KRIEG DEVAULT

Insights

Colorado SB 26-189 Overhauls Its Landmark AI Law

June 29, 2026

By: David A. Bowen

On May 14, 2026, Colorado Governor Jared Polis signed Senate Bill 26-189 into law, repealing and reenacting Part 17 of Article 1 of Title 6 of the Colorado Revised Statutes, which was originally adopted under Senate Bill 24-205 (the Colorado Artificial Intelligence Act, or "**CAIA**"). SB 26-189 is the product of an extended stakeholder process that followed widespread industry concern with the original CAIA's broad scope, prescriptive duties, and uncertain interaction with established federal consumer finance laws. The final law narrows applicability, eliminates several of the most burdensome obligations originally imposed on developers and deployers, and introduces a series of provisions designed to reduce duplicative compliance burdens. It takes effect January 1, 2027.

Background

Colorado enacted CAIA in May 2024 as the first comprehensive state-level law regulating "high-risk artificial intelligence systems." The original framework imposed extensive duties on both developers and deployers of high-risk AI to use reasonable care to prevent "algorithmic discrimination," to complete impact assessments at least annually, to implement risk management policies aligned with NIST or ISO standards, and to provide a number of consumer disclosures and appeal rights.

Following its enactment, the financial services industry raised significant concerns about the law's broad definitions, overlap with existing federal consumer financial laws, ambiguity around fraud and sanctions controls, and the practical infeasibility of certain disclosure and impact-assessment requirements. Governor Polis acknowledged these concerns in his 2024 signing statement, and the legislature convened a multi-stakeholder task force to refine the framework. SB 26-189 reflects that work product.

The result is a substantively different statute. Rather than amending discrete provisions, SB 26-189 repeals CAIA in its entirety and reenacts a new framework focused on "automated decision-making technology" ("**ADMT**") used in "consequential decisions" affecting consumers.

A New Regulatory Vocabulary

The most fundamental change is new terminology driving substantive narrowing throughout the statute.

The original CAIA regulated "high-risk artificial intelligence systems," defined as any AI system that "makes, or is a substantial factor in making, a consequential decision." The final law regulates "Covered ADMT," defined as automated decision-making technology "used to materially influence a consequential decision." "Materially influence" is in turn defined narrowly to mean that the ADMT output is a "non-de minimis factor" that "affects the outcome" of a consequential decision, and the statute expressly excludes "incidental, trivial, or clerical uses."

The final law also introduces the concept of an "adverse outcome," which is a decision that denies, terminates, revokes, or materially reduces access to a covered opportunity or service, or that results in materially less favorable differentiated pricing or terms. Several of the most consequential consumer-facing obligations (post-decision explanations, correction rights, and human review) are triggered only when an adverse outcome occurs, rather than upon any use of AI in a covered domain.

The list of regulated "covered domains" remains similar to CAIA, including education, employment, residential real estate, financial or lending services, insurance, health-care services, and essential government services, but the exemption framework has been substantially expanded.

In other words, a Covered ADMT is technology that processes personal data and generates an output (i.e., prediction, recommendation, score, ranking, or classification), where that output serves as a more?than? incidental factor that meaningfully affects the outcome of an important decision about an individual's access to, eligibility for, pricing of, or compensation in education, employment, housing, financial/lending services, insurance, health care, or essential government benefits.

Expanded Carve-Outs Particularly Relevant to Financial Institutions

SB 26-189 codifies several express exclusions from the definitions of "ADMT" and "consequential decision" that directly address the operational realities of financial services compliance. Most significantly:

- AML/CFT and sanctions compliance. Activities relating to technologies used for anti-money laundering and counter-terrorist financing controls are excluded from "consequential decision." Likewise, technologies used for economic sanctions compliance (i.e., OFAC programs) are excluded subject to a limited facial-recognition caveat.
- Fraud prevention. Technologies used for fraud prevention, including identity verification, consumer identification, and monitoring and reporting controls required under state or federal law, are excluded.
- Cybersecurity. Activities relating to cybersecurity, spam filtering and system reliability are excluded.
- Routine operations. Low-stakes or routine business processes (i.e., administrative routing, customer service triage, workflow management, communication of decisions) and advertising, marketing, search, and content moderation are excluded.
- Static technologies. Anti-malware, anti-virus, calculators, databases, data storage, firewalls, spell-checking, spreadsheets (that do not use machine learning or foundation models), and similar utility technologies are excluded from the definition of ADMT.

These carve-outs effectively address concerns that the original CAIA might include essential BSA/AML monitoring, sanctions screening, and fraud detection systems required by law for financial institutions.

Elimination of Certain Developer and Deployer Affirmative Obligations

Perhaps the most significant shift is the elimination of certain foundational obligations:

- CAIA's affirmative duty for developers and deployers to "use reasonable care to protect consumers from any known or reasonably foreseeable risks of algorithmic discrimination" is not carried forward in the final law. The free-standing "algorithmic discrimination" cause of action created by CAIA has been eliminated; algorithmic discrimination is now addressed through existing Colorado anti-discrimination law overlaid with a fault-allocation provision (discussed below).

- The requirement that deployers complete annual impact assessments (and additional assessments within 90 days of any intentional and substantial modification).
- The requirement that deployers implement a written risk management policy and program aligned with the NIST AI Risk Management Framework, ISO/IEC 42001, or a comparable framework.
- Obligation that developers and deployers report known or reasonably foreseeable risks of algorithmic discrimination to the Attorney General.
- Public-statement obligations requiring developers and deployers to publish summaries of high-risk AI systems on their websites.

In their place, the final law imposes more modest requirements. Developers must make available to deployers a general statement describing the covered ADMT's intended and known harmful uses, the categories of training data, known limitations, instructions for appropriate use, and the information deployers need to satisfy their own disclosure obligations. Developers must retain records for at least three years, notify deployers of material updates, and provide information sufficient for the deployer's consumer-facing notices.

Streamlined Consumer-Facing Obligations

The consumer-facing disclosure obligations have been reorganized around the new "adverse outcome" trigger:

- **Pre-use notice.** Before a deployer uses a covered ADMT to materially influence a consequential decision, the deployer must provide clear and conspicuous notice to the consumer.
- **Post-adverse-outcome disclosures.** Within 30 days after a consequential decision that results in an adverse outcome, the deployer must provide a plain-language description of the decision and the ADMT's role, instructions for requesting additional information, and an explanation of consumer rights.
- **Consumer rights.** Consumers who experience an adverse outcome may request correction of factually incorrect or materially inaccurate personal data used in the decision, and an opportunity for meaningful human review to the extent commercially reasonable. The right to correction does not extend to opinions, predictions, scores, or protected evaluations. The "meaningful human review" concept is defined to require, among other things, a trained reviewer who does not default to the system output and who has access to sufficient information to understand the output's intended use, material limitations, and principal factors.

Federal Law Harmonization and Exemptions

For regulated industries, it is important to note SB 26-189's express federal-law harmonization provisions and sector specific exemptions:

- **ECOA/Regulation B and FCRA Safe Harbor.** A creditor that provides a notice to a consumer under the Equal Credit Opportunity Act and Regulation B (and, when applicable, the Fair Credit Reporting Act) in connection with a consequential decision involving the offering, denial, pricing, or servicing of credit "complies with the notice or disclosure requirements of this section that relate to the same decision or adverse outcome" so long as the federal notice also satisfies the requirements of the Colorado statute. The creditor is not required to provide a separate or duplicative notice.
- **GLBA Carve-Out.** SB 26-189 "does not require a person to disclose nonpublic personal information in a manner that would violate the federal Gramm-Leach-Bliley Act…or its implementing regulations."
- **Sensitive-Program Confidentiality.** Nothing in SB 26-189 requires disclosure that would compromise the confidentiality or integrity of cybersecurity, fraud prevention, AML/CFT, or sanctions compliance programs

required by law.

- **Insurance Practice Compliance.** Insurers subject to Colorado's existing AI insurance regulation are deemed compliant with SB 26-189 in the "practice of insurance."
- **HIPAA-Covered Entity Carve-Out.** HIPAA-covered entities and their business associates are generally exempt (with a narrow exception for employment-related decisions and a specific disclosure obligation for ADMT used in determining patient financial assistance eligibility).

Notably, the final law does not include a separate, comprehensive carve-out for banks, credit unions, or other depository institutions analogous to the safe harbor in CAIA (which deemed institutions to be in full compliance if they were subject to prudential examination under published guidance substantially similar to CAIA).

Liability and Fault Allocation

SB 26-189 creates a liability and fault-allocation framework that overlays Colorado's existing anti-discrimination laws (i.e., Colorado Anti-Discrimination Act) rather than establishing a standalone cause of action. Fault is apportioned among developers and deployers according to their relative responsibility, with no joint-and-several liability imposed beyond what current law already permits. A developer's exposure is further limited to situations in which the deployer used the ADMT in a manner the developer intended, documented, marketed, advertised, configured, or contracted for. Contractual provisions that indemnify, defend, or hold harmless a developer or deployer for their own acts or omissions violating anti-discrimination laws are void as against public policy. SB 26-189 creates no new private right of action, but it expressly preserves all existing remedies under the Colorado Anti-Discrimination Act, the Colorado Consumer Protection Act, product-liability law, and other applicable statutes. This indemnification ban marks a notable departure from standard vendor contracting practices, requiring financial institutions, fintech companies, and ADMT developers to revisit indemnification, defense, and hold-harmless language in master service agreements, data-processing addenda, and statements of work.

Enforcement & Rulemaking

Enforcement is vested exclusively in the Colorado Attorney General, who treats violations as deceptive trade practices under the Colorado Consumer Protection Act subject to tailored procedural modifications. Before filing suit, the AG must issue a notice of violation and afford a 60-day cure period if remediation is possible (though no cure period is required for knowing or repeated violations.

The AG is also required to promulgate rules by January 1, 2027, clarifying post-adverse-outcome disclosures, the correction and human-review process, the meaning of "materially influence," and other implementation details.

For assistance or additional guidance on the impact of SB 26-189 on your institution, please contact David Bowen or any member of Krieg DeVault's Financial Services practice group.

Disclaimer: The contents of this article should not be construed as legal advice or a legal opinion on any specific facts or circumstances. The contents are intended for general informational purposes only, and you are urged to consult with counsel concerning your situation and specific legal questions you may have.