

# AI and Emerging Technologies

## CORPORATE

### Is Your Board Thinking Strategically About Emerging Tech?

The job of a public company director is only getting harder and harder as the landscape within which companies operate seems to be changing faster than ever. Gone are the days when only companies with explicitly technology-driven lines of business need technical expertise and strategic thinking in the board room. As the pace of change increases and emerging technologies impact how companies do business across sectors, boards need to develop an intentional approach to managing the risks and capitalizing on the opportunities presented by the new economy. As a starting point, boards should consider asking themselves the following questions to make sure they are safeguarding the long-term success of their companies.

#### **Is your board thinking about more than just the risks associated with emerging technology?**

Boards are absolutely responsible for overseeing and managing the risks associated with a company's use of emerging technology. Quite explicitly, the US Securities and Exchange Commission (SEC) [adopted new rules](#) last year that implement required disclosures related to cybersecurity risk management and governance, and those disclosures should be talking about how boards or board committees are involved in the process. We've also seen the SEC initiate [enforcement actions](#) against companies for alleged misstatements in cybersecurity-related disclosures in the wake of widespread cyber incidents. To be clear, the emphasis by boards on the inherent risks of technology is not unfounded. In addition to cybersecurity considerations, the risks associated with a company's use of generative AI or blockchain and digital assets should be in the focus of the board's risk management oversight responsibilities. Making sure a company is managing risks is always a board responsibility.

With that said, too often boards are **only** focused on the risks presented by emerging technology, and not also curious and thinking strategically about the opportunities presented by such technological advances. In this hypercompetitive economy, the ability for a company to think strategically and intentionally about how technology can provide an advantage in the market can make a huge difference. The ability to innovate and appropriately invest in the right technological solutions sits squarely in the strategic thinking function of the board and boards that have invested time in creating governance structures that support strategic thinking around technology have benefited in the short- and long-term.

The board is in a perfect position to leverage its bird's eye view of a company and the market in which it operates. Boards can use that high level thinking, combined with the hopefully diverse viewpoints and backgrounds of the directors, to evaluate the potential opportunities associated with long-term investments in technology. If your company isn't thinking about how technology can make it better, faster, more efficient and more profitable, its likely your competitor is and it is always better to be at the table than on the table.

#### **Does your board's governance structure support strategic thinking about emerging technology?**

In the last five years, we've seen an increase in the number of public company boards that have a dedicated technology committee. Based on our own review of Fortune 500 companies over the last five years, we estimate that the number of public companies with a board committee focused specifically on technology has increased over 5 percent to just over 20 percent as of the 2024 proxy

season. Because technology committees are not a required board committee, boards have flexibility in defining the focus and responsibilities of such committees and their approach to evaluating and prioritizing a company's investment in technology which can be tailored to the specific industry or business goals.

Ultimately, a technology committee's ability to focus on a rapidly shifting technology landscape can bring important strategic opportunities into focus for the full board and help guide management to invest time and resources in the technologies that make the most sense. With that said, it is certainly not the case that every public company needs a dedicated technology committee and many companies might determine it is more appropriate to delegate this kind of strategic thinking to a different standing committee or keep it on the full board's agenda. Either way, the important exercise is asking the question: *Is our board's governance structure designed to manage the risks associated with technology and also think strategically about the opportunities new technology presents to ensure the long-term strength and competitiveness of the business?* Even if a dedicated technology committee isn't the right approach for your company, making sure the board's governance structure and annual agenda includes a focus on emerging technology is critical.

### **Is your board equipped with the right tools to succeed at thinking strategically about technology?**

Assuming the board gets to a place where it is thinking about both the risks and opportunities about emerging technology and its governance structure is aligned to

support that strategic priority, boards also need to make sure their directors are equipped with the necessary knowledge and access to experts to be effective thought leaders regarding emerging technology. Governance experts and consultants have spilled a lot of ink discussing the relative shortage of technology experts on public company boards. Given such a competitive market for directors with expertise in emerging technology, ensuring that board education and agendas fill any potential knowledge gaps for directors without such expertise is important. As a board engages in strategic thinking about technology, it must be able to evaluate its opportunities while also maintaining a focus on actionable, realistic investments or valuable resources. Even the most experienced technologists have to be intentional not to get distracted by the emerging tech trends that capture the most headlines at any given moment at the expense of missing the technology solutions that are truly worth the investment.

Board education can include bringing in outside resources and consultants, but looking internally is also a valuable approach to board education. Internal resources can be particularly helpful when it comes to a board or technology committee understanding the specific ways investment in technology may add value to their company. Bringing senior managers from the technology-focused business units into board-level discussions about a company's technology priorities may shine a light on areas where immediate or modest strategic investments in emerging technology can make a huge difference to the bottom line.

No matter where your company is on the path to embracing the opportunities technology may offer, it is critical to make sure that your board is at least considering its role in the process. There is nowhere to hide anymore as emerging technology is rapidly changing the way companies do business regardless of their industry. Keeping the risks associated with technology in sharp focus is absolutely the first priority for any board managing its duties of risk oversight. But boards that are thinking strategically about how their companies can properly embrace technology's evolving suite of tools will be at an advantage compared to peers that are slower or more resistant to change.



**Blockchain Legal Resource**  
ANALYSIS AND INSIGHT IN BLOCKCHAIN LAW

**Subscribe to receive the latest blockchain law insights delivered to your email.**



**Mayme Beth F. Donohue**  
Partner, Richmond

---

## INTELLECTUAL PROPERTY

# The USPTO Issued Additional (New) AI Guidance on Patent Subject Matter Eligibility

In a February 2024 client alert, [A Brief Explanation of the USPTO's Useful New AI-Assisted Invention Guidance](#), as well as in the [AI and Emerging Technologies Spring 2024 Newsletter](#), we discussed the US Patent and Trademark Office (USPTO)'s [Inventorship Guidance for AI-assisted Inventions](#), 89 Fed. Reg. 10043 (Feb. 13, 2024).

In mid-July, the USPTO released another set of AI guidance, focusing on patent subject matter eligibility: [2024 Guidance Update on Patent Subject Matter Eligibility, Including on Artificial Intelligence](#), 89 Fed. Reg. 58128 (Jul. 17, 2024). This follows the aforementioned February guidance, as well as [Guidance on Use of Artificial Intelligence-Based Tools in Practice Before the USPTO](#), 89 Fed. Reg. 25609 (Apr. 11, 2024), and [Director Guidance on party and practitioner misconduct related to use of AI](#) (Feb. 6, 2024). Additionally, the USPTO has a [one-stop AI webpage](#).

Effective as of July 17, 2024, the new guidance should be viewed in concert with that which came before it, and covers two primary bases: 1) addressing patent eligibility of AI-related inventions and 2) further explaining Step 2A of the

USPTO's eligibility analysis. Also released with the guidance are [three examples](#), following the format of the USPTO's previously-released subject matter eligibility examples and providing an exemplary application of the guidance.

### The USPTO's Subject Matter Eligibility Framework is Not Changed

The first, and perhaps most critical, takeaway from the new guidance is that AI-related inventions do not get any special treatment. These inventions will be examined under the existing patent framework.

In sum, the USPTO's eligibility framework consists of two main steps. Step 1 is an assessment of whether the invention for which patent protection is sought falls within a statutory category (i.e., process, machine, manufacture or composition of matter). Step 2 applies the Supreme Court's *Alice/Mayo* analysis to identify whether the patent claims are directed to a judicial exception and then to evaluate whether additional elements in the claim provide an inventive concept. Step 2 has two sub-steps: Step 2A (that includes Prong One and Prong Two) and Step 2B.



---

## Updates to the Guidance

The new guidance notes that stakeholder feedback to prior guidance identified two areas of “particular concern” regarding patentability of AI-related inventions: “(1) the evaluation of whether a claim recites an abstract idea in Step 2A, Prong One; and (2) the evaluation of the improvements consideration in Step 2A, Prong Two.” The guidance admits that Step 2A, Prong One may be “challenging for AI inventions.” This is likely because “it is common for claims to AI inventions to involve abstract ideas.” The guidance directs USPTO personnel to distinguish “between a claim that ‘recites’ an abstract idea (and thus requires further eligibility analysis) and one that merely involves, or is based on, an abstract idea.”

To address the concerns, the guidance refers to recent case law updates on mathematical concepts, certain methods of organizing human activity, and mental processes, “which may be useful to USPTO personnel and stakeholders in evaluating Step 2A, Prong One.” And for Step 2A, Prong Two, the guidance discusses “how to demonstrate an improvement for AI inventions and recent case law that may be helpful in demonstrating such an improvement.”

The guidance then proceeds to walk through Step 2A, Prong One (whether a claim recites an abstract idea), providing hypothetical examples, as well as examples from recent case law. Next, it goes through Step 2A, Prong Two in a similar manner, relying primarily on case law examples and discussion of AI inventions and how such fit into this step.

The guidance finally notes that, whether an invention is developed with AI is not a consideration in the eligibility analysis, referencing prior guidance on AI-assisted inventions. Critically, the USPTO reinforces that “AI-assisted inventions are not categorically unpatentable.”

## New Examples

As mentioned above, the guidance includes three new examples, numbered 47 to 49 (46 examples pertaining to other technologies in the context of the eligibility framework were previously issued). First, Example 47 applies the eligibility analysis to claims related to “the use of an

artificial neural network to identify or detect anomalies.” Next, Example 48 applies the eligibility analysis to claims reciting “AI-based methods of analyzing speech signals and separating desired speech from extraneous or background speech.” Finally, Example 49 applies the eligibility analysis to claims reciting “an AI model that is designed to assist in personalizing medical treatment to the individual characteristics of a particular patient.” While the examples are narrowly focused on certain AI-related technologies, they demonstrate application of the framework in different scenarios, and are instructive at least from that aspect.

## Future Challenges and Takeaways

This was a crucial step from the USPTO to attempt to clarify how its eligibility framework applies to AI-related inventions.

During patent prosecution, it is critical to understand how the eligibility framework is applied, as well as where to focus arguments in response to rejections. Ensuring that a patent specification provides sufficient technical details, including the areas of improvement offered by the invention, is critical because such technical details may be needed to reinforce the claims through amendments to overcome a subject matter eligibility rejection. Further, establishing a dialogue with the examiner is important, as many examiners will provide suggestions on claim amendments to overcome an eligibility rejection.

Patent applicants should review this guidance and apply it as best they can in developing their own AI-related inventions to try to avoid (or overcome) a subject matter eligibility rejection. While the hypotheticals and examples in the guidance are limited to specific applications, an applicant can attempt to match his/her own invention to one of them.



**Steven L. Wood**  
Counsel, Washington, DC



---

## LABOR AND EMPLOYMENT

# DOL's Wage & Hour Division Delivers Guidance on AI

On April 29, 2024, in compliance with [President Biden's October 2023 Executive Order](#) addressing artificial intelligence, the Department of Labor's Wage & Hour Division (WHD) issued guidance regarding the potential risks posed by employers using AI tools to monitor or augment worker productivity to violate the Fair Labor Standards Act (FLSA). The 12-page [Field Assistance Bulletin](#) No. 2024-1 (FAB) covers more than just the expected topics, such as hours worked and wages paid, it also touches on AI's implications for other worker protection laws, like the Family and Medical Leave Act (FMLA), the recently-effective Providing Urgent Maternal Protections for Nursing Mothers Act (PUMP Act), as well as the Employee Polygraph Protection Act (EPPA).

It is worth noting that this FAB is agency guidance to its investigative staff. A FAB is not binding regulation. As the DOL acknowledges, FABs "provide positions reflecting changes or clarifications in the administration of laws and related regulations based upon court decisions, legislative changes and opinions of the WHD Administrator."

### Tracking Time Worked

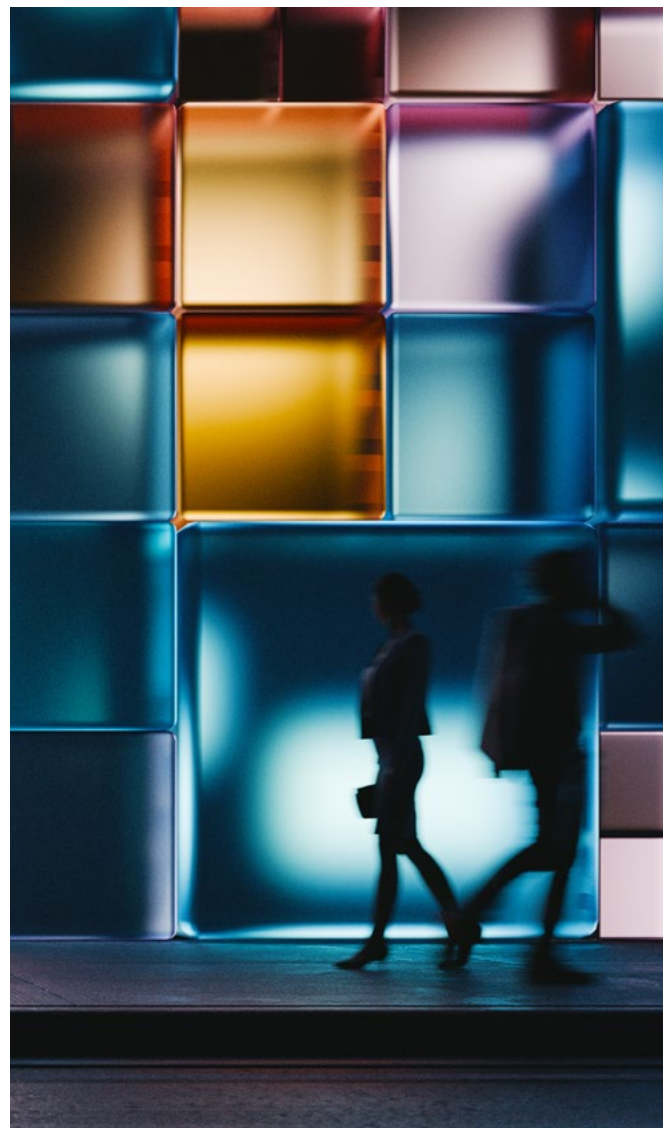
The first half of the FAB is devoted to outlining the risks that AI poses when used to monitor employee productivity and break time. The WHD flags AI or automated systems that companies may use to track when employees are actively working or are idle, potentially by monitoring computer keystrokes, mouse clicks, or an employee's presence in front of a computer's camera, etc. Employers are reminded that time spent working must be paid "regardless of the level of productivity or performance of the employee," so these tracking systems are not determinative of whether the employees' time is "work time," and thus compensable.

Likewise, software or AI systems that predict when and if an employee has taken a break may not be 100% accurate and may conflate non-computer work time with break time. Breaks are non-compensable only when workers are fully relieved of their duties—a subjective assessment that may not be well suited to computer automation. For workers who might be assigned tasks by an automated system, such as warehouse workers, time spent waiting on the system to assign a task may be compensable when the employee is not free to use that time for their own purposes. Under the FLSA, this "engaged to wait" time is compensable.

Finally, the FAB warns that AI-powered systems that use geolocation to track employee "clock-ins and -outs" may not adequately account for worker tasks that occur at multiple locations or locations away from the "main" office. Using

construction workers as an example, the WHD notes that time spent at job sites without geolocation infrastructure, or time spent traveling between job sites, might not be appropriately tagged as compensable work time by the system. Analogously, workers whose job responsibilities include intermittent travel outside of an office setting, like non-commissioned salespeople, could face similar issues.

A discussion of worker monitoring using AI would be incomplete without noting that the National Labor Relations Board will be taking a hard look at AI systems that are used to surveil workers. Indeed, the FAB references the NLRB's guidance in its own and cautions that AI-based surveillance may constitute retaliation under the FLSA as well. More coverage of the NLRB guidance can be found in a prior post by Hunton attorneys.



## Calculating Wages

The FAB moves on to address use of AI or automated systems to calculate workers' wage rates, including systems that combine different wage rates, e.g., hourly and piece rate depending on the task. In an apparent reference to "gig workers," the FAB spotlights algorithms that determine workers' rates of pay based on "fluctuating supply and demand, customer traffic, geographic location, worker efficiency or performance, or the type of task performed by the employee." Even where such tools and data are utilized, the calculation for minimum wage is still the same: total pay divided by number of hours worked.

## Other Worker Protection Laws Potentially Impacted by AI

The remainder of the FAB addresses other workplace areas where workers are protected by laws administered by the DOL and where AI might pose risks.

Under the FMLA, workers become eligible for protected leave after 12 months of employment and 1,250 hours of service. Based on the same flaws that AI could exhibit in monitoring break time, these systems may also miscalculate an employee's hours of service, leading to an improper eligibility determination for coverage under FMLA. Additionally, once the automated system determines that an employee is eligible for FMLA leave, the employers are not permitted to "retest" the employee's eligibility until the beginning of a new 12-month period or upon a different FMLA request. A system that continually tracks eligibility under FMLA violates this rule. Once an FMLA leave request is made, employers may request that an employee submit a certification for the need to take FMLA, i.e., a "doctor's note." An AI system that determines the sufficiency of this health care provider's certification is at risk of requesting more medical information from the employee than the law permits. Because the FMLA provides an independent cause of action for workers, any or all of these scenarios could expose an employer to liability under the law.

The FAB also addresses the 2023 PUMP Act, which guarantees "reasonable break times" for nursing mothers to express breast milk at work. Reiterating AI's potential problems tracking break time, the FAB warns employers against penalizing nursing mothers for taking lactation breaks. An automated system that considers breaks taken to assign "productivity scores," or to determine future work scheduling, could violate the FLSA if it uses these inputs to negatively impact nursing mothers.

The rarely-mentioned Employee Polygraph Protection Act received some attention in the FAB, with the WHD cautioning that AI systems that measure an employee's truthfulness through voice, "micro-expression," or other behavioral analysis, may be prohibited by the Act. These "lie-detector" tests are only permitted under certain exceptions, such as in the security and pharmaceutical industries, or for workers reasonably suspected of involvement in workplace theft and embezzlement.

The FAB wraps with a blanket warning to employers attempting to use AI or other automated systems as a defense to retaliation under the FLSA: blaming the algorithm will not avoid liability. Therefore, employers are urged to take a measured approach to AI-based employee monitoring and to always include a human in the loop to double-check the system's homework.



**Kevin J. White**  
Partner, Washington, DC and Houston



**Daniel J. Butler**  
Associate, Miami



**Subscribe to receive current analysis and developments directly to your inbox.**

**[HUNTONLABORBLOG.COM](https://www.huntonlaborblog.com)**

---

## INSURANCE

# Should Artificial Intelligence Supply Plain Meaning? The Eleventh Circuit Wants to Know

Insurance coverage lawsuits often hinge on the plain and ordinary meaning of specific words or phrases. But not every word in an insurance policy can be defined. Yet without stable and predictable definitions, neither policyholders nor insurers can establish a clear and consistent scope of coverage. In a recent concurring opinion, Eleventh Circuit Judge Kevin Newsom suggests that artificial intelligence (AI) large language models (LLMs) could help resolve these definitional debates. His opinion in *Snell v. United Specialty Insurance Company*, No. 22-12581, 2024 WL 2717700 (11th Cir. May 28, 2024) highlights the pros and cons of calling upon technology to supply plain meaning.

This approach may even offer promise for a fundamental issue plaguing the insurability of AI risk, which we [previously discussed](#), on how to define AI to ensure a functional and predictable scope of coverage.

### LLMs as a Tool in the Interpretive Toolkit

In *Snell*, an insured sought coverage under a Commercial General Liability policy in connection with a lawsuit brought after a child sustained injuries while using an in-ground trampoline. The insurer denied coverage and refused to defend the lawsuit. The lawsuit alleged that Snell, a landscaper, negligently installed the trampoline in a client's backyard. The district court found that coverage would turn on whether installation of the trampoline amounted to "landscaping," as that term was used in the policy. But the policy did not supply a definition for the term "landscaping." The court, therefore, turned to the "common, everyday meaning" of the term, which the district court found to not include trampoline installation.

The Eleventh Circuit ultimately affirmed the district court's decision based on Alabama-law specific grounds unrelated to the meaning of "landscaping." Yet, of particular note, in a concurring opinion, Judge Newsom suggested that LLMs like OpenAI's ChatGPT, Google's Gemini and Anthropic's Claude could help discern the ordinary meaning of undefined words in legal instruments, including insurance policies.

Judge Newsom identified several benefits to using LLMs for this purpose. LLMs train on vast amounts of ordinary-language data—much more than might be available through a dictionary—making them particularly adept at determining common usage. They understand context, which helps detect nuanced language patterns. LLMs are also increasingly accessible, making their use an inexpensive research tool for judges, lawyers and ordinary citizens. In addition, using LLMs to facilitate ordinary meaning interpretation enhances the transparency of the interpreting process because queries and outputs from LLMs can be fully disclosed to the public.

Judge Newsom also pointed out potential drawbacks. LLMs can "hallucinate" and generate incorrect information at times. They might not fully capture offline speech, potentially missing how underrepresented groups use language. There is also the risk that lawyers, judges or litigants may try to manipulate LLMs to favor their preferred interpretation. Moreover, over-reliance on LLMs could lead to dystopian "robo judges."

Despite these concerns, Judge Newsom suggests that AI could be another tool in the judiciary's toolbox, alongside dictionaries and semantic canons.



## Can LLMs Define AI?

As [discussed previously](#), we have identified the general inability to clearly and uniformly define “AI” for purposes of insuring AI risks. Following Judge Newsom’s suggestion, we asked ChatGPT to provide a stable and predictable definition of AI for use in insurance policies to answer the question posed in our last article. That is, how should insurance policies define AI to ensure a functional scope of coverage? Here’s ChatGPT’s response:

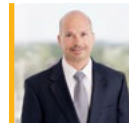
Artificial Intelligence (AI) refers to the capability of a machine to perform tasks that typically require human intelligence, such as learning, reasoning, problem-solving, perception, and natural language understanding. AI systems include technologies like machine learning algorithms, neural networks, and natural language processing, which enable these machines to analyze data, recognize patterns, and make decisions or predictions based on that analysis.

ChatGPT even explained why its definition is a good one. It explained that this definition is comprehensive, covering all AI capabilities and ensuring all current and foreseeable technologies are included. It is clear and specific, identifying key components of AI systems, and technologically neutral, making it adaptable to future advancements. By focusing on AI’s functional aspects, it aligns with practical

insurance concerns. This definition provides a clear framework, reducing disputes and aligning with existing legal frameworks, making it easier to use in legal contexts. It also minimizes differing interpretations, leading to more straightforward claims processes and fewer litigation risks. Whether this AI-generated definition or some iteration might provide a functional definition for purposes of insurance remains to be seen.

## Conclusion

As policyholders and insurers work to resolve the age-old task of supplying meaning to undefined terms, or defining new risks like those posed by AI, they might find it useful to follow Judge Newsom’s recommendation and use AI among the other tools in their toolkits to resolve definitional debates. For now, however, while landscapers and acrobats can rest assured knowing that trampolines are not landscaping (at least in the Eleventh Circuit), the more vexing insurance-related AI issue remains: what *is* AI?



**Michael S. Levine**

Partner, Washington, DC and New York



**Alex D. Pappas**

Associate, Washington, DC

# Hunton Insurance Recovery Blog

UPDATES, ANALYSIS AND BREAKING NEWS FOR COMMERCIAL POLICYHOLDERS

Subscribe to have updates and analysis delivered directly to your inbox.

[HUNTONINSURANCERECOVERYBLOG.COM](https://HUNTONINSURANCERECOVERYBLOG.COM)





---

## PRIVACY AND CYBERSECURITY

# Emergence of AI Laws in the United States: A Closer Look at Colorado's AI Act

On May 17, 2024, Colorado became the first US state to pass legislation that imposes comprehensive and generally applicable legal obligations on “developers” and “deployers” of AI systems. Specifically, the Colorado AI Act (the Act) requires developers and deployers of “high-risk AI systems” to adopt a series of measures to protect Colorado residents from algorithmic discrimination arising from the use of such AI systems. The Act will become fully effective on February 1, 2026, and will be enforced exclusively by the Colorado Attorney General.

### Scope of the Colorado AI Act

As with the EU AI Act, Colorado's AI Act takes a risk-based approach to regulating AI. At a high level, the Act requires developers and deployers of AI systems doing business in Colorado to use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination arising from the use of high-risk AI systems.

The Act uses the following key terms:

- An “AI system” is any machine-based system that, for any explicit or implicit objective, infers from the inputs the system receives how to generate outputs, including content, decisions, predictions, or recommendations, that can influence physical or virtual environments.
- A “high-risk AI system” is an AI system that “makes, or is a substantial factor in making, a consequential decision” when deployed, subject to certain enumerated exceptions (e.g., systems that perform narrow procedural tasks).
- A “consequential decision” is one that has a “material legal or similarly significant effect” on the provision or denial to any consumer of, or the cost or terms of, (1) education enrollment or an education opportunity; (2) employment or an employment opportunity; (3) a financial or lending service; (4) an essential government service; (5) healthcare services; (6) housing; (7) insurance; or (8) a legal service.
- “Algorithmic discrimination” is any condition in which the use of an AI system results in an unlawful differential treatment or impact that disfavors an individual or group of individuals on the basis of a classification protected under Colorado or federal law (e.g., race, gender, age).
- A “developer” is a person doing business in Colorado that develops or intentionally and substantially modifies an AI system.
- A “deployer” is a person doing business in the state that deploys (i.e., uses) a high-risk AI system.



Though the Act is the first of its kind in the US, it shares some similarities with rules regulating automated decision-making under US state privacy laws, particularly with its focus on decisions that produce material legal or similarly significant effects.

Under the Act, both developers and deployers are subject to various transparency, disclosure, and reporting requirements. The law also provides both developers and deployers with an affirmative defense if they can demonstrate steps taken to address any discovered violations of the Act and can otherwise demonstrate compliance with a recognized risk management framework for AI, such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework.

When determining the Act's applicability, companies should consider the list of exemptions under Section 6-1-1705 of the Act. For example, the Act exempts companies that employ fewer than 50 full-time employees from certain deployer responsibilities, subject to various conditions. The law also includes exemptions for certain organizations, including (1) HIPAA-covered entities that use AI systems to generate recommendations that are not considered to be high risk and require a health-care provider to take action to implement; (2) insurers (or developers of AI systems used by insurers) that are subject to Section 10-3-1104.9 of the Colorado Code and implementing rules adopted by the Colorado Commissioner of Insurance; and (3) banks or credit unions (or affiliates thereof) subject to examination by a regulator under any published guidance or regulations that impose substantially equivalent requirements to the Act.



## Developer Obligations

Developers of high-risk AI systems are subject to an obligation to “make available” certain documentation to deployers or other developers regarding a high-risk AI system, including:

- A statement describing the reasonably foreseeable uses and known harmful or inappropriate uses of the high-risk AI system;
- Documentation disclosing (1) high-level summaries of the data used to train the system; (2) known or reasonably foreseeable limitations of the system, including risks of algorithmic discrimination; (3) the purpose of the system; (4) intended benefits and uses of the system; and (5) all other information necessary to allow the deployer to comply with its legal obligations under the Act; and
- Documentation describing (1) how the high-risk AI system was evaluated for mitigation of algorithmic discrimination; (2) data governance measures used on the training datasets including measures to “examine the suitability of data sources, possible biases, and appropriate mitigation”; (3) intended outputs of the system; (4) measures taken to mitigate algorithmic discrimination; (5) instructions on how the system should be used and monitored when used for consequential decision-making; and (6) any additional documentation necessary to help understand system output and monitor its performance for algorithmic discrimination.

In addition, a developer is also obligated to publish certain information, such as the types of high-risk AI systems the developer has developed or intentionally and substantially modified and makes available and how the developer manages known or reasonably foreseeable risks of algorithmic discrimination.

Furthermore, developers of high-risk AI systems must report to the Colorado Attorney General and all known deployers or other developers any known or reasonably foreseeable risks of algorithmic discrimination arising from the intended uses of the high-risk AI system within 90 days of discovery.

## Deployer Obligations

The Act sets forth various obligations for deployers of high-risk AI systems, including the requirement to implement a risk management policy and program governing the deployment of such systems. The risk management policy must specify and incorporate the principles, processes and personnel that the deployer uses to identify, document and mitigate known or reasonably foreseeable risks of algorithmic discrimination.

The Act also requires deployers to conduct an annual impact assessment of high-risk AI systems. In the event that a substantial modification to the system is made, an impact assessment must be completed within 90 days. The impact assessment must include:

- A statement disclosing the system’s purpose, intended use cases, deployment context and benefits;
- An analysis of whether deployment of the system poses risks of algorithmic discrimination, the nature of such risks, and mitigation steps;
- A description of data categories the system processes as inputs and produces as outputs;
- An overview of the data categories used to customize the system (if the system was customized by the deployer);
- Any metrics used to evaluate performance and limitations of the system;
- A description of transparency measures including consumer disclosures regarding AI system use; and
- A description of post-deployment system monitoring and user safeguards, including the oversight, use, and learning process established by the deployer to address any issues.

In addition, deployers using a high-risk AI system for consequential decision-making impacting a consumer

must (1) notify that consumer; (2) provide the consumer with a statement disclosing the purpose of the system, the nature of the consequential decision, the deployer’s contact information, a plain language description of the AI system, and instructions on how to access a required disclosure statement on the deployer’s website; and (3) provide information on the consumer’s right, under the Colorado Privacy Act, to opt out of the processing of their personal data for purposes of profiling in furtherance of decisions that produce legal or similarly significant effects. With respect to the required website disclosure, the deployer must make available a statement on its website that summarizes (1) the type of high-risk AI systems that are currently deployed by the deployer; (2) how the deployer manages known or reasonably foreseeable risks of algorithmic discrimination that may arise from the deployment of each high-risk AI system described in the statement and (3) the nature, source and extent of the information collected and used by the deployer. The statement must be periodically updated by the deployer.

#### Enforcement

The Act does not provide for a private right of action. The Colorado Attorney General has exclusive enforcement authority and may seek up to \$20,000 per violation of the Act. The Colorado Attorney General is also authorized to promulgate rules under the law on certain topics, including the content and requirements of the risk management policy and program that must be implemented by deployers.



**Michael La Marca**  
Partner, New York



**Samuel Grogan**  
Associate, New York



**Liliana Fiorenti**  
Associate, New York

## Privacy & Information Security Law Blog

GLOBAL PRIVACY AND CYBERSECURITY LAW UPDATES AND ANALYSIS

**Subscribe to have updates and analysis delivered directly to your inbox.**

[HUNTONPRIVACYBLOG.COM](https://www.huntonprivacyblog.com)



# AI Regulation in the EU: Obligations Applicable to High-Risk AI Systems

After a long wait, on July 12, 2024, Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonized rules on artificial intelligence (the AI Act) was finally published in the Official Journal of the EU.

As a reminder, the AI Act introduces a risk-based legal framework that establishes different requirements depending on the level and type of risks related to the use of the concerned AI system. The AI Act establishes the following types of AI systems: (1) prohibited AI systems, (2) high-risk AI systems, (3) systems with transparency requirements, and (4) general-purpose AI models. The different types of AI systems listed below are not mutually exclusive. For example, a high-risk system may also be subject to transparency requirements.

In this edition, we delve in more detail on the obligations applicable to providers and deployers of high-risk systems.



## High-Risk Systems

High-risk AI systems are deemed to present a potentially high risk to the rights and freedoms of individuals and thus subject to particularly stringent obligations under the AI Act. The AI Act differentiates between two buckets of high-risk AI systems:

1. An AI system will be considered high-risk when:
  - (i) it is intended to be used as a safety component of a product, or the AI system is itself a product covered by the EU harmonization legislation identified in Annex I of the AI Act and (ii) the product or system has to undergo a third-party conformity assessment under applicable EU harmonization legislation. This may cover AI systems used in, for example, machinery, toys, lifts, equipment and safety components for use in medical devices and in vitro diagnostic medical devices, civil aviation related products and various types of vehicles.
2. Annex III of the AI Act lists AI systems that are expressly stated to be high-risk in the AI Act itself, unless such systems do not pose a significant risk of harm to the health, safety or fundamental rights of natural persons. High-risk AI systems identified in Annex III are divided into eight categories, examples of which include:
  - **Biometrics**, including remote biometric identification systems and emotion recognition AI systems.
  - **Critical infrastructure**, including AI systems intended to be used as safety components in the management and operation of critical digital infrastructure, road traffic or in the supply of water, gas, heating or electricity.
  - **Education and vocational training**, including AI systems intended to be used to determine the access, admission or assignment to educational and vocational training institutions at all levels.
  - **Employment, workers management and access to self-employment**, including AI systems intended to be used to recruit or select individuals, in particular to place targeted job advertisements, to analyze and filter job applications and to evaluate candidates.
  - **Access to and enjoyment of essential private services and essential public services and benefits**, including AI systems intended to be used to evaluate the creditworthiness of individuals or establish their credit score (except for AI systems used to detect financial fraud and risk assessment), or to be used for pricing in relation to individuals in the case of life and health insurance.



## Obligations of Providers of High-Risk AI Systems

In addition to the type of system, the AI Act allocates obligations based on the organization's role in the development or deployment of an AI system (e.g., providers or deployers). Providers of high-risk AI systems are subject to the majority of and to the strictest requirements under the new law, including:

- establishing, implementing, documenting and maintaining a risk management system and quality management system;
- data governance requirements, including bias mitigation;
- drafting and maintaining technical documentation with respect to the high-risk AI system;
- record-keeping, logging and traceability obligations;
- designing the AI system in a manner that allows effective human oversight;
- designing the AI system in a manner that ensures an appropriate level of accuracy, robustness and cybersecurity;
- complying with registration obligations;
- ensuring that the AI system undergoes the relevant conformity assessment procedure;
- making the provider's contact information available on the AI system, packaging or accompanying documentation;
- drawing up the EU declaration of conformity in a timely manner; and
- affixing the "CE marking" to the AI system.

## Obligations of Deployers of High-Risk AI Systems

Deployers of high-risk AI systems also will have a significant number of direct obligations under the AI Act, although these are more limited in scope than the providers' obligations. The deployers' obligations include:

- assigning human oversight of the AI system to a person with the necessary competence, training, authority and support;
- if the deployer controls input data, ensuring that the data is relevant and sufficiently representative in light of the purpose of the AI system;
- informing impacted individuals when the deployer plans to use a high-risk AI system to make decisions or assist in making decisions relating to such individuals;
- if the deployer is an employer and the AI system will impact workers, informing workers representatives and the impacted workers that they will be subject to a high-risk AI system;

- conducting a fundamental rights impact assessment for certain deployers and high-risk systems, namely deployers using AI systems to evaluate the creditworthiness of individuals or establish their credit score, and for risk assessment and pricing in relation to individuals in the case of life and health insurance; and
- when a decision generated by the AI system results in legal effects or similarly significantly affects an individual, providing a clear and meaningful explanation of the role of the AI system in the deployer's decision-making procedure and the main elements of the decision.

## When Will the AI Act Apply?

The AI Act entered into force on August 1, 2024, and will become applicable following a transition period. The length of the transition period will vary depending on the type of AI system:

- obligations applicable to **prohibited AI systems** and the obligations related to AI literacy will become applicable on February 2, 2025;
- specific obligations applicable to **general-purpose AI models** will become applicable on August 2, 2025;
- most obligations under the AI Act, including the rules applicable to **high-risk AI systems under Annex III** of the AI Act and **systems subject to specific transparency requirements** will become applicable on August 2, 2026; and
- obligations related to **high-risk systems included in Annex I** of the AI Act will become applicable on August 2, 2027.

Both providers and deployers of high-risk AI systems should start putting in place their respective AI compliance programs as soon as possible in order to have adequate time to evaluate the necessary measures, plan their implementation and ensure compliant deployment.



**Sarah Pearce**  
Partner, London



**Tiago Sérgio Cabral**  
Associate, Brussels

---

## LITIGATION

# Recent N.D. Ill. Ruling Upholds Common Interest Doctrine Over Communications Between Biometric Technology Vendors and Customers

In a welcome win for defendants litigating claims under the Illinois Biometric Information Privacy Act (BIPA), earlier this month a Northern District of Illinois magistrate judge denied a plaintiff's motion to compel communications between defendant Union Pacific Railroad Company (Union Pacific) and the vendors that provided it with fingerprint-activated security gates. *Fleury v. Union Pac. R.R. Co.*, No. 20 C 390, 2024 WL 1620613, at \*4-6 (N.D. Ill. Apr. 15, 2024). In so doing, the court implicitly affirmed that, in a BIPA lawsuit, the common interest doctrine presumptively protects the communications between biometric technology vendors and their customers, regardless of which entities are named as defendants. This ruling is a powerful tool in the BIPA landscape for employers (who are typically the customers in this scenario) and other defendants alike because it supports the ability of BIPA defendants to coordinate their defense strategy with entities who share their legal interest. The opinion is also a good reminder, however, that vendors and their customers should use best practices early on in a BIPA litigation to maximize the scope of the common interest doctrine.

Union Pacific operates a network of railroads in North America that includes facilities located in Illinois. The plaintiff, who worked as a truck driver in 2019, alleged that Union Pacific violated BIPA by requiring him and class members to scan their fingerprints at an entry gate kiosk each time they entered the railyard without their consent, among other claims.

BIPA lawsuits are typically aimed at third-party vendors who operate the technology that captures biometric information, the customers of these vendors, or both. Many plaintiffs are going after their former employers, for example, for using biometric technology in the workplace provided by various vendors (e.g., fingerprint timekeeping clocks). Thus, such lawsuits often benefit from coordination between these various players, regardless of whether they are named defendants in the lawsuit.

Judge Cole's April 15 decision affirms the importance of the common privilege doctrine in protecting communications among BIPA lawsuit targets. The plaintiffs sought to compel production of correspondence between counsel for Union Pacific and counsel for the vendors that licensed and sold the finger scan technology and hardware to Union Pacific. Union Pacific refused, claiming that the communications were protected by the "common interest privilege."

Judge Cole agreed that "the defendant has some common legal interests with its software and hardware providers in a BIPA case." *Fleury*, No. 20 C 390, 2024 WL 1620613, at \*4-6. He reminded the parties that the common privilege interest was an extension of the attorney-client privilege and applied when entities shared an "identical" interest in the suit, though the interest "need not be compatible in all respects." *Id.* While a written joint defense agreement is "one factor to consider," it is not dispositive.

Given that the vendors' technology prompted key issues in the case regarding the alleged collection, capture and disclosure of biometric information, "one can say that the defendant and [the vendors] have some common legal interests." However, similar to the assertion of other privileges, the protection extends only to communications that further this common interest. Judge Cole concluded his decision by ordering Union Pacific to produce a privilege log of the purportedly protected communications.

Judge Cole's implication that communications between biometric technology vendors and their customers are presumptively protected under the common privilege doctrine is a welcome development for defendants. However, the decision is also a reminder for defendants to follow best practices when forming alliances with interested parties. These practices include entering into clear joint defense agreements and limiting written communications to those that truly reflect a common legal interest.



**Torsten M. Kracht**

Partner, Washington, DC  
and New York

## BANKING AND FINANCE

# AI and Emerging Technologies in Financial Services

Federal and state banking regulators view artificial intelligence (AI) and emerging technologies in much the same way that they have traditionally viewed all technological developments in the financial services space—the *activity itself* is regulated, despite what technological channel it occurs in and despite features of that underlying technology. That being said, financial institutions need to pay close attention to AI in three key areas of financial institution and banking activities:

1. Activities Involving AI (and corresponding regulations and regulator expectations) in customer-facing delivery of financial services.
2. Incorporation of AI features by third-party vendors in platforms and technology that financial institutions use to conduct banking operations or delivery of customer financial services (for both consumer and commercial customers).
3. Use of AI by financial institution employees in day-to-day business operations that do not touch on delivery of financial services, banking activities or customer personal information.

### Activities Involving AI in Customer-Facing Delivery of Financial Services

On August 12, 2024, the Consumer Financial Protection Bureau (CFPB) provided comments on the use of AI in the financial services sector that are among the most comprehensive from the CFPB regarding risks and expectations for the use of AI in consumer financial services, and the CFPB's approach to regulating AI.

The CFPB's comments were issued in response to a separate US Treasury Department request for information (RFI) issued June 6, 2024. The US Treasury Department's "Request for Information on Uses, Opportunities, and Risks of Artificial Intelligence in the Financial Services Sector" stated that it was seeking to increase its understanding of AI use in the financial services sector, including:

- "Potential obstacles for facilitating responsible use of AI within financial institutions."
- "The extent of impact on consumers, investors, financial institutions, businesses, regulators, end-users, and any other entity impacted by financial institutions' use of AI."
- "Recommendations for enhancements to legislative, regulatory, and supervisory frameworks applicable to AI in financial services."

The RFI includes 19 separate questions that address a wide range of topics around AI in financial services, such as:

- how to define AI;
- uses and benefits of AI;
- challenges that AI presents (including the demand for consumer data and related data privacy considerations);
- fair lending and other consumer compliance issues;
- issues that small financial institutions face regarding AI;
- AI risk management;
- third-party oversight;
- fraud and illicit finance risks; and
- recommendations for actions that the US Treasury Department can take to promote the responsible use of AI and protect consumers and financial institutions.

A key focus of the RFI is balancing the potential for AI to promote inclusiveness and the risk that AI may exacerbate bias and fair lending. While some of the issues the US Treasury Department is seeking information on may be new and unique to AI, others are not. For example, the FDIC, Federal Reserve Board and OCC all have supervisory guidance on model risk management and model validations, and these have been around for many years.



The CFPB's statement on comments emphasizes that existing laws apply fully to uses of AI in financial services, and it will continue to assess AI uses for compliance with those laws, including fair lending laws. Specific AI uses that the CFPB identifies as presenting potential compliance risk include automated customer service processes such as chatbots, fraud detection models and loan origination.

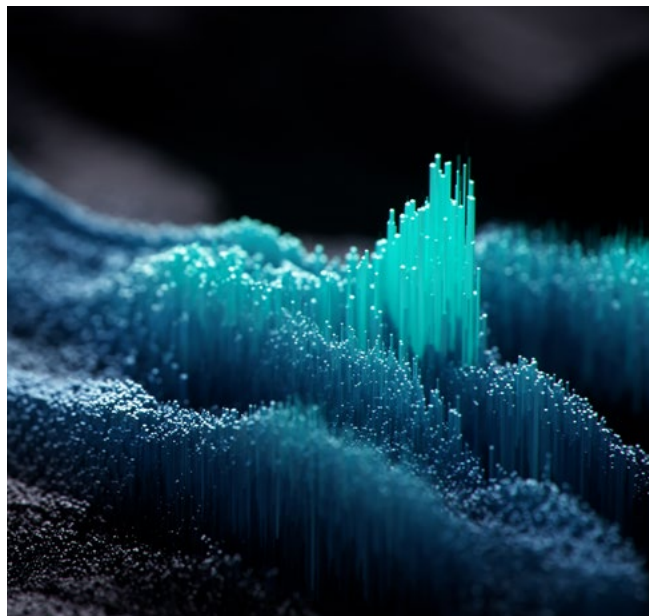
The CFPB's comments on the US Treasury Department's RFI (the "CFPB Comment") emphasize two central points:

1. A number of existing laws already apply to the use of AI by financial institutions.
2. Regulation of the financial services sector, including regulation of AI, should foster competition by creating a level playing field, rather than giving special treatment to particular institutions.

The CFPB Comment notes that there are no exceptions to the federal consumer financial protection laws for new technologies. Regulators are required to apply existing rules to such new technologies (which includes AI). In that regard, the CFPB Comment lists a number of CFPB publications and guidance documents regarding consumer protection issues that may be implicated by the use of AI, including:

- Chatbots and other automated customer service technologies built on large language models may: (i) provide inaccurate information and increase risk of unfair, deceptive and abusive acts and practices in violation of the Consumer Financial Protection Act (CFPA); (ii) fail to recognize when consumers invoke statutory rights under the Electronic Funds Transaction Act/Regulation E and the Truth In Lending Act/Regulation Z; and (iii) raise privacy and security risks, resulting in increased compliance risk for financial institutions.
- A central focus of the CFPB's Comment is the prohibition against discrimination and the requirement to provide consumers with information regarding adverse action taken against them, as is already required pursuant to the Equal Credit Opportunity Act (ECOA). The CFPB Comment notes that courts have already held that a financial institution's decision to use algorithmic, machine-learning or other types of automated decision-making tools can itself be a policy that produces bias under the disparate impact theory of liability.

The CFPB states in the Comment that it will continue to closely monitor financial institutions' fair lending testing protocols, including those relating to "complex models." Such testing should include regular testing for "disparate treatment and disparate impact," and consideration of less discriminatory alternatives using manual or automated techniques.



The CFPB Comment also emphasizes that the use of BSA/AML, OFAC and fraud screening tools, such as those offered by third-party vendors that provide fraud risk services, must be offered in compliance with ECOA and the CFPB. In addition, the CFPB Comment states that because such screening is often used to assess creditworthiness (i.e., by determining who gets "offered or approved for a financial product"), institutions that compile and provide such information are likely "subject to the requirements of the Fair Credit Reporting Act."

The second key point of the CFPB Comment is that uniform enforcement of rules by regulators serves to foster innovation since regulated entities are incentivized to invest in innovative products and services that benefit consumers/customers rather than circumvent the rules. With respect to AI, this means ensuring that regulation does not stifle competition in pricing or in favor of incumbents, that there is consistent treatment under the law for similar products and services, and that regulators combat anticompetitive practices and monitor the market to ensure accountability.

Since the CFPB and other federal financial regulators have not issued or proposed comprehensive regulations addressing AI specifically, publications such as the CFPB Comment provide key insights into the CFPB's priorities (and likely the priorities of other federal financial regulators) and potential future supervisory, enforcement and actions regarding AI. The CFPB has not yet proposed any new rules or guidance governing AI, which is a strong indication that the CFPB intends to rely on existing laws and regulations to regulate AI. Accordingly, financial institutions need to assess their contemplated and actual use of AI for compliance with current laws and regulations, especially with respect to the specific laws cited in the CFPB Comment discussed above.



In addition to federal financial services regulatory authorities, states and state regulators are also starting to pass legislation and take action with regard to AI. For example, the ways in which AI can be used to discriminate against individuals is a focus of the recently enacted Colorado Artificial Intelligence Act. That act, which goes into effect in February 2026, is primarily focused on AI systems used to make a “consequential decision” involving areas such as financial services. It is designed to protect against algorithmic discrimination—namely unlawful differential treatment that disfavors an individual or group on the basis of protected characteristics.

### **Incorporation of AI by Third-Party Vendors and Service Providers in Platforms and Technology Used by Financial Institutions**

As part of a financial institution’s standard due diligence, contract negotiation and monitoring/oversight of third-party vendors and service providers, financial institutions need to revise/expand their RFP questions, processes and procedures to take into account AI technology, whether directly provided by a third-party vendor or otherwise embedded in the third-party vendor’s products and services (even if provided by a “4th party” service provider to the third-party vendor).

If the financial institution is negotiating with a third-party vendor who itself has developed and will provide AI technology and services, the financial institution will want to make sure that it is obtaining an “enterprise” or “proprietary” license such that the financial institution’s proprietary information and/or customer information (including the personally identifiable information of consumer customers) are not ingested to a large language learning model that is available to other companies or individuals. And promises by third-party vendors to only ingest anonymized/de-identified data into large language learning models available to other companies and individuals may not address all of the financial institution’s business and regulatory concerns, so this will be a heavily negotiated issue in third-party vendor contracts.

Even if the financial institution is not thinking that it is specifically contracting with a third-party vendor for AI services, financial institutions should be aware that many third-party vendors to financial institutions put together their entire suite of products and services using “4th party” vendors and service providers in the background. For example, a financial institution may be using a core processor for a variety of services, including those that are customer-facing, and that core processor may in turn be using a “4th party” vendor in the background for BSA/AML and OFAC screening who uses AI in identify verification or name recognition activities. The financial institution will (a) want to

know that and (b) understand how the financial institution can meet its regulatory obligations with regard to that “4th party” vendor, including monitoring, oversight and testing.

### **Use of AI by Financial Institution Employees in Day-to-Day Business Operations**

Finally, a last consideration for financial institutions is whether the entity should adopt clear internal policies and procedures regarding “allowed” and “prohibited” use of AI technology by employees for day-to-day tasks. For examples, some financial institutions have enacted a policy that prohibits the use of AI in delivery of financial services unless provided by a financial institution-approved AI vendor under contract with the financial institution. However, such policies may allow, for example, employees to use AI for composing internal emails, note taking and summarization for meetings, etc., so long as (1) the employee either uses financial institution-approved vendors or seeks permission for the type of AI technology they want to use, (2) the AI technology will not be used for any regulated financial services activity (e.g., credit underwriting, loan decisioning, etc.), and (3) the AI will not ingest customer/consumer financial or personally identifiable information. The same considerations stated above regarding enterprise/proprietary large language model and licensing issues apply for any AI technology utilized by financial institution employees.

### **Conclusion**

Technology in the AI space is moving quickly, so financial institutions must stay abreast of new and changing laws, regulations and regulatory interpretations and guidance regarding use and deployment of AI in financial services. Financial institutions should contemplate the entity’s proposed use and adoption of AI in board-approved policies and procedures, as well as working AI-specific issues and topics into third-party service provider due diligence, contract negotiation and ongoing monitoring of deployment and performance of AI by the financial institution, the financial institution’s third-party vendors and service providers (as well as “4th party” vendors to those third-party service providers).



**Erin F. Fonté**  
Partner, Austin



**Betsy Lee Montague**  
Associate, Dallas

