HUDSON COOK

Colorado Special Session Update: AI Law Delayed to June 2026, What the Rental Housing and Financial Services Industries Can Do Next

September 10, 2025 | Jay Harris, Webb McArthur and Mark D. Metrey

On August 28, 2025, Governor Jared Polis signed the AI Sunshine Act (Senate Bill 25B 004) into law, moving the effective date of the Colorado Artificial Intelligence Act (CAIA; Col. Rev. Stat. § 6-1-1701) to June 30, 2026. Colorado lawmakers are expected to revisit elements of the framework during the General Assembly's next regular session that begins in January 2026, meaning provisions of the law may change again in the Spring. Still, preparing now is prudent given the time needed to inventory systems, align documentation, and implement disclosure processes.

The delay does not alter the core framework enacted in 2024. Unless amended further in the regular legislative session in the Spring, the law will impose duties on both developers and deployers of high-risk AI systems as of the new date. These duties include creating developer documentation and public statements, deployer risk management programs and impact assessments, consumer disclosures when AI contributes to consequential decisions, and AI interaction disclosures for systems intended to engage directly with consumers. The Attorney General retains exclusive enforcement authority, and violations of the CAIA remain actionable as deceptive trade practices under the Colorado Consumer Protection Act.

What counts as "high risk" and who is covered - § 6-1-1701

The CAIA defines a "high-risk artificial intelligence system" as one that "makes, or is a substantial factor in making, a consequential decision" about a consumer. A "consequential decision" includes those that have a "material legal or similarly significant effect" on the provision, denial, cost, or terms of a financial or lending service, housing, insurance, health care, education, employment, legal services, or essential government services. Below we discuss several specific applications of this broad scope of coverage.

For transactional deployer disclosures, the statute requires notifying the consumer that a high-risk AI system is in use, providing "a description, in plain language," and, if the outcome is adverse, disclosing the principal reasons, "the degree to which, and manner in which, the high-risk artificial intelligence system contributed," the "type of data," and the "source or sources of the data," plus opportunities to correct and to appeal, with human review when feasible.

The CAIA distinguishes developers from deployers. A developer is a business that "develops or intentionally and substantially modifies" an AI system, defined as a "deliberate change . . . that results in any new reasonably foreseeable risk of algorithmic discrimination." A deployer is a business that uses a high-risk system. It is possible to be both for the same tool.

Practical obligations that apply on June 30

Developers, summary of duties - § 6-1-1702

Developers must exercise reasonable care to protect consumers from known or reasonably foreseeable risks of algorithmic discrimination arising from intended and contracted uses. To support their deployer clients, developers must provide deployers with documentation such as model cards and dataset cards that explain intended uses, training data at a high level, known limitations, mitigation steps, and how the system should and should not be used and monitored when it affects consequential decisions. In addition, developers must maintain a public statement or use case inventory describing the types of high-risk systems they make available and how they manage algorithmic discrimination risks. Developers must notify the Attorney General and known deployers of discovered risks within ninety days and must respond to Attorney General requests for documentation within ninety days. Developers submitting documentation to the Attorney General may designate proprietary information as confidential, which prevents disclosure under the Colorado Open Records Act.

Deployers, summary of duties - § 6-1-1703

Deployers must implement and maintain a risk management policy and program that is iterative and aligned to a recognized framework such as the National Institute of Standards and Technology (NIST) AI Risk Management Framework or the International Organization for Standardization (ISO) 42001. Deployers must also complete impact assessments before deployment, updated at least annually and within ninety days of intentional and substantial modifications. Furthermore, deployers must maintain assessment records, review each high-risk system annually to ensure it is not causing algorithmic discrimination, and be able to furnish the risk program or assessments to the Attorney General upon request. In following these obligations, deployers benefit from a rebuttable presumption of reasonable care should challenges arise from the Attorney General.

Consumer disclosures for consequential decisions - § 6-1-1703(4)

Before using a high-risk AI system to make, or to be a substantial factor in making, a consequential decision, the deployer must notify the consumer that a high-risk AI system is in use, provide a plain language description of the system and the nature of the decision, give the deployer's contact information, and explain how to access required statements. If the consequential decision is adverse, the deployer must provide the principal reasons, the degree and manner the AI contributed, the types of data processed and the data sources, an opportunity to correct personal data used, and an opportunity to appeal that allows for human review when feasible. The deployer must also

provide information to consumers about the right to opt out of profiling under the Colorado Privacy Act where applicable.

These pre- and post- decision consumer disclosure obligations for AI users parallel, and in some respects overlap with, long-standing federal requirements. For example, the Fair Credit Reporting Act (FCRA) requires adverse-action notices that identify the principal reasons for a denial when a consumer report is used, and the Equal Credit Opportunity Act requires creditors to state reasons for adverse credit decisions. Similarly, the Fair Debt Collection Practices Act regulates disclosures in collection activity. The CAIA appears to occupy some of the same disclosure space by requiring explanations of how AI factored into consequential decisions. Deployers will need to work carefully through these overlapping disclosure obligations and resolve potential tension between federal preemption of state laws, particularly the FCRA's targeted preemption provisions, and CAIA requirements that appear to cover the same ground.

AI interaction disclosure - § 6-1-1704

If a developer or deployer offers or makes available an AI system that is intended to interact with consumers, the consumer must be told that they are interacting with an AI system. However, a disclosure is not required where it would be obvious to a reasonable person that the interaction is with AI.

Exemptions - § 6-1-1703(6); 1705(5)

Deployers with fewer than 50 employees that do not train their own models and use high-risk systems only as intended, while providing the developer's impact assessment to consumers, are exempt from certain obligations. Exemptions also apply when an AI system has been approved by a federal agency, or when entities are already regulated under frameworks such as HIPAA for health information.

Which Financial Services and Rental Housing Activities May be Covered?

Because the definition of a high-risk AI system hinges on whether the AI system makes, or is a substantial factor in making, a consequential decision, coverage turns on how the tool is used in practice. The following lines of business may be covered when an AI tool, such as a score, substantially influences eligibility, pricing, terms, or other consequential determinations (e.g., hiring):

Consumer credit and auto finance deployers using covered underwriting score models for eligibility or pricing

Activities covered:
The statute defines "high-risk" AI systems to include those that make, or are a substantial factor in making, consequential decisions about lending services. Underwriting models for approval or credit-line assignment, APR and tier pricing, and ongoing account-management models that change terms or access.

Statutory obligations:
In consumer credit and auto finance, covered entities such as direct and indirect finance

companies, payday lenders, small-dollar lenders, consumer insurance providers, and debt collectors may be considered deployers when they use AI scoring or pricing models that substantially influence eligibility, cost, or terms. As deployers, they must operate risk management programs, complete and update impact assessments, publish public statements describing their high-risk deployments, and provide consumer disclosures whenever AI contributes to consequential decisions. At the time of a decision, consumers must receive plain-language explanations of the system's role, and in adverse cases, the reasons for the outcome, the degree of AI involvement, the data sources used, and opportunities for correction and appeal with human review when feasible.

Vendor documentation:
Developers in this space, including score modelers and software providers that create or substantially modify scoring tools, may be expected to supply deployers with documentation covering intended uses, training-data summaries, known limitations, and mitigation steps. This documentation, often in the form of model or dataset cards, would enable deployers to complete their required impact assessments and to align deployment with the developer's intended use. Developers must also publish public statements describing the high-risk systems they make available and notify deployers of newly identified risks. Resellers that simply pass through scores without modification may not be considered developers, but if they fine-tune or adapt models for new purposes, they may assume these same obligations.

Mortgage lenders deploying AI for eligibility, pricing, or fraud

Activities covered:
Machine-learning underwriting for approval or pricing, layered risk scores, and tools used as decision inputs in mortgage eligibility and pricing appear to be covered when they "substantially factor" into approval or pricing determinations, even if a human underwriter signs the final decision.

Statutory obligations:
Mortgage lenders as deployers are subject to the same obligations as above. The law also specifies that adverse consequential decision disclosures must describe how AI contributed to the decision, the data types and sources, and provide correction and appeal opportunities.

Rental housing providers deploying AI screening or pricing tools

Activities covered:
Renter screening and fraud detection scores and pricing tools appear to be covered when used by a covered deployer, such as a property manager, as a substantial factor in leasing eligibility or risk pricing decisions, such as setting transactional security deposit amounts. Anti-fraud tools that do not use facial recognition are expressly listed among technologies excluded from high-risk status. Therefore, if a housing provider uses an AI system to analyze a selfie alongside a driver's license photo to verify the identity of a prospective tenant, the system could be considered "high-risk." Although it is deployed as an anti-fraud tool, its reliance on facial recognition technology could bring it within the statute's scope.

Statutory obligations:
Deployers in the housing sector must make a website statement describing the use of high-risk AI systems and related risk management practices, provide consumer disclosures at the decision point, and for adverse eligibility decisions, disclose reasons, the AI's role, data types and sources, and offer correction and appeal opportunities.

Debt collection and recovery

Activities covered:

AI used to set or substantially influence eligibility for payment plans, settlement offers, escalations to litigation, or account treatment that materially affects cost or terms potentially falls within financial or lending services and therefore within consequential decisions. Thus, consumer scores used to determine settlement eligibility may be covered.

Statutory obligations:

Deployers (such as covered creditors and third-party debt collectors) must run a risk management program, conduct and update impact assessments, publish a statement describing their use of AI, and give consumers disclosures when AI influences repayment options or account treatment. Developers must provide documentation, publish statements on their systems, and take reasonable steps to prevent algorithmic discrimination. As stated earlier, the CAIA expressly states that none of its obligations restrict a developer or deployer from complying with other federal, state, or local laws.

Small-dollar lending and specialty finance

Activities covered:

Small-dollar lending refers generally to certain consumer-purpose credit products such as payday loans, installment loans, auto title loans, credit-builder loans, and earned wage access or payroll advance programs when structured as loans. These products fall within the statute when AI substantially factors into eligibility, pricing, renewals, or refinancing.

Statutory obligations:

Deployers using AI for eligibility, pricing, or renewals must maintain risk management programs, update impact assessments, notify regulators of discrimination, and disclose AI use and reasons for adverse decisions. Developers must provide documentation on intended use, risks, and mitigations, and notify deployers and regulators of problems.

Employment

Activities covered:

Hiring, promotion, and termination decisions that rely on AI are expressly defined as consequential decisions under the statute, and screening or risk-scoring systems that substantially factor into those outcomes also likely fall within scope.

Statutory obligations:

Employers using AI in hiring or promotion must manage risks, complete impact assessments, publish statements, and disclose AI's role in decisions, including reasons, data sources, and appeal rights. Developers must provide supporting documentation and publish statements about their systems and safeguards.

Marketing and advertising tools

Activities covered:

Marketing and ad-serving tools are generally not high-risk unless they are used to make, or substantially factor into, consequential decisions. For instance, when an advertising platform applies its own AI models to determine which consumers see credit or lending ads, that targeting decision is likely not a consequential decision under the statute because it does not itself provide or deny credit or alter its terms. In that case, the advertising platform, not the financial institution, would be the deployer. By contrast, if a lender's own AI system determines what terms are presented in an ad based on data unique to the targeted consumer, that use may qualify as a consequential decision .

The statute expressly excludes a wide range of chatbots - i.e., "technology that communicates with consumers in natural language for the purpose of providing users with information, making referrals or recommendations, and answering questions," provided there is an Acceptable Use Policy to prevent discriminatory or harmful content.

Statutory obligations:

If marketing tools cross into eligibility or pricing decisions, deployers may be required to apply the full obligations: risk management, impact assessments, public statements, and consumer disclosures. Developers here must provide documentation and publish system statements. Separately, while excluded from high-risk AI, chatbots or assistants are still required to clearly disclose when consumers are interacting with AI.

Quick readiness checklist for the June 2026 start date

A wide range of covered companies are already at work with outside counsel to determine the CAIA's applicability to their businesses and begin to develop required documentation and updated business workflows. By engaging experienced consumer data counsel now, covered companies can create a clear path to the CAIA compliance with confidence, subject to available confidentiality and attorney-client privilege. A compliance checklist would include several of the following tasks:

- Map high-risk use cases across company activities.
- Adopt an AI risk management program aligned to NIST AI RMF or ISO 42001 and scaled to the company's size and complexity.
- Develop an impact assessment template and complete assessments for each high-risk system before deployment.

- Draft applicable public statements, developer or deployer, and establish an update cadence.
- Create correction and appeal workflows, with human review where feasible.
- Generate and arrange availability to deployer clients for developer artifacts, updates, and cooperation, and specify Attorney General notice duties and timelines.
- Schedule regular anti-bias reviews to test for algorithmic discrimination and record the results in a monitoring program with the involvement of counsel.

Bottom line

The immediate outcome of the special session is a delay of the CAIA's effective date to June 30, 2026. This gives the Colorado General Assembly time during its 2026 session to introduce substantive amendments to the law. Until then, the underlying structure remains. Working with experienced counsel under appropriate confidentiality protections, covered companies should use the additional time to secure developer documentation, tighten deployer risk programs and assessments, and finalize combined disclosure packages for transactional use cases.

HUDSON
COOK

Hudson Cook, LLP is a national law firm representing the financial services industry in compliance, privacy, litigation, regulatory and enforcement matters.

7037 Ridge Road, Suite 300, Hanover, Maryland 21076
410.684.3200

hudsoncook.com