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

P 202 371 0910

Writer's direct dial: +1 (202) 408-7407

CDIAONLINE.ORG

March 27, 2023

Via Electronic Delivery to
regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Kevin Sabo
2101 Arena Blvd.
Sacramento, CA 95834

RE: Invitation for Preliminary Comments on Proposed Rulemaking on Cybersecurity Audits, Risk Assessments, and Automated Decisionmaking (PR 02-2023)

To whom it may concern:

The Consumer Data Industry Association submits this comment letter in response to the invitation of the California Privacy Protection Agency ("CPPA"). In this invitation, the CPPA seeks input on proposed rulemaking under the California Privacy Rights Act ("CPRA") relating to cybersecurity audits, risk assessments, and automated decision-making.[1]

CDIA strongly urges the CPPA to limit cybersecurity audit and risk assessment requirements to processing that presents significant consumer risk and to craft requirements that are flexible and permit businesses to appropriately identify and address their unique risks. CDIA also urges the CPPA to clarify that their requirements will apply directly only to CCPA businesses so that businesses can address particular risks with their service providers by contract within the context of the business' data processing activities. Finally, CDIA urges the CPPA to clarify that consumer rights other business requirements related to automated decision-making do not apply to personal information processed for security and integrity activities.

CDIA members have been complying with laws and regulations governing the consumer reporting industry for decades. Members have complied with the Fair Credit Reporting Act ("FCRA"), which is often viewed as the nation's first national consumer privacy law. The FCRA governs the collection, assembly, and use of consumer report information and provides the framework for the U.S. credit reporting system. The FCRA incorporate fair information principles, like access, notice, choice, consent, correctability, and accountability.

[1] The Consumer Data Industry Association ("CDIA") is the voice of the consumer reporting industry, representing consumer reporting agencies including the nationwide credit bureaus, regional and specialized credit bureaus, background check and residential screening companies, and others. 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 all over the world, helping ensurefair and safe transactions for consumers, facilitating competition, and expanding consumers'access to financial and other products suited to their unique needs.

In particular, the FCRA outlines many consumer rights with respect to the use and accuracy of the information contained in consumer reports. Under the FCRA, consumer reports may be accessed only for permissible purposes, and a consumer has the right to dispute the accuracy of any information included in his or her consumer report with a consumer reporting agency ("CRA").

Our members are at the forefront of consumer privacy protection in ways that protect consumers and meet their expectations for fast, friction-free transactions. Fair, accurate, and permissioned use of consumer information is necessary for consumers and businesses to do business effectively. As we describe in greater detail below, CDIA members provide identity verification and fraud prevention services to their customers, and such services involve the processing of personal information. Identity verification and fraud services providers may offer their services to CCPA businesses as service providers.

To assist the agency in promulgating clear and effective regulations that allow businesses to best support customers and consumers, CDIA offers the following comments on the topics as presented in the Invitation for Preliminary Comments:

I. Cybersecurity Audits and Risk Assessments

The Invitation for Preliminary Comments raises questions related to existing laws that require cybersecurity audits and risk assessments. The Invitation also poses the following questions:

5. What else should the Agency consider to define the scope of cybersecurity audits?

First and foremost, CDIA encourages the CPPA to limit the scope of required cybersecurity audits to personal information processing that presents significant risk to consumer privacy or security. The CPRA authorizes the CPPA to issue regulations requiring cybersecurity audits for the processing of personal information *that presents significant risk to consumers' privacy or security*. Cal. Civ. Code § 1798.185(a)(15)(A). Because of this qualifier, it is clear that not all personal information processing would present significant consumer risk to privacy or security, so the CPPA should consistently limit any regulatory requirements.

Additionally, CDIA urges the CPPA to establish cybersecurity standards that are flexible and permit businesses to implement cybersecurity audit procedures specific to the risks present with their businesses,' systems, and data. This includes permitting businesses to undertake such audit efforts internally rather than through a third party, which could still ensure independence in audit functions while mitigating any additional privacy and security risks caused by a third-party audit-related disclosures.

Further, CDIA urges the CPPA to clarify that the CPRA's cybersecurity audit

requirements apply directly to CPPA businesses and only by service provider agreement to service providers. This flexibility will allow businesses to both protect consumers and better meet their needs. Among other products and services, CDIA members provide fraud, identity theft, and security incident detection and prevention services to clients. Such providers may offer these services as service providers under the CCPA, acting at the direction of and for the benefit of their clients that may be businesses directly subject to the CCPA.

Civil Code, § 1798.140(ag)(1)(D) of the CPRA contemplates business oversight of their service providers with regard to assessments, audits, and other technical and operational testing. CDIA members are acutely aware of the need for businesses to develop and implement cybersecurity protections tailored to the nature of their business, data, and systems. Especially where service provider services are related to the business' cybersecurity, businesses need to be empowered to set the standards, including audit requirements, that apply to their businesses.

Accordingly, CDIA believes that the CPPA should set standards for cybersecurity audits that are flexible and allow businesses to make decisions based on identifying specific risks to their business, systems, and data, and those businesses, instead of the CPPA, should set the oversight appropriate to their service providers. CDIA urges the CPPA to clarify that the audit requirements apply directly only to businesses as defined by the CCPA and to processing that presents significant privacy and security risks.

Finally, CDIA recommends aligning any proposed cybersecurity standards with existing and well-established industry standards and risk assessment models utilized broadly. Any new standards implemented should permit the continued use of these models. Examples include ISO 27001 and ISO 27002 and NIST.

II. Risk Assessments

The Invitation for Preliminary Comments poses questions related to existing laws requiring data processing risk assessments and further asks:

8. What else should the Agency consider in drafting its regulations for risk assessments?

First and foremost, CDIA encourages the CPPA to limit the scope of required risk assessments to personal information processing that presents significant risk to consumer privacy or security. The CPRA authorizes the CPPA to issue regulations requiring risk assessments with respect to the processing of personal information ersonal information *that presents significant risk to consumers' privacy or security*. Cal. Civ. Code § 1798.185(a)(15)(A). Because of this qualifier, it is clear that not all personal information processing would present significant consumer risk to privacy or security, so the CPPA should consistently limit any regulatory requirements.

Further, like with cybersecurity audits discussed above, CDIA urges the CPPA to establish risk assessment requirements that are flexible so that businesses can identify and mitigate risks appropriately and efficiently based on the nature of the business, its systems, and its data. CDIA also urges the CPPA to clarify that the risk assessment requirements apply to businesses directly, not their service providers.

Just as data processing activities vary across different businesses, data processing risks to consumers, the business, and the public at large differ as well. As a result of these differences, the procedures needed to assess changing risks specific to the business's particular data processing activities may need to vary as well, and any need for service providers to participate should flow down to service providers rather than applying independently. Risks associated with data processing by a service provider, like a CDIA member, need be assessed within the context of the business's data processing, and it would not be effective to merely attempt to identify processing risks in a vacuum for a particular service provider.

III. Automated Decision-making

The Invitation for Preliminary Comments poses the following question:

> *4. How have businesses or organizations been using automated decisionmaking technologies, including algorithms? In what contexts are they deploying them? Please provide specific examples, studies, cases, data, or other evidence of such uses when responding to this question, if possible.*

CDIA members provide a wide range of products and services that involve the automated processing of personal information, like identify verification and fraud detection services. Fraud prevention and detection services may provide information on known fraudsters and fraud strategies and identify potential fraud risks based on comparing applicant-supplied data with data available from third-party sources. Subscribers of these types of services use the information provided to mitigate against fraud loss. Businesses regularly need to engage in identity verification and fraud detection efforts, in some circumstances by law or collective standard but otherwise to reduce risk of harm to the business and to consumers. By preventing fraud and identity theft on consumers, such efforts further consumer privacy.

The proposal should not include identity theft and fraud detection services in the term "automated decisionmaking technologies." Identity theft and fraud detection products and services are meant to confirm identity or identify fraud or other related risks in a proposed transaction; they are not meant to make a decision as to whether an individual is eligible for a particular product or service. Thus, it does not appear that the term "automated decisionmaking technologies" describes identity verification and fraud detection efforts.

Further, Civil Code, § 1798.140(z) defines the term "profiling" as automated processing "to evaluate certain aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, behavior, location or movements." Efforts to detect fraud and verify identity are distinct from "profiling" activities because such efforts attempt to confirm what a consumer told the business and otherwise detect fraudulent activities in order to reduce risk.

The Invitation also asks:

> *8. Should access and opt-out rights with respect to businesses' use of automated decisionmaking technology, including profiling, vary depending upon certain factors (e.g., the industry that is using the technology; the technology being used; the type of consumer to whom the technology is being applied; the sensitivity of the personal information being used; and the situation in which the decision is being made, including from the consumer's perspective)? Why, or why not? If they should vary, how so?*

Even though identity theft and fraud detection services should not be considered "profiling" or otherwise an "automated decisionmaking technology," CDIA encourages the CPPA to expressly exempt personal information processing for these purposes, "security and integrity" activities under the CPRA, from any access, opt-out, or other rights or requirements.

Civil Code, § 1798.140(ac) defines "security and integrity" to include activities related to detecting security incidents, detecting fraud or other illegal action, and verifying identity. Unlike other comprehensive state data privacy laws, the CCPA does not have a broad exemption for personal information processed for fraud detection or similar purposes, but the CCPA text reflects the drafter's intent and desire to protect personal information processed for these purposes for consumer privacy purposes.

Civil Code, § 1798.120(d) provides that the right to delete does not apply to personal information reasonably necessary to be maintained to help ensure security and integrity. Civil Code, § 1798.130(a)(3)(B) provides that, for purposes of the right to know, "specific pieces of personal information" do not include "data generated to help ensure security or integrity or as prescribed by regulation." And Civil Code, § 1798.140(e)(2) includes "security and integrity" purposes as "business purposes" distinct from commercial purposes like selling personal information.

If the CPPA were to include "security and integrity" activities in its conception of automated decision-making such that consumers would have access and opt out rights, businesses would be impeded from appropriately engaging in fraud detection and identity theft efforts. Consumers intending to commit fraud could simply opt out of automated

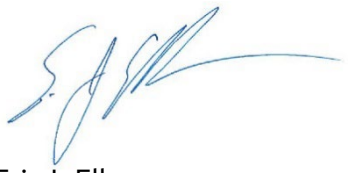
processing, and a business might not be able to prevent the intended fraud. Fraudsters could also exercise access requests in order to learn how such business detects fraud, which if shared, could prevent such business from appropriately detecting fraud not only for the consumer making such a request, but for consumers generally.

Accordingly, in light of the law's recognition of the importance of security and integrity activities and the current lack of clarity around the scope of "automated decisionmaking technologies" for a rule, CDIA urges the CPPA to clarify that personal information processed for "security or integrity" purposes is not subject to automated decision-making rights or requirements.

* * *

Thank you for the opportunity to share our views on the anticipated rulemaking under the CPRA. Please contact us if you have any questions or need further information based on comments.

Sincerely,



Eric J. Ellman
Senior Vice President, Public Policy & Legal Affairs