposing counsel, etc.): 58%
- Conducting legal research: 53%
- Summarizing legal narratives: 42%
- Reviewing legal documents: 34%
- Drafting/templating legal contracts: 23%
- Conducting due diligence: 21%
- Reviewing discovery: 15%
- Negotiating/redlining contracts: 11%
- Preparing case filings (e.g., pleadings, motions, jury instructions, etc.): 8%
- Estate planning: 2%

*Source: Bloomberg Law  
(<https://pro.bloomberglaw.com/insights/technology/ai-in-legal-practice-explained/#what-is-artificial-intelligence>)*

# AI Ethics – Duty of Competency

---

## Model Rule 1.1:

- Attorneys must be competent in their work: “[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation necessary for the representation.”
- The ABA adopted revised Comment 8 to this rule in 2012 to clarify that the duty of competence requires a reasonable understanding of the benefits and risks associated with relevant technology. At least 40 states have adopted revised Comment 8.
  - Attorneys must stay informed about technology developments impacting the legal services they offer to their clients.
  - Attorneys may need to attend continuing legal education (CLE) programs or courses on AI technology. Some states (CA, FL, NC, NY) mandate technology-related CLE courses. More states are likely to follow as attorneys increasingly use AI and advanced technology.

## Hallucinations:

- LLMs have a documented tendency to “hallucinate,” or make up false information.
- Models represent billions of connections and as a result it is almost impossible to explain why an LLM responded the way it did when creating output. Due to this unpredictability, users must validate output when accuracy matters.
- Attorneys have been sanctioned for irresponsible use of Generative AI.
  - In a 2023 case, two New York attorneys faced sanctions for citing ChatGPT-invented fictional cases in a legal brief. See *Mata v. Avianca, Inc.*, 2023 WL 4114965 (S.D.N.Y. 2023). The attorneys did not perform any follow up research, and one stated in his defense that “I did not comprehend that ChatGPT could fabricate cases.” The attorneys were fined and their client’s personal injury case against an airline dismissed. <https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/>.
- Possible causes of hallucinations: (1) flawed datasets; (2) flawed training methodologies; and (3) programming that introduce randomness in the creation process, leading to outputs that don’t make sense.

## AI Ethics – Communication

---

### Model Rule 1.4:

- As part of their duty to communicate with their clients, attorneys must “reasonably consult with the client about the means by which the client's objectives are to be accomplished.”
- An attorney that wants to use AI tools to assist with providing legal services should:
  - Inform the client (company) about your intention to use an AI tool for a specific task, detailing the types of client information that will be input into the AI tool, and explaining how that information may be utilized and disclosed.
  - Discuss the benefits, risks, and limitations of using an AI tool with the client.
  - Obtain informed consent to use the AI tool.
- **Using AI tools without your company’s knowledge and approval, could violate Rule 1.4!**
  - “[C]lients would need to be informed in advance, and to give informed consent, if the lawyer proposes to input information relating to the representation into the GAI tool.” ABA Formal Opinion 512.

## AI Ethics – Confidentiality

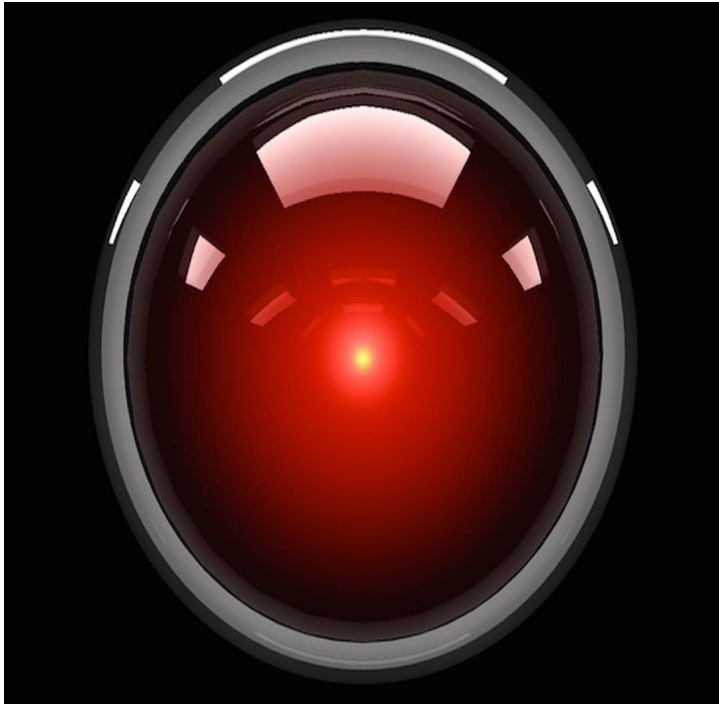
---

### **Model Rule 1.6 (1.9(c) and 1.18(b) for former and prospective client information):**

- Attorneys must not disclose “information relating to the representation of a client unless the client gives informed consent” or the disclosure is otherwise permitted [e.g., prevent death/bodily harm, crime/fraud, comply with court order].
- Self-learning AI tools raise the risk that client information may be disclosed improperly (even if exclusively used by employees in same company or firm).
- Know the capabilities and limitations of the AI tool you are using!
  - Read the terms of use, privacy policy and other policies related to the AI tool.
  - Know whether and how an IA tool protects information from improper disclosure – private versus public tools.

# Tips for Using AI Tools Effectively and Responsibly

---



[This Photo](#) by Unknown Author is licensed under [CC BY-NC-ND](#)

- **VERIFY, VERIFY, VERIFY.** Always read output carefully and edit, as necessary. Never send out output that you have not reviewed to a client.
- Understand the capabilities and limitations of the AI tools that you (and your company) use and manage AI service providers.
- Never compromise confidential client data by inputting into an AI tool that does not have appropriate safeguards.
- Be clear and specific in our prompts about what you want the AI tool to do for you, providing as much context and detail as possible.
- Understand that the AI tools are still learning and developing and may not always meet your expectations.
- AI tools are not a replacement for legal work prepared by a skilled attorney.
- Scrutinize your company's use of AI – flawed data can introduce bias into outputs; Generative AI can create outputs with incorrect information, IP infringement issues, deepfakes, personal information, etc.
- Even if an attorney takes all necessary precautions when using an AI tool, if the tool fails to complete the assigned task, makes an error, or inadvertently discloses client data, it is the attorney that is ultimately responsible to the client.

*"A.I. will probably most likely lead to the end of the world, but in the meantime, there'll be great companies."* Sam Altman, OpenAI CEO.

# AI IN FINANCIAL SERVICES



# AI in Financial Services: A Legal Flashpoint

- AI is transforming financial services—and drawing scrutiny.
- AI systems drive underwriting, fraud detection, and servicing decisions.
- Regulators are applying legacy laws (ECOA, FCRA, UDAAP) to AI tools.
  - *Circular 2022-03*, CFPB: Entities must comply with adverse action notice requirements even when using complex algorithms.
- AGs and legislatures are advancing targeted AI laws to close perceived gaps.
- Enforcement risk is rising across all credit-related automation functions.
  - State AI laws are being passed rapidly (e.g., CO SB 205), and the regulatory environment is no longer hypothetical.



# ECOA, UDAAP, and the FCRA

- **Equal Credit Opportunity Act (15 U.S.C. § 1691 et seq.) and Regulation B**
  - Applies to credit decisions made using AI, including scoring or eligibility tools.
  - Requires 'specific reasons' for adverse actions—even if derived from complex ML models.
  - The creditor must be able to provide a specific and accurate explanation, even if the algorithm is not transparent. *Circular 2023-03*, CFPB.
- **Unfair, Deceptive, or Abusive Acts or Practice (UDAAP)**
  - Opaque or biased AI outputs may constitute unfair or abusive practices.
  - Systems must be explainable, predictable, and regularly tested for discriminatory impact.
- **Fair Credit Reporting Act (FCRA)**
  - AI use in credit eligibility or reporting must comply with dispute, reinvestigation, and accuracy rules.
  - AI systems that generate consumer reports or make eligibility decisions may trigger FCRA obligations.
  - Dispute resolution, data accuracy, and reinvestigation obligations apply.
  - Institutions cannot rely on vendor automation to avoid liability under 15 U.S.C. § 1681i



# Profiling and Automation

- **California Privacy Rights Act (CPRA)**
  - Provides access, deletion, and opt-out rights for consumers - Cal. Civ. Code § 1798.121.
  - Proposed ADMT regulations would require notices for ADMT use and profiling risk assessments. California Privacy Protection Agency, Notice of Proposed Rulemaking: CCPA Updates, Cybersecurity Audits, Risk Assessments, Automated Decision-making Technology (ADMT), and Insurance Companies, (Nov. 22, 2024).
- **Colorado Privacy Act (CPA)**
  - Colo. Rev. Stat. § 6-1-1701 et seq. (Effective Feb. 1, 2026)
  - First comprehensive state AI law
  - Applies to high-risk AI systems, defined to include those making decisions about “financial lending services”
  - Key Requirements for both Developers and Deployers
- **Utah Artificial Intelligence Policy Act (UAIPA)**
  - Establishes liability for use of artificial intelligence (AI) that violates consumer protection laws if not properly disclosed.
  - Requires disclosure when an individual interacts with AI in a regulated occupation.
- **Secondary Use Restrictions**
  - Re-use of consumer data for AI training may require new consent under state privacy laws.
  - Violations may also constitute deceptive practices under UDAP statutes.

# California's Recent AI Legislation

- **AB 2013 (2024)**
  - Effective January 1, 2026
  - Public Disclosure Obligation: Developers of generative AI systems must post a public summary of the datasets used to train their models on a publicly accessible website.
  - Content of Dataset Summary:
    - The source or owner of each dataset;
    - The purpose of each dataset in the training process;
    - The approximate number and type of data points; and
    - Whether the dataset contains copyrighted material or personal information.
  - Timing Requirement: The disclosure must be made prior to or concurrent with making the generative AI system available for use in California.
  - Enforcement & Scope: Applies to any developer that makes a generative AI model available in California and is not limited to California-based companies—potentially giving the law extraterritorial effect.

# California's Recent AI Legislation

- **SB 942 – California AI Transparency Act (2024)**
  - Effective January 1, 2026
  - Free AI Detection Tool: Providers must offer a public tool to identify whether content (image/audio/video) was AI-generated.
  - Manifest Disclosure Option: Users must be able to add an “AI-generated” label to content in a clear, understandable way.
  - Latent Disclosure Required: Providers must embed provenance metadata or link to source info when technically feasible.
  - License Revocation: Providers must revoke licenses from third parties who strip out required disclosures.

# Federal Developments

- **Executive Order 14110 (2023)**
  - Outlined government-wide AI safety and transparency principles under the Biden Administration.
  - Now rescinded; future direction under new administration expected to be less prescriptive.
- **NIST AI Risk Management Framework (2023)**
  - Voluntary but widely used.
  - Framework:
    - MAP
    - MEASURE
    - MANAGE
    - GOVERN
  - Provides structure for internal AI governance aligned with federal expectations.
- **NTIA AI Accountability Report (2024)**
  - Recommends documentation, audits, and external evaluation of high-impact AI.
  - Encourages transparency measures even without regulation.

# Outside the US

- **European Union Artificial Intelligence Act (2024)**
  - Regulation (EU) 2024/1689
  - Applies extraterritorially to US-based providers targeting EU markets.
  - Classifies AI systems into risk tiers; high-risk systems require CE certification, audits.
    - Unacceptable
    - High
    - Limited
    - Minimal
  - High-Risk System Obligations: High-risk systems (e.g., for creditworthiness) require compliance with risk management, data governance, transparency, human oversight, and conformity assessments.
  - Transparency Requirements: Requires that users are informed when interacting with AI systems, including AI-generated content and emotion recognition systems.
  - Market Surveillance & Penalties: Establishes a European AI Board, national supervisory authorities, and imposes fines of up to €35 million or 7% of global turnover for preceding year for violations.

# Best Practices for Financial Services

- **Inventory and Classification**
  - Maintain a current inventory of all AI and ADMT systems across business units.
  - Classify tools based on use case and legal impact.
- **Risk and Impact Assessments**
  - Conduct pre-deployment testing for bias, fairness, and explainability.
  - Document findings and remediation steps.
- **Consumer Disclosures and Appeals**
  - Provide layered notices where AI affects legal or financial rights.
  - Offer a meaningful human review pathway for AI-driven decisions.
- **Vendor and Government Oversight**
  - Include audit rights, model documentation, and legal compliance terms in vendor contracts.
  - Designate internal teams for AI monitoring, escalation, and policy updates.

# Looking Ahead to 2025

- **Regulatory and Enforcement Trends**
  - More states are expected to introduce or pass AI-specific legislation this year.
  - Attorneys General are actively investigating algorithmic harms: bias, deception, and unfair outcomes.
  - Regulatory agencies are leveraging existing authorities to police AI misuse.
- **Litigation and Risk Management**
  - Expect increase in FCRA, ECOA, and privacy-based litigation tied to AI usage.
  - Best defense is proactive governance, transparency, and risk documentation. AI governance is new data governance.



A blue-toned image of a robotic hand, possibly a prosthetic or a futuristic robot arm, hovering over a surface that appears to be a digital data display or a circuit board. The hand is composed of various mechanical joints and segments, with a glowing blue light emanating from its palm. The background is dark and filled with blurred, glowing lines and patterns, suggesting a high-tech or digital environment. The overall aesthetic is futuristic and technological.

# APPLICATIONS THROUGH EXAMPLES



# Putting It All Together:

Issue Spotting AI and Ethical Issues with some Examples

A Biometrics Integration

An Entity/Account Validation Project

Information Only Clearing/Matching

# A Biometric Integration



- Business team says they want to start using faces in lieu of authorized persons for validations of payments.
- They have identified a third-party they are ready to work directly with.

Laws Applicable to Financial Institutions where AI may shift application

- Model risk Requirements
- Third Party Oversight
- UDAAP and/or anti-discrimination
- Privacy Laws & Regulations

Ethical Considerations for Counsel

- Duty of Competence

# An Entity/Account Validation Project



- Business team says they want to start offering ability of customers (business and consumer) to validate accounts and individuals for services.
- Business team wants to use a mix of Company data and third-party data.
- Business team is interested in using scoring models that use AI.

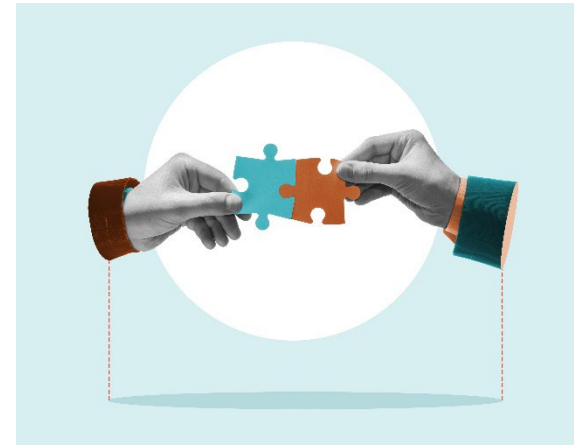
Laws Applicable to Financial Institutions where AI may shift application

- Model risk Requirements
- Third Party Oversight
- UDAAP and/or anti-discrimination
- Fair Credit Reporting

Ethical Considerations for Counsel

- Duty of Competence

# Information Only Clearing/Matching



- Business team says they want to start offering invoice to payment matching for B2B and B2C customers.
- Business team wants to use a third-party solution with Company directed enhancements storing data on Company servers.
- Business wants to use a priority/recommendation queue for customers that involves AI.

Laws Applicable to Financial  
Institutions where AI use may  
shift application

- Model Risk Requirements
- Third Party Oversight
- UDAAP and/or anti-discrimination
- Fair Debt Collection Practices Act
- Privacy Laws & Regulations

Ethical Considerations for  
Counsel

- Duty of Competence



# QUESTIONS?

# **APPENDIX**

## AI Ethics Resources

---

- **American Bar Association** – Formal Opinion 512 ([https://www.americanbar.org/content/dam/aba/administrative/professional\\_responsibility/ethics-opinions/aba-formal-opinion-512.pdf](https://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/ethics-opinions/aba-formal-opinion-512.pdf))
- **California** – Practical Guidance for the Use of Generative AI in the Practice of Law (<https://www.calbar.ca.gov/Portals/0/documents/ethics/Generative-AI-Practical-Guidance.pdf>)
- **D.C.** – Ethics Opinion 388 (<https://www.dcbart.org/For-Lawyers/Legal-Ethics/Ethics-Opinions-210-Present/Ethics-Opinion-388>)
- **Florida** – Ethics Opinion 24-1 (<https://www.floridabar.org/etopinions/opinion-24-1/>)
- **Mississippi** – Ethics Opinion No. 267 (<https://www.msbar.org/ethics-discipline/ethics-opinions/formal-opinions/267/>)
- **Missouri** – Informal Opinion 2024-11 (<https://mo-legal-ethics.org/informal-opinion/2024-11/>)
- **New Mexico** – Formal Opinion 2024-004 ([https://www.sbnm.org/Portals/NMBAR/GenAI%20Formal%20Opinion%20-%20Sept\\_2024\\_FINAL.pdf](https://www.sbnm.org/Portals/NMBAR/GenAI%20Formal%20Opinion%20-%20Sept_2024_FINAL.pdf))
- **New York** – Report and Recommendations of the New York State Bar Association Task Force on Artificial Intelligence (<https://nysba.org/app/uploads/2022/03/2024-April-Report-and-Recommendations-of-the-Task-Force-on-Artificial-Intelligence.pdf>)
- **New Jersey** – Preliminary Guidelines on the Use of Artificial Intelligence (<https://www.njcourts.gov/notices/notice-legal-practice-preliminary-guidelines-use-of-artificial-intelligence-new-jersey>)
- **Pennsylvania/Philadelphia** – Joint Formal Opinion 2024-200 (<https://www.pabar.org/Members/catalogs/Ethics%20Opinions/Formal/Joint%20Formal%20Opinion%202024-200.pdf>)
- **Kentucky** – Ethics Opinion KBA E-457 ([https://cdn.ymaws.com/www.kybar.org/resource/resmgr/ethics\\_opinions\\_\(part\\_2\)/kbae457artificialintelligenc.pdf](https://cdn.ymaws.com/www.kybar.org/resource/resmgr/ethics_opinions_(part_2)/kbae457artificialintelligenc.pdf))
- **N. Carolina** – 2024 Formal Ethics Opinion 1 (<https://www.ncbar.gov/for-lawyers/ethics/adopted-opinions/2024-formal-ethics-opinion-1>)
- **Texas** – Opinion 705 (<https://www.legalethicstexas.com/resources/opinions/opinion-705/>)
- **Virginia** – Guidance on Generative AI (<https://vsb.org/Site/Site/lawyers/ethics.aspx>).
- **West Virginia** – Legal Ethics Opinion 24-01 (<https://storage.googleapis.com/msgsndr/Rgd68xOkcVdteTsBkf6O/media/667ac9c219bb7a1f7a4df4c2.pdf>).

## About Our Speakers

---



**Webb McArthur, Partner**

[wmcarthur@hudco.com](mailto:wmcarthur@hudco.com)

202.715.2012

Webb helps financial institutions and technology companies navigate the evolving landscape of data privacy and consumer financial regulations. As a partner in our Washington, DC office, he advises a broad range of financial institutions, consumer reporting agencies, data brokers, data providers, and technology firms on compliance with federal, state, and international data use and privacy laws. His practice focuses on the Fair Credit Reporting Act, the Gramm-Leach-Bliley Act, state consumer data privacy laws, General Data Protection Regulation, prohibitions against unfair, deceptive, and abusive acts and practices, and other privacy and security laws and regulations.

HUDSON  
COOK



## About Our Speakers

---



### **David Bowen, Of Counsel**

[dbowen@kdlegal.com](mailto:dbowen@kdlegal.com)

312-235-1116

David Bowen is a member of Krieg DeVault's Financial Institutions Practice, where he provides comprehensive counsel on consumer and commercial financial services. His practice focuses on regulatory compliance, consumer lending, electronic payments, electronic contracting, commercial transactions, corporate governance, privacy, and cybersecurity. David brings extensive experience in navigating complex regulations, managing teams, and advising executives on high-stakes legal matters.

David advises clients on a wide array of financial laws and regulations, including the Consumer Financial Protection Act, Gramm-Leach-Bliley Act, Fair Credit Reporting Act, Truth-in-Lending Act, CARD Act, Equal Credit Opportunity Act, E-SIGN Act, Electronic Funds Transfer Act, Federal Trade Commission rules, Telephone Consumer Protection Act, California Consumer Privacy Act, Articles 3 and 9 of the Uniform Commercial Code, and state consumer protection laws.

Active in both financial and civic organizations, David was a member of the American Financial Services Association Law Committee and the Association of Corporate Counsel.



## About Our Speakers

---



**Julia Riley, Assistant General Counsel & Director**

[julia.riley3@bofa.com](mailto:julia.riley3@bofa.com)

Julia is an attorney for Bank of America's Global Payments Services group supporting Deposits, Liquidity and Receivables for business, commercial, large corporate and financial institution customers.

With extensive background in corporate banking transactional and product advisory legal work her experience spans a broad spectrum of legal areas, including contract law, international regulations, administrative law, and financial services law. Julia's prior roles also include focused work on data use, artificial intelligence/machine learning and privacy issues particularly in the payments, FinTech, and innovative banking solutions.