



www.fdata.global

October 26th, 2026

Office of the Attorney General
Colorado Department of Law
Consumer Protection Section
Ralph L. Carr Judicial Center
1300 Broadway, 9th Floor
Denver, CO 80203

Submitted via the Colorado Attorney General's public comment portal.

Re: Interim Draft Automated Decision-Making Technology & Conversational Artificial Intelligence Service Rules, 4 CCR 904-6

The Financial Data and Technology Association ("FDATA") appreciates the opportunity to provide comments to the Colorado Department of Law (the "Department") on its interim draft of the Automated Decision-Making Technology & Conversational Artificial Intelligence Service Rules (the "Draft Rules"). The Draft Rules would implement the Automated Decision-Making Technology in Consequential Decisions Act, as amended by SB 26-189 (the "ADMT Act"). FDATA's comments are limited to the provisions implementing that ADMT Act.

FDATA supports the ADMT Act's goal of giving Colorado consumers transparency into, and recourse from, consequential decisions that are materially influenced by automated technology. The interim draft reflects a number of thoughtful changes, and FDATA is encouraged in particular by the Department's clarification that tools used solely to summarize, organize, translate, draft, route, or present information are not ADMT and do not Materially Influence a Consequential Decision.

As currently written, however, FDATA believes the Draft Rules remain overly broad and could be read to include activity that has no connection to a Consequential Decision. Additionally, the draft rules are not clear where the statutory exclusion for fraud prevention and identity verification ends. This lack of clarity may have the unintentional effect of making providers hesitant to offer such safeguards to protect Coloradans. FDATA respectfully urges the Department to clarify the scope of the rules to align correction obligations with the way data moves through the financial system, and to avoid sweeping in the payment risk tools that protect consumers.

About FDATA

FDATA and our members have for years been strong advocates for providing consumers, small business owners, investors, and other end users with legally binding financial data rights. As we have seen in other jurisdictions around the world that have granted their citizens legal rights to access and share their financial data, a customer-centric ecosystem in which the end user is in full

control of their data leads to a more innovative, more competitive, and more transparent financial marketplace.

Our members' products, services, and tools underscore this reality. FDATA's Membership includes firms with a variety of business models, from budgeting and personal financial management tools to lending platforms and pay-by-bank payment solutions, and collectively they provide more than 100 million American consumers and small business owners, including many in Colorado, access to vital financial services and products. Regardless of their business model, every FDATA member's products or services share one fundamental and foundational requisite: the ability of a customer to actively permission access to some component of their own financial data that is held by another financial services provider. Because a growing number of credit, payment, and account-opening decisions now rely in whole or in part on consumer-permissioned data, our members have a direct interest in the regulatory boundaries of the ADMT Act.

Deployer Responsibilities Should Remain with the Decision-Maker

FDATA supports the revised definition of "Deploy" and Rule 4.3's allocation of Deployer responsibilities to the entity making the Consequential Decision. We urge the Department to retain these provisions and agree that operating Covered ADMT and delivering its output to another entity does not, by itself, transform a provider into a Deployer where that other entity is the one making the Consequential Decision. Obligations based on assisting a Deployer, if any, should be commercially reasonable, defined by contract, and limited to functions and information within the provider's control, without duplicating any Developer obligations.

FDATA further appreciates that Rule 4.3(B) presents contracting between a Deployer and a third party that runs Covered ADMT on the Deployer's behalf as something a Deployer "may" do. Other language in Rule 4.3, however, could be read to suggest that such a third party can be compelled to take on the obligations of the Deployer. Rule 4.3(B) refers to contracting "as necessary, to require the third party to perform functions to assist the Deployer." Rule 4.3(C) provides that a third party "can only be required to assist the Deployer" where the Deployer is itself covered by the Act, which implies that the third party can be required to do so whenever the Deployer is covered. The example in Rule 4.3(C)(2) likewise describes contracting "to require" a provider's help. FDATA asks the Department to clarify that Rule 4.3 imposes no independent obligation on third parties and that the scope of any assistance under Rule 4.3 is set by the parties' contract. For example, the Department could add to Rule 4.3: "Nothing in this Rule 4.3 imposes an obligation on a third party to assist a Deployer except as the third party and the Deployer agree by contract, or as required by other applicable laws."

Consumer-Permissioned Data Access Is Not ADMT

The ADMT Act defines ADMT as technology that processes personal data and uses computation to generate output, including classifications, rankings, and scores, that is used to make, guide, or assist a decision concerning an individual. Consumer-permissioned data access does not fit that definition. Data access platforms retrieve information from the consumer's financial institution, transmit it to the provider the consumer has chosen, and normalize it into a standard format so that it can be read. In doing so, it does not render any judgment, either about the data it transmits or the consumer to whom it belongs.

FDATA appreciates that the ADMT Act and the Draft Rules already reflect the distinction that consumer-permissioned data access, transmission, normalization, and objective categorization are not ADMT and are not a “component” of Covered ADMT, and asks the Department to preserve this distinction in the final rules. The Draft Rules already draw this line well: 6.1(C) defines “other inference” as an opinion, characterization, or non-objective conclusion reached by the ADMT, and the housing examples in Rule 6.2(D) distinguish between a tool that labels applicant data as “positive” or “negative” and a tool that organizes the same data without scoring or recommending anything.

This position is consistent with the position FDATA has taken before federal regulators. In comments to the Consumer Financial Protection Bureau (“CFPB”) on its proposed amendments to Regulation V, FDATA explained that consumer-permissioned data platforms, and the analytics providers that help lenders organize bank account data, do not fit the role or function the Fair Credit Reporting Act assigns to consumer reporting agencies, and warned against conflating these fundamentally different business models.¹

Everyday Transaction Categorization Is Organizing Information, Not ADMT

Categorization is one of the most common functions performed with consumer-permissioned data. For example, budgeting apps sort a consumer’s spending into groceries, utilities, and dining so they can see where their money goes, thereby giving the tools to better manage their money, and tax preparation tools separate income from transfers between the consumer’s own accounts. Because categorization is often performed with machine learning and assigns a label to each transaction, however, it could be characterized as a “classification” under section 6-1-1701(2)(a), C.R.S., even though transaction categorization technology does not generate a prediction or classification about an individual. Categorization describes what a transaction is, not who the consumer is or what they are likely to do. It is simply an organization of the consumer’s own records, not a prediction, classification, or determination about the consumer.

FDATA strongly supports the exclusion in section 6-1-1701(2)(b)(II), C.R.S., and Rule 6.1(D) for tools used solely to summarize, organize, translate, draft, route, or present information for human review, and urges the Department to retain it in the final rules. Transaction categorization and similar data enrichment that organizes a consumer’s own financial data without generating a score, prediction, or determination about the consumer falls within that exclusion, as the Department’s own example Rule 6.2(D)(2) illustrates. FDATA encourages the Department to add transaction categorization as an illustrative example.

FDATA also notes that the Draft Rules leave unclear whether a miscategorized transaction is subject to the correction requirements in Rule 8.4. For example, a deposit labeled as a transfer rather than payroll could be construed to be required to be treated as factually incorrect Personal Data that must be corrected within 45 days. FDATA recommends that the Department clarify that the appropriate remedy for a miscategorized transaction is to re-categorize it, or to flag it for

¹ Financial Data and Technology Association, Comment Letter on Protecting Americans from Harmful Data Broker Practices (Regulation V), Docket No. CFPB-2024-0044 (Feb. 24, 2025).

consideration in any reconsideration of the decision, and that the underlying transaction record remains the responsibility of the institution that holds the account.

Material Influence Should Turn on the Output’s Actual Role in the Decision

FDATA supports the revised substantial-factor standard and the recognition that independent evidence and decision criteria can establish that an ADMT output was a De Minimis Factor. However, Rule 6.1(A) continues to presume material influence where an individualized output is reviewed or used to screen information and is consistent with the outcome. Directional consistency does not establish that an output substantially affected the decision.

FDATA asks the Department to remove this presumption or, alternatively, limit it to circumstances in which the output determines the outcome, controls an eligibility threshold, or serves as the sole individualized basis for the decision. Documented, consistently applied decision criteria and contemporaneous evidence demonstrating that the output was not a substantial factor should be sufficient to rebut any remaining presumption.

Consumer-Permissioned Data Should Be Corrected at the Source

FDATA has long maintained that responsibility for the accuracy of consumer financial data should rest with the original holder of that data, so long as no entity with access to it has modified, combined, reformatted, or evaluated the data in a way that could alter its meaning or accuracy.² The bank or credit union that holds the consumer’s account is the source of truth for the consumer’s transactions and balances. A data recipient that merely displays or transmits that data cannot amend it. If it tries, the result is two conflicting records of the same account: the actual record at the consumer’s financial institution and a “corrected” copy held by a third party with no control over the account. That phantom record can be relied upon in later decisions while the error at the source goes uncorrected and continues to flow to every other provider the consumer has authorized.

FDATA is concerned that Rule 8.4(B) could unintentionally produce exactly this result due to the requirement for a Deployer to correct Personal Data in its possession or control within 45 days. A lender receiving transaction history through a data aggregator possesses a *copy* of that information, but does not have the access to correct the *original* account-holding institution’s underlying records. The final rules should explain how correction obligations apply in that circumstance without creating inconsistent versions of the same account data.

FDATA appreciates that the interim draft removes the prior provision under which a consumer’s assertion alone established inaccuracy, and allows a Deployer to direct the consumer to the third-party source of the data. FDATA urges the Department to go a step further and provide that, where an error originates in an account-holding institution’s records and the Deployer received those records without introducing the error, the Deployer may satisfy the applicable correction requirement through a coordinated process that directs the consumer to the institution, obtains refreshed data after correction, and reconsiders the decision if appropriate. This approach should not excuse a Deployer or intermediary from correcting factual errors it introduced or controls, or

² Id.

displace FCRA dispute and accuracy obligations, to the extent such obligations are independently applicable.

Retention Obligations Should Be Reconciled with Data Minimization

FDATA has consistently advocated for data minimization as key best practice when handling consumer financial data. Our members believe that consumers own their data and determine who has access to it, that data aggregators and third parties should delete consumer data when the consumer revokes access, when the data is no longer necessary for the product or service, or when the relationship with the consumer ends.³ FDATA has also opposed regulatory requirements that would force consumer-permissioned platforms to collect and retain more personal information than they need.⁴

Several provisions of the Draft Rules assume that detailed records will be retained long after a decision is made. For example, Rule 8.3(B)(2) gives consumers the right to obtain all ADMT inputs pertaining to them, Rule 8.7(H) requires a record of the primary evidence available to a human reviewer, and Rule 7.6(A)(5) requires Deployers to identify each source of Personal Data by name. To be clear, FDATA does not object to the goals behind these provisions, but is concerned that together they may push Deployers and their service providers to retain full transaction histories that would otherwise be deleted, including after a consumer has revoked access. FDATA urges the Department to clarify that the Rules do not create retention obligations that override or conflict with data retention or deletion obligations arising under other applicable law.

The Final Rules Should Align with Federal FCRA and ECOA Obligations

FDATA urges the Department to expressly recognize compliance with existing federal requirements as satisfying the corresponding requirements of the final rules where those federal requirements provide equivalent consumer protections. This principle should guide the treatment of disclosures, access, and correction rights, while preserving any additional protections required by Colorado law.

Several parts of the Draft Rules would create additional obligations that may be unnecessary given existing federal laws. For example, Rule 5.2.B would require developers to describe the types of Consequential Decisions for which a Covered ADMT is intended and those for which a Covered ADMT would be inappropriate or harmful. But the FCRA already strictly limits the purposes for which a consumer report may be provided to a user (who might be a Deployer under the ADMT Draft Rules). The FCRA further requires consumer reporting agencies to maintain reasonable policies and procedures to limit the furnishing of consumer reports to permissible purposes, including “require[ing] that prospective users of the information identify themselves, certify the purposes for which the information is sought, and certify that the information will be used for no other purpose.”⁵ For consumer reports, the Developer disclosures would offer no benefit to

³ Id.; see also FDATA North America, Privacy Principles (Mar. 2023); Financial Data and Technology Association, Comment Letter on Personal Financial Data Rights Reconsideration, Docket No. CFPB-2025-0037 (Oct. 21, 2025).

⁴ Comment Letter on Protecting Americans from Harmful Data Broker Practices, *supra* note 1.

⁵ 15 U.S.C. § 1681e(a).

Deployers, who will have already certified the purposes for which they are requesting a consumer report. FDATA requests that the Department provide a safe harbor for compliance with the FCRA.

Similarly, the Equal Credit Opportunity Act (“ECOA”) and Regulation B require creditors to provide adverse action notices that state the specific reasons for the action taken, and the FCRA governs the accuracy of information in consumer reports and the consumer’s right to dispute it. FDATA appreciates that Rule 7.7 permits applicable ECOA or FCRA adverse action notices to satisfy the Adverse Outcome disclosure requirement when accompanied by the additional information required under Colorado law, including through a separate supplement provided in accordance with the rule. The Department should preserve this flexibility. The consumer rights in Rule 8, however, apply in full on top of these federal requirements. For example, a consumer whose credit application was denied based in part on a cash-flow score furnished by a consumer reporting agency could pursue a FCRA dispute with the agency and a separate correction request with the lender under Rule 8.4. The final rules should coordinate these processes to avoid duplicative handling and inconsistent outcomes regarding the same information.

FDATA urges the Department to extend the approach of Rule 7.7 to the consumer rights in Rule 8. Where information used in a Consequential Decision is subject to the FCRA’s dispute and accuracy requirements, a Deployer should satisfy its access and correction obligations by directing the consumer to that process and honoring its outcome.

Routine and Low-Stakes Decisions Should Be Clearly Excluded from Consequential Decisions

FDATA supports the ADMT Act’s focus on decisions that determine a consumer’s access to credit, housing, employment, and other important opportunities. The General Assembly made clear, however, that the Act is not intended to reach every determination a business makes about a consumer. Section 6-1-1701(3)(b)(I), C.R.S., excludes from the definition of Consequential Decision “low-stakes or routine decisions, actions, and business processes” that do not materially influence eligibility for, selection for, denial of, compensation for, pricing of, or access to an opportunity or service in a Covered Domain.

The Draft Rules should give these exclusions practical content and provide additional examples, particularly for financial services. Rule 2 defines “Financial or Lending Service” to include “the extension of credit or a loan, transmitting or exchanging funds, the provision of deposit or checking accounts, check cashing, or installment payment plans.” FDATA urges the Department to provide in the final rules examples of decisions that are not Consequential Decisions, such as:

1. Selecting which payment methods to offer a consumer for a particular transaction, or asking a consumer to complete a transaction with a different payment method, where the consumer can still complete the transaction;
2. Deciding whether to provide an optional benefit beyond a provider's standard terms, where the consumer still receives the standard terms;
3. Requesting additional information before processing a particular transaction or account change;
4. Determining how a consumer-initiated payment is authorized, routed, or processed, where the consumer can still complete the transaction; and
5. Determining the timing or channel of account notifications and reminders.

Each of these may involve a technology-assisted inference about an individual consumer, but none denies, terminates, or materially restricts the consumer's access to a Financial or Lending Service.

Payment Risk Scores Should Not Be Covered Under the Rule

FDATA is particularly concerned that the Draft Rules could reach consumer-friendly payment risk scores made possible by consumer-permissioned data access. As noted above, Rule 2 defines "Financial or Lending Service" to include transmitting or exchanging funds and the provision of deposit or checking accounts. A tool that scores the likelihood that a pay-by-bank payment will be returned for, e.g., insufficient funds, produces a score about an individual that may be used to approve, delay, or decline a transfer of funds, or direct the consumer to a different method of transfer. Read literally, that determination could be a Consequential Decision and the tool could be Covered ADMT.

The ADMT Act excludes technologies used for anti-money laundering and sanctions compliance, and for fraud prevention, including identity verification, consumer identification, monitoring, and reporting controls.⁶ Rule 7.8(C) is limited to similar anti-money laundering, sanctions compliance, and fraud prevention programs. Much of the payment risk work in the pay-by-bank ecosystem, however, is neither solely fraud prevention, nor mandated by statute. It is driven by industry and risk management practices that payment providers, financial institutions, and data platforms have developed together to combat scams and first-party fraud, in addition to insufficient funds or ineligible accounts. If these tools fall outside the exclusion because their purpose is not solely fraud-prevention or consumer identification, providers would have to choose between delivering adverse outcome disclosures, data access responses, and human review for every flagged payment, or scaling back industry controls that protect consumers.

Burden aside, explaining the factors behind a risk score to the person who triggered it would also give bad actors a roadmap for evading detection, potentially encouraging "gaming" of the system. With respect to pay-by-bank, the result would be to place such products at a disadvantage to card payments, potentially limiting the options available to consumers, and undermine the industry-led anti-fraud efforts that policymakers have rightly encouraged.

Principal Factor Requirements Should Be Removed for Developers as Well as Deployers

⁶ Section 6-1-1701(3)(b)(VI)-(VIII), C.R.S.

FDATA supports the removal of the requirements from Rule 7.4(B) that Deployer Adverse Outcome disclosures include principal factors and inferences. Consistent with this change, FDATA asks the Department to remove Rule 5.2(C)(3)'s requirement that Developers provide instructions for determining a Covered ADMT's "reasoning and primary factors," as these instructions no longer support a required disclosure.

Although the ADMT Act requires individuals conducting Meaningful Human Review to understand "the principal factors used to generate the output," this obligation can be addressed through the general Developer documentation required by section 6-1-1702(1)(d), C.R.S., describing the categories of inputs and the types of factors the Covered ADMT generally relies on.

Developer Documentation Should Be Proportionate and Protect Confidential Information

FDATA supports Rule 5.3's recognition that Developers may provide summaries, categorical descriptions, or generalized information that protects trade secrets. Rules 5.2 and 5.3 should clarify that documentation addresses intended uses, relevant data categories, known limitations and risks, and practical instructions sufficient to support appropriate use and applicable consumer disclosures. These provisions should not require disclosure of proprietary model logic or reconstruction of protected information through alternative disclosures.

A Developer withholding protected information should be permitted to identify the category withheld and the basis for protection without a separate requirement to cite legal authority. Rule 4.2 should also permit downstream documentation requirements to be satisfied through appropriate summaries, subject to confidentiality protections consistent with statutory disclosure duties. If the Department adopts additional testing-disclosure requirements, they should be limited to whether testing occurred, the general type of testing, and material findings, rather than raw results or proprietary methodologies.

Conclusion

FDATA supports the Department's efforts to give Colorado consumers transparency and recourse when automated technology materially influences decisions that determine their access to credit, housing, employment, and other important opportunities. The clarifications requested in this letter would preserve those protections while keeping the final rules focused on consequential decisions, consistent with the Act's text and exclusions, rather than the consumer-permissioned data infrastructure, budgeting tools, and fraud controls on which consumers rely every day. Thank you for considering our comments. FDATA and our member companies welcome the opportunity to provide further insights and to serve as a resource to the Department as it finalizes the rules.

Sincerely,

A handwritten signature in dark ink, appearing to read "SB", followed by a long horizontal line extending to the right.

Steven Boms
Executive Director
FDATA