CENTER FOR DEMOCRACY & TECHNOLOGY

Testimony of Dr. Travis Hall
Center for Democracy & Technology

SB 26-189 – Regarding the Implementation of Automated Decision-Making Systems in Matters of Significant Consequence

Colorado Senate Business, Labor and Technology Committee

May 5, 2026

Chair and Members of the Committee –

I appreciate the opportunity to testify on behalf of the Center for Democracy & Technology regarding SB 26-189.

CDT is a nonprofit, nonpartisan organization that works to advance civil rights and civil liberties in the digital age, for everyone. A key part of that mission, since our founding 30 years ago, when the internet was in its infancy, is working to protect consumers against invasion of their privacy, and misuse of their private personal information, to exploit them or discriminate against them.

To be clear: automated decision systems are powerful tools, and we should seek to ensure that any bias in these systems does not lead to unfair discrimination based on protected classes. Unfortunately, there are documented instances of these tools discriminating against legally protected classes (whether intentional or not),

causing harm to real people's lives and livelihoods. The core problem these systems present is the fact that they obfuscate decision making processes, black boxing how and why a particular determination is made, and even who is responsible.

SB 24-205 sought to rectify this problem by making developers and deployers explicitly responsible for assessing and mitigating the potentially harmful discrimination caused by the use of automated decision systems. SB 189 walks back many of these responsibilities, but maintains some of the fundamental requirements for disclosure and transparency. At a baseline level, deployers must have the information necessary to determine whether a tool they are considering using in a consequential decision carries unwarranted risks. Individuals should be able to understand what role an automated decision system played in decisions about their access to opportunities like housing, health, employment, or education, and should be empowered to challenge these decisions.

And, perhaps most importantly, when unlawful discriminatory impact occurs through the use of these systems, those responsible for that impact must be held rightly accountable. As SB 189 has walked back the explicit responsibilities of developers and deployers to assess potential discriminatory impact, the incentives to ensure that they mitigate such harm must be clear.

SB 189 is a limited step in the right direction on these fronts. However, there are still many areas for improvement. For example, cabining notification to only "adverse" decisions without clarifying what is or is not "adverse" will likely lead to under-reporting. The section on liability is confusing as drafted, and should be reconsidered to provide clear liability. We are happy to work with the committee on these and other drafting issues.

ata ACTION
Telehealth Policy to Transform Healthcare

May 4, 2026

The Honorable Jessie Danielson
Chair, Senate Business, Labor, and Technology Committee
Colorado State Senate
200 E Colfax Avenue
RM 346
Denver, CO 80203

RE: ATA ACTION CONCERNS REGARDING SB 189

Dear Chair Danielson and Members of the Senate Business, Labor, and Technology Committee,

On behalf of ATA Action, I am writing to share our perspective on Senate Bill 189 concerning the use of automated decision-making technology in consequential decisions. While our organization is not opposed to the intent of the legislation, we believe that there are areas of the legislation lacking necessary clarity that should be addressed before the legislation is advanced.

ATA Action is the affiliated policy and legislative advocacy arm of the American Telemedicine Association. ATA Action is the leading advocacy organization dedicated to advancing policy and accelerating the adoption of technology-enabled healthcare. Working collaboratively with federal and state legislators and policymakers, our organization drives industry momentum by influencing legislative and regulatory developments in telehealth, virtual care, remote patient monitoring, artificial intelligence in health, health data privacy, private sector healthcare investment, and more. We represent a diverse membership – including hospital systems, technology companies, professional associations, direct-to-consumer digital health providers, payers, pharmaceutical manufacturers, digital therapeutics developers, and remote monitoring organizations.

First, we understand and appreciate the attempt to exempt certain health care entities from the framework, given that health entities already must follow multiple federal and state laws, including regulation on discrimination, privacy of patient information, informed consent, and use of clinical decision support in the EHR. However, we have concerns about why Section 6-1-1708 only exempts covered entities under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Our organization represents both HIPAA covered entities and entities who comply with HIPAA guidelines but are not covered entities as they are cash-pay and do not accept insurance. It is unclear why the legislature would distinguish between HIPAA covered healthcare entities and those who are not for this legislation, as HIPAA does not have any specific provisions for the use of automated decision making for consequential decisions.

Likewise, Section6-1-1708(3)(b) states that "this subsection (3) applies only if the health-care provider is operating from a location in Colorado." This creates confusion and potential compliance challenges for telehealth providers treating patients in Colorado. For example, a telehealth platform may treat patients in Colorado using providers located both inside and outside of Colorado, creating two different compliance pathways for Colorado-based and out-of-state providers, who have the same Colorado license and treat the same Colorado patients.

Finally, it is unclear, under the drafted definition of "consequential decision," when the provisions of this legislation would be triggered in healthcare settings. For example, the current definition excludes "routine

ata ACTION
Telehealth Policy to Transform Healthcare

scheduling" by classifying it as a low-stakes decision; however, in a healthcare setting when a patient's appointment is scheduled could also be considered to impact a consumer's access to a "covered domain," with the bill deeming health-care services to be a "covered domain."

We believe all of these issues can be solved by exempting all health-care providers, regardless of HIPAA status or location, from the provisions of this legislation. We believe this change is necessary to avoid confusion for providers who are already using safe and proven automated technologies to aid in patient care and will allow for the proper consideration on how to best regulate the use of these technologies in health-care settings.

We share the Legislature's commitment to protecting Coloradans and to ensuring that automated tools are deployed responsibly and with appropriate oversight. We urge the Committee to exempt health-care providers from this bill before it is advanced. If you have any questions or would like to discuss further, please contact me at hyoung@ataaction.org.

Kind regards,

Hunter Young

Hunter Young
Head of State Government Relations
ATA Action

Business Software Alliance

May 5, 2026

The Honorable Jessie Danielson
200 E Colfax Ave.
Denver, CO 80203

Re: Significant Concerns with Liability Regime and Definitions in SB 189

Dear Chair Danielson,

The Business Software Alliance appreciates the opportunity to share insights from the enterprise software sector on artificial intelligence (AI) and SB 189. BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing cutting edge services, and their products are used by businesses of all sizes across every sector of the economy.

AI is changing the way we live and work, and it has real-world benefits. Realizing the potential of AI requires trusting that the technology is developed and deployed responsibly. Crafting AI legislation that promotes responsible uses of AI and protects against misuse is one of the most important technology issues today, and one we already see governments beginning to tackle. The most effective way to address this issue is through a single, national law. However, just as states took the lead in adopting consumer privacy laws, we recognize states are again leading with AI legislation.

Although we appreciate the notable improvements made in SB 189, including the removal of the disclosure requirements to the Attorney General and the streamlined developer disclosure requirements, we have significant concerns with the bill's unworkable liability regime and broad definitions. We are concerned not only about the effect those provisions will have on responsible AI adoption in the state but also the precedent those provisions will set across the country.

Below we discuss our concerns in more detail. We would welcome the opportunity to further discuss these issues with you or a member of your staff.

[1] BSA's members include: BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. AI Legislation Should Hold Companies Accountable for Risks Within Their Control

The bill opens the door for AI developers to be held liable under the state's anti-discrimination law. That approach creates significant concerns and could have significant negative consequences on the responsible adoption of everyday AI tools. We strongly recommend policymakers avoid new and untested liability regimes and focus instead on alternative accountability frameworks that are workable in practice.

When crafting legislation, several mechanisms are available to policymakers to ensure companies comply with their legal obligations. Not all mechanisms, however, are best suited for AI policy. The most straightforward approach to ensuring that companies develop and use AI responsibly is to place clear obligations on them, based on their role in the AI value chain, and to hold them liable when they fail to comply. This approach creates clarity for businesses in understanding their responsibilities and provides robust protections for consumers.

At the state level, we've seen interest in ensuring companies develop and deploy AI responsibly by assigning them a duty of care. The concept of a "duty of care" is deeply rooted in tort law, which governs civil wrongs and personal injury. Courts frequently impose a duty of care on individuals or organizations that have the power to prevent foreseeable harm to others. For example, drivers must operate their cars safely to avoid injuring pedestrians; a doctor must act as a reasonably competent physician would under similar circumstances; a company must ensure that its products are safe for ordinary use. These duties are not static rules — they evolve with context, technology, and social expectations. The standard is flexible, focusing on whether an actor took reasonable steps to prevent foreseeable harm given their role, expertise, and resources. As a result, that flexibility can promote responsible development and the use of fast-changing technologies like AI, especially when paired with a specific list of actions that companies can take to meet the standard.

The approach to liability taken in the bill confuses the roles of developers and deployers and risks holding developers liable for decisions they have no insight into or control over. Particularly in the enterprise context, AI developers often do not have the necessary information to know how their customer made a consequential decision and are not in a position to mitigate risks of discrimination when their customer makes those decisions.

All companies that develop and use AI systems have responsibilities to manage AI risks, but those obligations must reflect the role of each type of company, since each will know different information about an AI system and will be able to take different actions to identify

and mitigate risks. Legislation must reflect these differences to create obligations that work in practice to safeguard consumers.

Distinguishing between different entities based on their role in the AI ecosystem can ensure companies are better able to fulfill their obligations and better protect consumers. For example, a developer would be able to describe the features of data used to train an AI system, but it generally would not have insight into how the AI system is used after another company has purchased and deployed the AI system. Instead, the deployer using the system is generally best positioned to understand how the AI system is being used, including whether that use aligns with its intended use, any human oversight, any complaints received, and real-world factors affecting the system's performance.

The bill's liability regime is novel and risks making Colorado an outlier in its approach to AI regulation. In contrast to the bill's approach to liability, a straightforward approach to assigning responsibilities to different companies and holding each company accountable for their obligations emphasizes responsible behavior — encouraging both developers and deployers to identify and address risks, conduct robust testing, and act promptly when problems emerge.

II. AI Legislation Should Focus on AI Systems That Decide Consumers' Important Life Opportunities

While we appreciate that the bill includes a focus on ADMTs intended or contracted to make consequential decisions, we are concerned that several of the bill's definitions are broadly construed and undercut that focus. We strongly recommend the bill be amended to tailor its scope. We specifically recommend revising the definitions of ADMT, covered ADMT, consequential decision, materially influences, deployer, and developer.

These definitions are critical to ensuring that AI legislation focuses on the uses of AI that have the most impact on consumers' lives and avoid broadly regulating a particular type of technology, since risks will vary greatly across different uses of AI systems. Many everyday uses of AI present few risks to individuals and create significant benefits, like helping organize digital files, auto-populate common forms for later human review, improve a company's ability to forecast supply chain issues, and detect, prevent, and respond to cybersecurity threats. AI legislation should avoid a one-size-fits-all approach, since the risks associated with AI tools are use-case dependent.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

* * *

Thank you for allowing us to provide the enterprise software sector's perspective on the bill. We welcome the opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Meghan Pensyl
Director, Policy

Cc: Vice Chair Hinrichsen; Members of the Senate Business, Labor, & Technology Committee

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Business Software Alliance

May 5, 2026

The Honorable Jessie Danielson
200 E Colfax Ave.
Denver, CO 80203

Re: Significant Concerns with Liability Regime and Definitions in SB 189

Dear Chair Danielson,

The Business Software Alliance appreciates the opportunity to share insights from the enterprise software sector on artificial intelligence (AI) and SB 189. BSA is the leading advocate for the global software industry.[1] BSA members are at the forefront of developing cutting edge services, and their products are used by businesses of all sizes across every sector of the economy.

AI is changing the way we live and work, and it has real-world benefits. Realizing the potential of AI requires trusting that the technology is developed and deployed responsibly. Crafting AI legislation that promotes responsible uses of AI and protects against misuse is one of the most important technology issues today, and one we already see governments beginning to tackle. The most effective way to address this issue is through a single, national law. However, just as states took the lead in adopting consumer privacy laws, we recognize states are again leading with AI legislation.

Although we appreciate the notable improvements made in SB 189, including the removal of the disclosure requirements to the Attorney General and the streamlined developer disclosure requirements, we have significant concerns with the bill's unworkable liability regime and broad definitions. We are concerned not only about the effect those provisions will have on responsible AI adoption in the state but also the precedent those provisions will set across the country.

Below we discuss our concerns in more detail. We would welcome the opportunity to further discuss these issues with you or a member of your staff.

[1] BSA's members include: BSA's members include: Adobe, Alteryx, Amadeus, Asana, Atlassian, Autodesk, Avalara, Bentley Systems, Box, Cisco, Cohere, Cohesity, Dassault Systemes, Databricks, Datadog, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, PTC, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Veeam, Workday, Zendesk, and Zoom Communications Inc.

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

I. AI Legislation Should Hold Companies Accountable for Risks Within Their Control

The bill opens the door for AI developers to be held liable under the state's anti-discrimination law. That approach creates significant concerns and would have significant negative consequences on the responsible adoption of everyday AI tools. We strongly recommend policymakers avoid new and untested liability regimes and focus instead on alternative accountability frameworks that are workable in practice.

When crafting legislation, several mechanisms are available to policymakers to ensure companies comply with their legal obligations. Not all mechanisms, however, are best suited for AI policy. The most straightforward approach to ensuring that companies develop and use AI responsibly is to place clear obligations on them, based on their role in the AI value chain, and to hold them liable when they fail to comply. This approach creates clarity for businesses in understanding their responsibilities and provides robust protections for consumers.

At the state level, we've seen interest in ensuring companies develop and deploy AI responsibly by assigning them a duty of care. The concept of a "duty of care" is deeply rooted in tort law, which governs civil wrongs and personal injury. Courts frequently impose a duty of care on individuals or organizations that have the power to prevent foreseeable harm to others. For example, drivers must operate their cars safely to avoid injuring pedestrians; a doctor must act as a reasonably competent physician would under similar circumstances; a company must ensure that its products are safe for ordinary use. These duties are not static rules — they evolve with context, technology, and social expectations. The standard is flexible, focusing on whether an actor took reasonable steps to prevent foreseeable harm given their role, expertise, and resources. As a result, that flexibility can promote responsible development and the use of fast-changing technologies like AI, especially when paired with a specific list of actions that companies can take to meet the standard.

The approach to liability taken in the bill confuses the roles of developers and deployers and risks holding developers liable for decisions they have no insight into or control over. Particularly in the enterprise context, AI developers often do not have the necessary information to know how their customer made a consequential decision and is not in a position to mitigate risks of discrimination when their customer makes those decisions.

All companies that develop and use AI systems have responsibilities to manage AI risks, but those obligations must reflect the role of each type of company, since each will know different information about an AI system and will be able to take different actions to identify

and mitigate risks. Legislation must reflect these differences to create obligations that work in practice to safeguard consumers.

Distinguishing between different entities based on their role in the AI ecosystem can ensure companies are better able to fulfill their obligations and better protect consumers. For example, a developer would be able to describe the features of data used to train an AI system, but it generally would not have insight into how the AI system is used after another company has purchased and deployed the AI system. Instead, the deployer using the system is generally best positioned to understand how the AI system is being used, including whether that use aligns with its intended use, any human oversight, any complaints received, and real-world factors affecting the system's performance.

The bill's liability regime is novel and risks making Colorado an outlier in its approach to AI regulation. In contrast to the bill's approach to liability, a straightforward approach to assigning responsibilities to different companies and holding each company accountable for their obligations emphasizes responsible behavior—encouraging both developers and deployers to identify and address risks, conduct robust testing, and act promptly when problems emerge.

II. AI Legislation Should Focus on AI Systems That Decide Consumers' Important Life Opportunities

While we appreciate that the bill includes a focus on ADMTs intended or contracted to make consequential decisions, we are concerned that several of the bill's definitions are broadly construed and undercut that focus. We strongly recommend the bill be amended to tailor its scope, specifically the definitions of ADMT, covered ADMT, consequential decision, materially influences, deployer, and developer.

AI legislation should focus on the uses of AI that have the most impact on consumers' lives and avoid broadly regulating a particular type of technology, since risks will vary greatly across different uses of AI systems. Many everyday uses of AI present few risks to individuals and create significant benefits, like helping organize digital files, auto-populate common forms for later human review, improve a company's ability to forecast supply chain issues, and detect, prevent, and respond to cybersecurity threats. AI legislation should avoid a one-size-fits-all approach, since the risks associated with AI tools are use-case dependent.

* * *

Thank you for allowing us to provide the enterprise software sector's perspective on the bill. We welcome the opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,

Meghan Pensyl
Director, Policy

Cc: Vice Chair Hinrichsen; Members of the Senate Business, Labor, & Technology Committee

200 Massachusetts Avenue, NW
Suite 310
Washington, DC 20001

P 202-872-5500
W bsa.org

Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

May 5, 2026

Senator Jessie Danielson
Chair
Senate Business, Labor, & Technology Committee
Colorado House of Representatives
200 E Colfax Avenue
Denver, CO 80203

Chair Danielson, Vice Chair Hinrichsen, and members of the committee:

On behalf of the Consumer Data Industry Association (CDIA), I write to request amendments to SB26-189 to better align the bill with the federal Fair Credit Reporting Act (FCRA) that governs consumer reporting agencies (CRAs), consumer reports, and the users of consumer reports, particularly in relation to adverse outcomes. While the current text of the bill acknowledges consumer notices and dispute processes under the FCRA for certain permissible purposes, those requirements apply to all allowed uses of consumer reports, not just in the credit context. It is our desire to see existing language expanded to ensure that Colorado's artificial intelligence law treats all consumer reporting agencies, consumers reports, and users of consumer reports equally in all contexts.

CDIA is the trade association representing consumer reporting agencies ("CRAs"), including the nationwide credit bureaus, regional and specialized credit bureaus, and background check and residential screening companies. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, thereby helping ensure fair and safe transactions for consumers and facilitating consumer's access to financial products and other services suited to their unique needs.

CDIA and its members appreciate the thoughtful and iterative process that led to SB26-189. While we were unable to participate formally as part of the working group, the revised structure of the bill represents an improvement over current law, with clearer definitions, clearer obligations for developers and deployers, and clear consumer rights that are familiar, in concept, to our industry. In particular, and as noted above, CDIA appreciates the current structure's recognition that many of the consumer rights SB26-189 intends to establish related to automated decision making technology are already established under and required by the FCRA for the consumer reporting system.

As the committee may know, our members, their products and their customers are all tightly regulated at the federal level by the FCRA. In addition, the FCRA establishes robust rights for consumers related to how consumer reports are accessed and used, particularly in relation to consequential decisions. This includes the right to know who has requested a report, to know who is furnishing information appearing on a report, to dispute the completeness or accuracy of the report, and to know when information in the report led to an adverse outcome. Colorado has

previously incorporated much of the FCRA into state statute with similar Attorney General-driven enforcement, providing an additional layer of protection to consumers.
While CDIA recognizes that the concepts underpinning SB26-189 are in some way analogous to the existing regulations on the consumer reporting system, there are sufficient differences between the requirements of the FCRA and SB26-189 to justify expanding the existing compliance exemption.

For example, 6-1-1702(a) requires developers (CRAs) to provide deployers (Users) to provide a "general statement describing the intended uses and known or harmful inappropriate uses". However, the FCRA, at 15 U.S.C. § 1681b enumerates a list of "permissible purposes" under which a CRA may furnish a report to a user. Without attesting to having a permissible purpose, a CRA cannot furnish a report to a user. There are also circumstances where a type of report, for example a credit score, cannot be requested by a furnisher—such as the employment context. Similar issues abound in relation to 1702(b), (c), (d), and (e), as these areas are either already expressly regulated by the FCRA or outside of the CRAs area of expertise. In short, as drafted SB26-189 seems to require CRAs to provide blanket disclosures that could be confusing to users, if not contrary to the FCRA.

As it relates to deployer obligations, the FCRA already requires and prescribes the timing and much of the content of notices related to adverse outcomes based in whole or in part on information contained in a consumer report. Similarly, the process for both users of consumer reports and CRAs in relation to an adverse outcome or other consumer request related to the contents of their consumer report are tightly controlled by the FCRA.

However, the consumer notice required by SB26-189 cross-references 6-1-1306, the section of Colorado's comprehensive data privacy statute that establishes a variety of consumer rights related to their data. For CDIA members and users of consumer reports that do not meet the creditor exemption, this creates a challenge as consumer reports and the data streams that are used to create them are exempt, in their entirety, from the data privacy statute but still subject to the FCRA and other Colorado consumer reporting law. As a result, despite the intention to ensure consumers can access information in a similar manner to what exists under the FCRA, SB26-189 could lead to an absurd outcome where consumers receive duplicative and possibly conflicting notices.

One set of notices would be triggered by the FCRA, requiring action both by the user of the consumer report and the CRA that provided the report to the user. The disclosure requirements for users are set forth at 15 U.S.C. § 1681m and include obligations to inform the consumer of the adverse action, if a score was used, information related to that score and associated required information, the name and contact information of the CRA that provided the report (and explicit notice that the CRA did not make the decision), notice of the consumer's right to obtain a free copy of the their consumer report, and information regarding their right to dispute the accuracy or completeness of the report or any information furnished by the CRA.

If and when the consumer contacts the CRA after an adverse action, as is their right, the CRA must comply with the procedures set forth at 15 U.S.C. § 1681g. This requires providing the consumer the entirety of their file, the sources of the information, who requested a report in a certain

timeframe depending on the permissible purpose, and notice that the consumer may also request a score from the CRA, subject to additional requirements laid out in 15 U.S.C. § 1681(f).

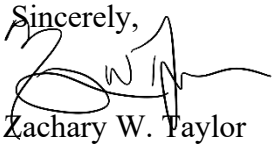
The second set of notices would be triggered by 6-1-1705 but could create the opposite impression, as consumers in Colorado do not have a right to request or correct information related to consumer reporting under 6-1-1306. That consumers do not have the right under the data privacy statute is not because they lack the right overall, but because the legislature previously determined that it would be best to let the FCRA govern FCRA activities, exempting consumer reports and the data streams used to create them from that statute. In relation to SB26-189, CDIA is simply requesting the state remain consistent in this view to ensure consumers receive clear, consistent, and actionable information from the users of consumer reports and CRAs in the event of an adverse outcome.

Given the ever-increasing interconnectedness of the modern economy, maintaining alignment between state consumer protection laws like SB26-189 and federal consumer reporting laws is more critical than ever. We appreciate the recognition of SB26-189 that the FCRA provides robust consumer protections and clear obligations for users of consumer reports and CRAs, particularly when a consumer report results in an adverse outcome for a consumer.

However, as the current structure of SB26-189 only deems "creditors" subject to and complying with the FCRA to meet the requirements of SB26-189, we believe there is a mismatch between the proposed law and the obligations of the FCRA that apply uniformly to all consumer reporting agencies and all users of consumer reports in all contexts for which a permissible purpose exists. To preserve the national, uniform standards that maintain a level playing field for the user of consumer reports and protect consumers coast to coast, CDIA respectfully requests the committee adopt amendments to SB26-189 that fully acknowledge the compliance obligations of the FCRA.

Thank you for your time and consideration.

Sincerely,



Zachary W. Taylor
Director, Government Relations
Consumer Data Industry Association

Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

May 5, 2026

Senator Jessie Danielson
Chair
Senate Business, Labor, & Technology Committee
Delaware House of Representatives
411 Legislative Ave.
Dover, DE 19901

Chair Danielson, Vice Chair Hinrichsen, and members of the committee:

On behalf of the Consumer Data Industry Association (CDIA), I write to request amendments to SB26-189 to better align the bill with the federal Fair Credit Reporting Act (FCRA) that governs consumer reporting agencies (CRAs), consumer reports, and the users of consumer reports, particularly in relation to adverse outcomes. While the current text of the bill acknowledges consumer notices and dispute processes under the FCRA for certain permissible purposes, those requirements apply to all allowed uses of consumer reports, not just in the credit context. It is our desire to see existing language expanded to ensure that Colorado's artificial intelligence law treats all consumer reporting agencies, consumers reports, and users of consumer reports equally in all contexts.

CDIA is the trade association representing consumer reporting agencies ("CRAs"), including the nationwide credit bureaus, regional and specialized credit bureaus, and background check and residential screening companies. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, thereby helping ensure fair and safe transactions for consumers and facilitating consumer's access to financial products and other services suited to their unique needs.

CDIA and its members appreciate the thoughtful and iterative process that led to SB26-189. While we were unable to participate formally as part of the working group, the revised structure of the bill represents an improvement over current law, with clearer definitions, clearer obligations for developers and deployers, and clear consumer rights that are familiar, in concept, to our industry. In particular, and as noted above, CDIA appreciates the current structure's recognition that many of the consumer rights SB26-189 intends to establish related to automated decision making technology are already established under and required by the FCRA for the consumer reporting system.

As the committee may know, our members, their products and their customers are all tightly regulated at the federal level by the FCRA. In addition, the FCRA establishes robust rights for consumers related to how consumer reports are accessed and used, particularly in relation to consequential decisions. This includes the right to know who has requested a report, to know who is furnishing information appearing on a report, to dispute the completeness or accuracy of the report, and to know when information in the report led to an adverse outcome. Colorado has

previously incorporated much of the FCRA into state statute with similar Attorney General-driven enforcement, providing an additional layer of protection to consumers.
While CDIA recognizes that the concepts underpinning SB26-189 are in some way analogous to the existing regulations on the consumer reporting system, there are sufficient differences between the requirements of the FCRA and SB26-189 to justify expanding the existing compliance exemption.

For example, 6-1-1702(a) requires developers (CRAs) to provide deployers (Users) to provide a "general statement describing the intended uses and known or harmful inappropriate uses". However, the FCRA, at 15 U.S.C. § 1681b enumerates a list of "permissible purposes" under which a CRA may furnish a report to a user. Without attesting to having a permissible purpose, a CRA cannot furnish a report to a user. There are also circumstances where a type of report, for example a credit score, cannot be requested by a furnisher—such as the employment context. Similar issues abound in relation to 1702(b), (c), (d), and (e), as these areas are either already expressly regulated by the FCRA or outside of the CRAs area of expertise. In short, as drafted SB26-189 seems to require CRAs to provide blanket disclosures that could be confusing to users, if not contrary to the FCRA.

As it relates to deployer obligations, the FCRA already requires and prescribes the timing and much of the content of notices related to adverse outcomes based in whole or in part on information contained in a consumer report. Similarly, the process for both users of consumer reports and CRAs in relation to an adverse outcome or other consumer request related to the contents of their consumer report are tightly controlled by the FCRA.

However, the consumer notice required by SB26-189 cross-references 6-1-1306, the section of Colorado's comprehensive data privacy statute that establishes a variety of consumer rights related to their data. For CDIA members and users of consumer reports that do not meet the creditor exemption, this creates a challenge as consumer reports and the data streams that are used to create them are exempt, in their entirety, from the data privacy statute but still subject to the FCRA and other Colorado consumer reporting law. As a result, despite the intention to ensure consumers can access information in a similar manner to what exists under the FCRA, SB26-189 could lead to an absurd outcome where consumers receive duplicative and possibly conflicting notices.

One set of notices would be triggered by the FCRA, requiring action both by the user of the consumer report and the CRA that provided the report to the user. The disclosure requirements for users are set forth at 15 U.S.C. § 1681m and include obligations to inform the consumer of the adverse action, if a score was used, information related to that score and associated required information, the name and contact information of the CRA that provided the report (and explicit notice that the CRA did not make the decision), notice of the consumer's right to obtain a free copy of the their consumer report, and information regarding their right to dispute the accuracy or completeness of the report or any information furnished by the CRA.

If and when the consumer contacts the CRA after an adverse action, as is their right, the CRA must comply with the procedures set forth at 15 U.S.C. § 1681g. This requires providing the consumer the entirety of their file, the sources of the information, who requested a report in a certain

timeframe depending on the permissible purpose, and notice that the consumer may also request a score from the CRA, subject to additional requirements laid out in 15 U.S.C. § 1681(f).

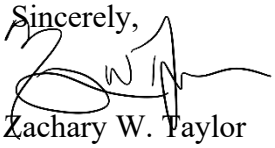
The second set of notices would be triggered by 6-1-1705 but could create the opposite impression, as consumers in Colorado do not have a right to request or correct information related to consumer reporting under 6-1-1306. That consumers do not have the right under the data privacy statute is not because they lack the right overall, but because the legislature previously determined that it would be best to let the FCRA govern FCRA activities, exempting consumer reports and the data streams used to create them from that statute. In relation to SB26-189, CDIA is simply requesting the state remain consistent in this view to ensure consumers receive clear, consistent, and actionable information from the users of consumer reports and CRAs in the event of an adverse outcome.

Given the ever-increasing interconnectedness of the modern economy, maintaining alignment between state consumer protection laws like SB26-189 and federal consumer reporting laws is more critical than ever. We appreciate the recognition of SB26-189 that the FCRA provides robust consumer protections and clear obligations for users of consumer reports and CRAs, particularly when a consumer report results in an adverse outcome for a consumer.

However, as the current structure of SB26-189 only deems "creditors" subject to and complying with the FCRA to meet the requirements of SB26-189, we believe there is a mismatch between the proposed law and the obligations of the FCRA that apply uniformly to all consumer reporting agencies and all users of consumer reports in all contexts for which a permissible purpose exists. To preserve the national, uniform standards that maintain a level playing field for the user of consumer reports and protect consumers coast to coast, CDIA respectfully requests the committee adopt amendments to SB26-189 that fully acknowledge the compliance obligations of the FCRA.

Thank you for your time and consideration.

Sincerely,



Zachary W. Taylor
Director, Government Relations
Consumer Data Industry Association

Consumer Data Industry Association
1090 Vermont Ave., NW, Suite 200
Washington, D.C. 20005-4905

P 202 371 0910

CDIAONLINE.ORG

May 5, 2026

Senator Jessie Danielson
Chair
Senate Business, Labor, & Technology Committee
Colorado House of Representatives
200 E Colfax Avenue
Denver, CO 80203

Chair Danielson, Vice Chair Hinrichsen, and members of the committee:

On behalf of the Consumer Data Industry Association (CDIA), I write to request amendments to SB26-189 to better align the bill with the federal Fair Credit Reporting Act (FCRA) that governs consumer reporting agencies (CRAs), consumer reports, and the users of consumer reports, particularly in relation to adverse outcomes. While the current text of the bill acknowledges consumer notices and dispute processes under the FCRA for certain permissible purposes, those requirements apply to all allowed uses of consumer reports, not just in the credit context. It is our desire to see existing language expanded to ensure that Colorado's artificial intelligence law treats all consumer reporting agencies, consumers reports, and users of consumer reports equally in all contexts.

CDIA is the trade association representing consumer reporting agencies ("CRAs"), including the nationwide credit bureaus, regional and specialized credit bureaus, and background check and residential screening companies. Founded in 1906, CDIA promotes the responsible use of consumer data to help consumers achieve their financial goals and to help businesses, governments, and volunteer organizations avoid fraud and manage risk. Through data and analytics, CDIA members empower economic opportunity, thereby helping ensure fair and safe transactions for consumers and facilitating consumer's access to financial products and other services suited to their unique needs.

CDIA and its members appreciate the thoughtful and iterative process that led to SB26-189. While we were unable to participate formally as part of the working group, the revised structure of the bill represents an improvement over current law, with clearer definitions, clearer obligations for developers and deployers, and clear consumer rights that are familiar, in concept, to our industry. In particular, and as noted above, CDIA appreciates the current structure's recognition that many of the consumer rights SB26-189 intends to establish related to automated decision making technology are already established under and required by the FCRA for the consumer reporting system.

As the committee may know, our members, their products and their customers are all tightly regulated at the federal level by the FCRA. In addition, the FCRA establishes robust rights for consumers related to how consumer reports are accessed and used, particularly in relation to consequential decisions. This includes the right to know who has requested a report, to know who is furnishing information appearing on a report, to dispute the completeness or accuracy of the report, and to know when information in the report led to an adverse outcome. Colorado has

previously incorporated much of the FCRA into state statute with similar Attorney General-driven enforcement, providing an additional layer of protection to consumers.
While CDIA recognizes that the concepts underpinning SB26-189 are in some way analogous to the existing regulations on the consumer reporting system, there are sufficient differences between the requirements of the FCRA and SB26-189 to justify expanding the existing compliance exemption.

For example, 6-1-1702(a) requires developers (CRAs) to provide deployers (Users) to provide a "general statement describing the intended uses and known or harmful inappropriate uses". However, the FCRA, at 15 U.S.C. § 1681b enumerates a list of "permissible purposes" under which a CRA may furnish a report to a user. Without attesting to having a permissible purpose, a CRA cannot furnish a report to a user. There are also circumstances where a type of report, for example a credit score, cannot be requested by a furnisher—such as the employment context. Similar issues abound in relation to 1702(b), (c), (d), and (e), as these areas are either already expressly regulated by the FCRA or outside of the CRAs area of expertise. In short, as drafted SB26-189 seems to require CRAs to provide blanket disclosures that could be confusing to users, if not contrary to the FCRA.

As it relates to deployer obligations, the FCRA already requires and prescribes the timing and much of the content of notices related to adverse outcomes based in whole or in part on information contained in a consumer report. Similarly, the process for both users of consumer reports and CRAs in relation to an adverse outcome or other consumer request related to the contents of their consumer report are tightly controlled by the FCRA.

However, the consumer notice required by SB26-189 cross-references 6-1-1306, the section of Colorado's comprehensive data privacy statute that establishes a variety of consumer rights related to their data. For CDIA members and users of consumer reports that do not meet the creditor exemption, this creates a challenge as consumer reports and the data streams that are used to create them are exempt, in their entirety, from the data privacy statute but still subject to the FCRA and other Colorado consumer reporting law. As a result, despite the intention to ensure consumers can access information in a similar manner to what exists under the FCRA, SB26-189 could lead to an absurd outcome where consumers receive duplicative and possibly conflicting notices.

One set of notices would be triggered by the FCRA, requiring action both by the user of the consumer report and the CRA that provided the report to the user. The disclosure requirements for users are set forth at 15 U.S.C. § 1681m and include obligations to inform the consumer of the adverse action, if a score was used, information related to that score and associated required information, the name and contact information of the CRA that provided the report (and explicit notice that the CRA did not make the decision), notice of the consumer's right to obtain a free copy of the their consumer report, and information regarding their right to dispute the accuracy or completeness of the report or any information furnished by the CRA.

If and when the consumer contacts the CRA after an adverse action, as is their right, the CRA must comply with the procedures set forth at 15 U.S.C. § 1681g. This requires providing the consumer the entirety of their file, the sources of the information, who requested a report in a certain

timeframe depending on the permissible purpose, and notice that the consumer may also request a score from the CRA, subject to additional requirements laid out in 15 U.S.C. § 1681(f).

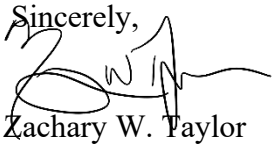
The second set of notices would be triggered by 6-1-1705 but could create the opposite impression, as consumers in Colorado do not have a right to request or correct information related to consumer reporting under 6-1-1306. That consumers do not have the right under the data privacy statute is not because they lack the right overall, but because the legislature previously determined that it would be best to let the FCRA govern FCRA activities, exempting consumer reports and the data streams used to create them from that statute. In relation to SB26-189, CDIA is simply requesting the state remain consistent in this view to ensure consumers receive clear, consistent, and actionable information from the users of consumer reports and CRAs in the event of an adverse outcome.

Given the ever-increasing interconnectedness of the modern economy, maintaining alignment between state consumer protection laws like SB26-189 and federal consumer reporting laws is more critical than ever. We appreciate the recognition of SB26-189 that the FCRA provides robust consumer protections and clear obligations for users of consumer reports and CRAs, particularly when a consumer report results in an adverse outcome for a consumer.

However, as the current structure of SB26-189 only deems "creditors" subject to and complying with the FCRA to meet the requirements of SB26-189, we believe there is a mismatch between the proposed law and the obligations of the FCRA that apply uniformly to all consumer reporting agencies and all users of consumer reports in all contexts for which a permissible purpose exists. To preserve the national, uniform standards that maintain a level playing field for the user of consumer reports and protect consumers coast to coast, CDIA respectfully requests the committee adopt amendments to SB26-189 that fully acknowledge the compliance obligations of the FCRA.

Thank you for your time and consideration.

Sincerely,



Zachary W. Taylor
Director, Government Relations
Consumer Data Industry Association

May 5, 2026

The Honorable Jessie Danielson
Chair, Senate Business, Labor, & Technology Committee
Colorado General Assembly
200 E. Colfax Avenue
Denver, CO 80203

RE: SB 26-189, Automated Decision-Making Technology in Consequential Decisions

Dear Chair Danielson:

On behalf of the American Innovators Network (AIN), I write to share implementation concerns regarding SB 26-189, legislation concerning automated decision-making technology (ADMT) in consequential decisions. AIN represents early-stage artificial intelligence startups and developers, part of the broader technology community we call “Little Tech.” These are small, high-growth companies building responsible tools across education, healthcare, workforce development, small-business services, and other sectors where innovation can expand opportunity.

AIN recognizes that SB 26-189 reflects meaningful progress from SB 24-205. The bill moves Colorado toward a more targeted framework, and we appreciate the effort to distinguish covered uses from lower-risk administrative, informational, and routine applications. We share the bill’s consumer-protection goals: consumers should have meaningful information about automated tools.

The question is how to make that framework workable for startups trying to build responsibly. Little Tech companies often operate with limited legal, compliance, and administrative capacity. They may have a small engineering team, a promising product, and a desire to comply, but not the infrastructure of a large enterprise. For those companies, the details of implementation will determine whether this bill creates clear rules of the road or a compliance structure only the largest companies can absorb.

Our core concern is the potential to impose burdens on startups that could make it harder for them to compete with Big Tech, which would increase concentration in AI markets. SB 26-189 establishes a layered regime of developer documentation, deployer notices, post-adverse-outcome disclosures, consumer-rights processes, and three-year record retention. These obligations may be manageable for large enterprises with dedicated compliance teams. They are significantly harder for a startup with a handful of employees and no in-house legal department. AIN is not suggesting that small firms should be exempt from responsible practices. We are urging that compliance expectations be scaled, practical, and tied to the company’s size, role, and control over the final decision. Consumer transparency should be useful and understandable, not so paperwork-heavy that smaller developers are effectively pushed out of consequential-decision markets.

In addition, accountability should follow control. In many consequential-decision settings, the deployer controls the final decision, the data, the workflow, the notice, and the appeal process. Upstream startups, general-purpose AI providers, and infrastructure developers often do not. The law should reflect that difference.

Additionally, the legislative record should be clear that ADMT is not unlawful in itself. Part 17 says it creates no new private right of action, but it also treats violations as deceptive trade practices and sets up a separate framework for allocating fault in discrimination claims involving ADMT. Those are new mechanisms built around a new category of technology. As implementation moves forward, it should not create the impression that building, selling, or using ADMT is enough on its own to trigger liability. A startup should not face liability simply because its technology appeared somewhere in a consequential-decision workflow, especially where the startup did not intend, market, configure, or contract for that use. Liability should turn on an independently established violation of existing law, such as the Colorado Anti-Discrimination Act, and a party's actual role in causing it. Implementation should also preserve ordinary commercial risk allocation for claims arising from a counterparty's misuse, unauthorized modification, failure to follow documented use limits, or conduct outside the developer's intended use.

Finally, rulemaking will matter enormously. SB 26-189 delegates important compliance details to the Attorney General, including post-adverse-outcome disclosures, consumer-rights processes, and the application of "materially influence." For startups, broad rulemaking is itself a source of uncertainty because companies cannot responsibly finalize disclosure workflows, update contracts, or train staff until the rules are known. The bill's notice-and-cure provision is an important backstop during this period. It allows good-faith companies to correct technical compliance gaps before facing enforcement, while preserving the Attorney General's authority to act immediately against knowing or repeated violations. AIN is concerned that the 2030 sunset on the cure provision would remove that backstop while the regulatory landscape is still developing.

As this process proceeds, AIN urges the legislature, and the Attorney General to preserve clarity for general-purpose APIs, models, and infrastructure tools. The interaction between the bill's developer definition, component coverage, and actual-knowledge limitation will matter significantly for upstream providers.

Colorado can protect consumers and still leave room for responsible startups to build here. AIN welcomes continued engagement with the Committee and the Attorney General's office to help ensure SB 26-189 is implemented in a way that protects consumers, supports responsible innovation, and remains workable for Little Tech.

Sincerely,

Jeremy Kudon
Executive Director
American Innovators Network

American Innovators Network (AIN) Testimony
Senate Business, Labor, & Technology Committee

Tuesday, May 5th

Chair Danielson, members of the Committee, thank you for the opportunity to testify.

My name is Cameron Onumah, and I am here on behalf of the American Innovators Network, or AIN. AIN represents early-stage AI startups and developers, part of the broader technology community we call Little Tech.

These are small, high-growth companies building responsible tools for teachers, patients, workers, small businesses, and community institutions. They are often the companies most likely to build for underserved communities, because the large incumbents are not building for rural school districts, community health centers, or Main Street businesses. These companies want to build responsibly, and they want clear rules they can actually follow.

We recognize that SB 26-189 reflects meaningful progress from SB 24-205. It moves Colorado toward a more targeted framework focused on automated decision-making technology that materially influences consequential decisions. We share the bill's consumer-protection goals. Consumers should have transparency, correction rights, and meaningful review when automated tools affect important opportunities.

Our concern is implementation.

For Little Tech, the details will determine whether this bill creates clear rules of the road or a compliance structure only the largest companies can absorb. Our core principle is simple: accountability should follow control.

In many consequential-decision settings, the deployer controls the final decision, the data, the workflow, the notice, and the appeal process. An upstream startup providing a general-purpose model, API, or infrastructure tool often does not. The law should reflect that difference.

SB 26-189 creates a layered framework of developer documentation, deployer notices, post-adverse-outcome disclosures, consumer-rights processes, and three-year record retention. Large enterprises with dedicated compliance teams may be able to absorb that. A startup with a handful of employees and no in-house legal department may not.

Consider what that means in practice. A five-person startup building a resume-screening tool for small employers would need to produce developer documentation,

track deployer compliance, build a consumer-rights response process, maintain three years of records, and monitor for material updates, all before generating meaningful revenue. That is the same compliance architecture required of a company with hundreds of lawyers and a dedicated policy team.

We are not suggesting that small firms should be exempt from responsible practices. We are urging that compliance expectations be scaled, practical, and tied to a company's size, role, and control over the final decision.

We also believe the legislative record should be clear that ADMT is not unlawful in itself. Part 17 says it creates no new private right of action. But it also treats violations as deceptive trade practices and sets up a separate framework for allocating fault in discrimination claims. Those are new legal mechanisms built around a new category of technology. The concern is that a startup could face liability not because it violated antidiscrimination law, but because its tool was used downstream in a workflow that someone else controlled and that someone else used in a way the startup never intended, marketed, configured, or contracted for. Liability should turn on an independently established violation of existing law and a party's actual role in causing it.

Finally, rulemaking will matter enormously. A startup deciding today whether to enter the Colorado market cannot answer basic operational questions: what disclosures will be required, what format they need to take, what "materially influence" will mean in practice. Those answers will come through rulemaking that has not yet begun. The bill's notice-and-cure provision is an important backstop while that landscape develops. It gives good-faith companies room to correct technical compliance gaps before facing enforcement, while preserving the Attorney General's authority to act immediately against knowing or repeated violations. We are concerned that the 2030 sunset would remove that protection too soon.

Colorado can protect consumers and still leave room for responsible startups to build here. AIN looks forward to continued engagement with the Committee and the Attorney General's office to help ensure SB 26-189 is implemented in a way that protects consumers, supports responsible innovation, and remains workable for Little Tech.

Thank you.

April 29th, 2026
Senator Robert Rodriguez
Room 346, Colorado State Capitol, 200 East Colfax Avenue,
Denver, CO 80203

RE: PBSA Considerations for Revised Act Concerning the Use of Automated Decision-Making Technology in Consequential Decisions

Dear Majority Leader Rodriguez,

On behalf of the Professional Background Screening Association (PBSA), we appreciate the opportunity to share our perspective on the latest bill draft concerning automated decision-making systems, and related regulatory frameworks. PBSA represents more than 700 companies, ranging from small businesses to global enterprises, dedicated to providing safe workplaces, homes, and volunteer environments through compliant background screening.

As you work to improve upon Colorado's existing law in this rapidly evolving space, we respectfully submit the following recommendations to help strike a balanced, innovation-forward approach that protects consumers, preserves privacy, and ensures practical implementation for those who rely on background screening tools.

First, we note that, in section 6-1-1701, the definition of "deployer" uses the undefined term "deploy." We propose to define "deployer" in a manner that does not use the word "deploy" and that we believe to be *consistent with the drafters' intent*, which focuses on materially influencing consequential decisions. Our one addition that deserves highlighting is that we propose to say that a person is a deployer as to the person's "own" consequential decisions. We intend that to eliminate the ambiguity of who is a deployer for a decision in which multiple persons participate, but that only one actually executes. For example, where an employer and its service provider are involved in an employment decision, the employer is the deployer. Similarly, where a creditor and its service provider are involved in a decision, the creditor is the deployer.

> "Deployer" means a person doing business in Colorado that uses the output of a covered ADMT in a manner that materially influences the person's own consequential decision about a consumer ~~deploys a covered ADMT~~.

Alternatively, one could achieve the same outcome by defining the word "deploy:

> "Deploys a covered ADMT" means use the output of a covered ADMT in a manner that materially influences the person's own consequential decision about a consumer.

Second, also in section 6-1-1701, we propose a carve-out to the definition of "materially influences" to promote facial transparency about the operation of ADMT. We expect that, in many situations, the operator of the ADMT (whether that is a developer or a deployer) would have the ADMT produce its outputs *along with its inputs*. This allows a human actually making the decision to readily see if the ADMT is doing what it ought and to substitute human judgment for the ADMT's output at the time of

making the decision. This would be beneficial generally and strictly superior to substituting human judgment for ADMT output later, through a human review. While it may be impractical in some circumstances, the statute should reward ADMT that is this transparent.

We also note that the "materially influences" standard is central to determining the scope of the statute. Because this standard will ultimately drive when obligations apply, additional clarity through rulemaking or illustrative examples would be helpful. In particular, guidance on how to evaluate material influence in multi-factor decision environments would support consistent interpretation and reduce uncertainty for both developers and deployers.

> "Materially influences" means the ADMT output:
>
> (a) is a non-de minimis factor that is used in making a consequential decision; and
>
> (b) affects the outcome of the decision, including by constraining, ranking, scoring, recommending, classifying, or otherwise meaningfully altering how the decision is made.
>
> Materially influences does not include incidental, trivial or clerical uses. Materially influences does not include the use of an ADMT's output in any consequential decision if (1) an individual or group is making the consequential decision, (2) the individual or group is presented with the inputs to the ADMT that are relevant to the consequential decision at the same time and in the same context as the output from the ADMT, and (3) the individual or group has the ability to ignore the output of the ADMT.

Third, in section 6-1-1704(3), we propose two changes to how a post-adverse notice would work:

- The current language requires a post-adverse notice when the ADMT *did not actually have anything to do with the adverse decision*. All that is required is that the ADMT was used in the decision and the decision was adverse. For example, in a background check, a consumer reporting agency might verify prior employment and conduct a criminal history check. The employer should not have to send a post-adverse notice if the criminal history was the only adverse information but the employment history was the only part that used ADMT. More generally, this provision ought to require a notice only when the ADMT *materially influenced the decision so that it became adverse*. Therefore, our first proposed change tightens the connection to require that the material influence results in the adverse decision.

- On the timing of the notice, the current language is ambiguous on whether the deployer could provide notice *before* the decision. We acknowledge that, in many circumstances, advanced notice is impossible. But in others (especially employment), there are already advance notice processes around adverse decisions. The language should not *prohibit* deployers from inserting the required post-adverse notice earlier into those processes.

> (3) If a deployer uses a covered ADMT to materially influence a consequential decision which results in an adverse outcome for a consumer, the deployer shall provide, no later than ~~within~~ thirty calendar days after making the consequential decision:

Additionally, within the provisions identifying the contents of the post-adverse notice, we suggest three clarifications.

- In clause (a), we suggest that the plain description could include the role that *the output from the ADMT* had (rather than the role that *the ADMT* had), because this will very frequently be

easier for the individual to understand and because the use of the ADMT itself was less relevant than its output.

(a) A plain-language description of the consequential decision and the role the covered ADMT or its output played in the decision;

- In clause (b), we propose to eliminate an ambiguity. In the current draft the term "the inputs" could mean either of two things: the inputs to the *consequential decision* or the inputs to the *ADMT*. We think that the drafters' intent was to require disclosure of the inputs to the ADMT, not to the consequential decision. (b) Instructions and a simple to follow process to request additional information about the ADMT and the inputs to the ADMT relevant to the adverse outcome, including the name of the ADMT, the ADMT version number if applicable, the ADMT developer and the types, categories, and sources of personal data used, to the extent reasonably known to the deployer and/or provided by the developer;

- In clause (c), we note that the Colorado Privacy Laws may not always apply, especially where federal or other state laws are in play. We therefore propose to allow a deployer governed by one of those other laws to identify the relevant process for correction under those other laws. (c) Information on how to request personal data under the Colorado Privacy Laws or other applicable law and how to correct materially inaccurate personal data consistent with section 6-1-1306 or other applicable law; and

In section 6-1-1704(6), we note that the draft covers a specific case where the impact of a federal law requires notices that the post-adverse notice could usefully be combined with. Subsection (6) provides that creditors can combine their ECOA and FCRA-based notices with the post-adverse notices. But subsection (6) is narrow. Other persons, including employers subject to the FCRA are in a similar position but are not covered by this provision. We believe that it would be appropriate to make this general, subject to the same constraints as in subsection (6).

More broadly, we encourage continued consideration of how these requirements will operate alongside existing federal and state employment law frameworks, including the Fair Credit Reporting Act and related adverse action processes. In many cases, deployers will already be operating within established notice, dispute, and review structures. Aligning this statute with those frameworks, where appropriate, will promote clarity for consumers and reduce duplicative or potentially conflicting obligations.

(7) A person that any federal or state law requires to provide a notice, explanation, or disclosure to a consumer about a consequential decision that has, will have, or might have an adverse outcome for that consumer may combine into that notice, explanation, or disclosure the notice that this section requires about a consequential decision that results in an adverse outcome for the consumer, so long as the combined notice, explanation, or disclosure includes all of the information that this section requires.

In section 6-1-1705, we propose to harmonize the requirement that a consumer can get incorrect information corrected with the Fair Credit Reporting Act's comparable provision, to the extent that it applies. The FCRA's dispute re-investigation provisions are longstanding, extensive, and supported by case law. The FCRA provides an existing private right of action that consumers do actually use. Creating a carve-out for those disputes will help prevent consumer confusion and reduce the risk of overlapping or conflicting processes.

This subsection does not apply to any information in a consumer report for which the consumer may require a re-investigation under the federal Fair Credit Reporting Act.

We also note that, in many consequential decision contexts, deployers rely on third-party providers for components of the decision-making process. As a result, the ability of a deployer to satisfy certain disclosure and documentation requirements may depend on information provided by developers. Continued clarity around the respective roles of developers and deployers will help ensure that obligations are aligned with the practical realities of how these systems are implemented.

Finally, we note that the draft introduces a more structured framework for allocating responsibility between developers and deployers, as well as provisions addressing contractual allocation of risk. Given the importance of these provisions, additional clarity regarding how responsibility is assigned in vendor-supported decision-making environments and how contractual limitations are intended to operate would be helpful to support consistent implementation.

We also recognize that several aspects of the draft appropriately rely on rulemaking for further clarification. Continued stakeholder engagement in that process will be important to ensure that implementing rules reflect operational realities across affected industries.

We believe that all of these proposed changes are highly aligned to the intent of the bill. If you read them any differently, please know that this is not our intent. If that happens, we would appreciate it if you would contact us and allow us to better explain our proposal.

PBSA and its members are eager to support thoughtful AI regulation that balances fairness, transparency, and innovation. We are available to participate in stakeholder sessions, contribute to rulemaking, and share operational insights from the background screening profession to help ensure that laws are clear, practical, and implementable.

Sincerely,
Rory Bogdon
PBSA State and Local Government Relations Director

PBSA
PROFESSIONAL BACKGROUND SCREENING ASSOCIATION