HUDSON COOK

Colorado Artificial Intelligence Act: What Indirect Finance Sources and Dealerships Should Do Now to Prepare

October 31, 2025 | Jay Harris and Mark D. Metrey

Colorado Governor Jared Polis signed a special session bill on August 28 moving the effective date of the Colorado Artificial Intelligence Act to June 30, 2026. Lawmakers are expected to revisit the framework during the 2026 regular session, so details may change again in the spring. Preparing now remains prudent given the time needed to determine the CAIA's application to operations, inventory systems, prepare required documentation for disclosure, bring risk management into compliance, and operationalize consumer notices.

Scope for indirect auto finance

The CAIA covers high-risk artificial intelligence systems that make, or are a substantial factor in making, consequential decisions about consumers and expressly includes financial or lending services. In practical terms, any decision model that is a substantial factor in consumer approval, credit tier, pricing, deposit, or down payment requirements; fraud holds that affect loan cost or access; or collections treatments that materially change terms can be in scope. A system is covered even if a human makes the final call, when the output substantially factors in that outcome. Dealers may also be deployers subject to CAIA obligations if they use a covered tool to pre-screen applicants, route applications, or present financing choices in ways that materially affect terms.

Developer duties in the auto credit stack

Vendors that create or intentionally and substantially modify underwriting, pricing, identity, or collections models may be developers covered by the CAIA. Covered developers must exercise reasonable care to avoid algorithmic discrimination and furnish their client deployers with documentation sufficient to support covered deployers' required impact assessments and ongoing governance.

At a minimum, indirect finance sources deploying or using covered AI tools should expect and request from their AI decision tool developer thorough documentation about the tool, including a clear statement of intended uses and reasonably foreseeable harmful uses, high-level descriptions of the data used for training and tuning, known limitations and risks, performance and fairness evaluation methods, mitigation steps taken, and practical instructions for human oversight and post-deployment monitoring.

Model cards and dataset cards are a sensible way for AI developers to deliver these materials to their deployer clients. Beyond client-facing documentation, developers must also maintain a public statement describing the high-risk systems they make available and their approach to managing algorithmic discrimination. When a developer discovers a likely risk of algorithmic discrimination in one of its high-risk systems, it must notify the Colorado attorney general and known deployers without unreasonable delay and in any event within 90 days.

Deployer duties for indirect finance sources

Any finance source that uses a high-risk system for "consequential decisions," such as consumer finance underwriting, pricing, or collections, may be a deployer. The CAIA defines a consequential decision as one that has a material legal or similarly significant effect on a Colorado consumer, including determinations in financial services, housing, employment, insurance, or similar areas. Deployers are therefore in scope whenever they use an AI system that makes, or is a substantial factor in making, such decisions.

Deployers subject to the CAIA must implement a documented AI risk management program that fits the size and complexity of the business and the systems used. A practical anchor is to map program controls to the NIST AI Risk Management Framework or ISO 42001 so that governance, testing, monitoring, incident response, and vendor oversight are clearly assigned and repeatable.

Deployers must complete an impact assessment before using a high-risk system and update the assessment at least annually or within 90 days of any intentional and substantial model modification. An impact assessment should describe the purpose and business rationale, data inputs and outputs, known limitations, plausible risks of algorithmic discrimination, mitigation measures, transparency steps, human oversight arrangements, and the post-deployment monitoring plan. Impact assessments and related records must be maintained by deployers, who should be prepared to provide them to the AG on request.

The CAIA's jurisdictional coverage is not limited to companies physically located in Colorado. The CAIA applies to any person doing business in Colorado that develops or deploys high-risk AI systems. A consumer is defined as a Colorado resident. Therefore, companies marketing or offering credit to Colorado residents are within scope, even if the company is based elsewhere.

The statute includes a limited exemption for smaller deployers. Businesses with fewer than 50 employees that do not train their own models and that only use systems as intended by the developer are relieved of running their own risk management program, completing impact assessments, and making a public statement. However, they must still provide consumers with the developer's impact assessment and required pre-decision and adverse decision notices.

Public transparency and consumer-facing notices

Deployers, such as finance sources relying on covered AI tools for loan decisioning, must publish a website statement that summarizes their high-risk deployments, how they

manage risks, and the nature, source, and extent of information used for those deployments. For indirect finance sources, that means a clear description of automated underwriting or pricing use cases and a high-level summary of testing and oversight practices in terms that non-specialists can understand.

Before using a high-risk system to make or substantially influence a consequential decision, the deployer must notify the consumer that an AI system is in use and provide a plain-language description of the system and the nature of the decision, contact information, and how to access required statements. If the outcome is adverse, the deployer must provide the principal reasons, explain the degree and manner in which the AI contributed, identify the types of data processed and the data sources, offer a path to correct personal data, and offer an appeal that allows for human review when feasible. Covered deployers should review with knowledgeable counsel whether this adverse consequential decision notice is preempted by applicable law or if it must be given in coordination with existing adverse action notices.

AI interaction disclosures

If a finance source or dealer offers a chatbot or virtual assistant that is intended to interact with consumers, it must disclose that the consumer is interacting with an AI system unless this fact would be obvious to a reasonable person. Identity verification or anti-fraud bots that use facial recognition can bring the deployment within high-risk coverage under the CAIA, even if the purpose is fraud prevention.

Dealership considerations in indirect workflows

Dealerships that only collect applications and transmit them to finance sources are unlikely to be developers. However, a dealer can become a deployer if it uses a pre-screening or decision tool that is a substantial factor in the dealer's decisions about contract eligibility or terms. Dealerships with fewer than 50 employees that do not train models and use systems only as intended may be exempt from certain obligations to create their own risk program and impact assessments, provided they give consumers access to the developer's impact assessment and the required pre-decision and adverse decision disclosures. Larger dealer groups should plan for the full deployer obligations where they use high-risk tools.

Fraud, collections, and account management examples

Fraud models that use facial recognition for identity verification, when used to gate access to credit or impose higher deposits or downpayments, may be viewed as covered high-risk AI tools, with both governance and disclosure duties. Collections models that set settlement or hardship eligibility in ways that materially affect settlement terms also may fit the consequential decision definition. Covered finance sources deploying AI should include these use cases in the system inventory, obtain developer artifacts that speak to known limitations and mitigation steps, and run outcome monitoring and bias tests tied to the specific decision context.

Governance and vendor contracting

Most indirect finance sources already have elements of model risk management and fair lending testing. The CAIA pushes those practices into a required formal, repeatable program with documented assessments and disclosures. Covered finance sources must update vendor diligence and contracts to require developer documentation, ongoing updates to artifacts, prompt notice of discovered risks within the statutory window, cooperation with deployer assessments, and clear statements of intended and prohibited uses. For internal builds or AI decision system tuning that constitutes intentional and substantial modification, covered users should plan to meet both developer and deployer duties.

Action plan for the 2026 effective date

Auto credit executives should work with experienced counsel now to determine if CAIA compliance programs are needed by June 30, 2026. A comprehensive CAIA compliance program for auto credit may include some or all of the following steps:

- mapping high-risk use cases across underwriting, pricing, fraud, and collections;
- standing up a risk management program aligned to the NIST AI Risk Management Framework or ISO 42001;
- building and piloting impact assessment templates with at least one high-value model;
- publishing a plain-language website statement;
- updating vendor contracts to reflect documentation and notice obligations; and
- training credit, compliance, and dealer relations teams on the new process so that pre-decision and adverse decision notices go out reliably in indirect channels.

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