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

November 8, 2021

Via Electronic Delivery to regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

RE: Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act (PRO 01-21)

Dear Ms. Castanon,

The Consumer Data Industry Association submits this comment letter in response to the invitation of the California Privacy Protection Agency ("CPPA") for preliminary comments on proposed rulemaking under the California Privacy Rights Act ("CPRA").

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 ensure fair and safe transactions for consumers, facilitating competition, and expanding consumers' access to financial and other products suited to their unique needs.

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 has been called the original federal 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. 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").

CDIA members have been at the forefront of consumer privacy protection. Fair, accurate, and permissioned use of consumer information is necessary for any CDIA member client to do business effectively.

CDIA appreciates the CPPA's broad invitation to comment at the beginning of the rulemaking process. 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, including sensitive personal information. CDIA strongly urges the CPPA to ensure that consumer rights related to automated processing, correction, and notice at collection do not interfere with security and integrity activities, service providers and contractors are permitted to combine personal information obtained from multiple sources, and all businesses are permitted to engage in identity verification and fraud detection activities, including those required by law and collective standard. Finally, CDIA urges the CPPA to advocate for the repeal of employment and business to business communication exemption sunsets and issue a policy statement providing for the consistent interpretation of the CPRA with similar state laws.

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. Automated Decisionmaking

The Invitation for Preliminary Comments states, in part:

> *2. Automated Decisionmaking*
>
> *The CPRA provides for regulations governing consumers' "access and opt-out rights with respect to businesses' use of automated decisionmaking technology." Civil Code, § 1798.185(a)(16).*
>
> *Comments on the following topics will assist the Agency in creating these regulations:*
>
> *a. What activities should be deemed to constitute "automated decisionmaking technology" and/or "profiling." Civil Code, §§ 1798.185(a)(16) and 1798.140(z).*

CDIA strongly urges the CPPA to exclude activities to ensure "security and integrity" from "automated decisionmaking" activities. "Security and integrity," as the CPRA defines that term, includes activities related to detecting security incidents, detecting fraud or other illegal action, and verifying identity.

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."

CDIA members provide a wide range of products and services related to identify verification and fraud detection. 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.

"Profiling" under the CPRA refers to particular methods of analyzing personal information to predict personal aspects, like work performance, financial status, preferences, and location. Efforts to detect fraud and verify identity are distinct from "profiling" activities because such efforts attempt to confirm what a consumer told the business in order to reduce risk, a "business purpose" under the CCPA and CPRA.

If the CPPA were to include "security and integrity" activities in its conception of automated processing 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, CDIA strongly urges the CPPA to exclude activities relating to "security and integrity" as defined by the CPRA from "profiling" or automated processing.

II. Consumer Right to Correct

The Invitation for Preliminary Comments states, in part:

> *4. Consumers' Right to Delete, Right to Correct, and Right to Know*
>
> *The CCPA gives consumers certain rights to manage their personal information held by businesses, including the right to request deletion of personal information; the right to know what personal information is being collected; the right to access that personal information; and the right to know what categories of personal information are being sold or shared, and to whom. See Civil Code, §§ 1798.105, 1798.110, 1798.115, and 1798.130. The CPRA amended the CCPA to add a new right: the right to request correction of inaccurate personal information. See Civil Code, §§ 1798.106 and 1798.130.*
>
> *The Attorney General has adopted regulations providing rules and procedures to facilitate the right to know and the right to delete. See Code Regs., tit. 11, §§ 999.308((c), 999.312–313, 999.314(e), 999.318, 999.323–326, and 999.330(c). The CPRA additionally provides for regulations that establish rules and procedures to facilitate the new right to correct. 2 See Civil Code, § 1798.185(a)(7).*

Comments on the following topics will assist the Agency in creating these regulations:

. . .

b. How often, and under what circumstances, a consumer may request a correction to their personal information. See Civil Code, ∬ 1798.185(a)(8).

. . .

d. When a business should be exempted from the obligation to take action on a request because responding to the request would be "impossible, or involve a disproportionate effort" or because the information that is the object of the request is accurate. Civil Code, ∬ 1798.185(a)(8)(A).

First, CDIA urges the CPPA to clarify by regulation that a consumer does not have a right to correct personal information processed by a business for "security and integrity" activities. The CPRA, at Civil Code, ∬ 1798.106(a), provides that consumers have the right to request correction of personal information maintained by a business, "taking in account the nature of the personal information and the purposes of the processing of personal information."

Businesses maintain personal information for "security and integrity" activities, either on their own or by way of a service provider, using such information to detect identity theft or other fraud instances by verifying personal information received by the business. If consumers are permitted to modify the personal information that a business uses to compare newly-received information against, fraudsters may easily be able to bypass checks and commit identity theft against a consumer or other fraud. Businesses need to be able to maintain personal information for such security and integrity activities without having to change that information. The Right to Delete, at Civil Code, ∬ 1798.105(d)(2), includes an exception to "[h]elp ensure security and integrity," and the Right to Correct needs an equivalent exception. CDIA urges the CPPA to clarify that the Right to Correct's provision for "taking account the nature of the personal information and the purposes of the processing of the personal information" includes denying a right to correct personal information maintained for "security and integrity" purposes.

Second, CDIA urges the CPPA to clarify that a business should be exempted from the obligation to take action on a request to correct where the personal information cannot be verified through official documentation. If a request cannot be verified through official documentation, like it could for a request to update an address or correct the spelling of a name, then responding to the request would be "impossible" and the business would not be able to confirm that the "object of the request is accurate." For example, a consumer should not have the right to "correct" a business' customer service notes, which might reflect an employee's understanding of a phone conversation between the employee and the consumer.

An employee might document that the consumer made a particular request and that, as a result, the business had a particular response to that request. A consumer being able to change such record would make it impossible for a business to keep accurate records of what it understood happened in a conversation with a consumer. Accordingly, CDIA urges the CPPA to clarify that absent the ability to verify the object of the correction request through official documentation, regardless of whether requesting such documentation is permissible or whether the business attempted to verify the information, the business should be exempted from the obligation to take action on the request.

III. Consumer Right to Limit the Use of Sensitive Personal Information

The Invitation for Preliminary Comments states, in part:

> *5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information*
>
> *The CCPA gives consumers the right to opt out of the sale of their personal information by covered businesses. See Civil Code, §§ 1798.120(a). In 2020, the Attorney General adopted regulations to implement consumers' right to opt out of the selling of their personal data under the CCPA. See Code Regs., tit. 11, §§ 999.306, 999.315, and 999.316. The CPRA now provides for additional rulemaking to update the CCPA rules on the right to opt-out of the sale of personal information, and to create rules to limit the use of sensitive personal information, and to account for other amendments. See Civil Code, §§ 1798.185(a)(4) and 1798.185(a)(19)–(20).*
>
> *Comments on the following topics will assist the Agency in creating these regulations:*
>
> *a. What rules and procedures should be established to allow consumers to limit businesses' use of their sensitive personal information. See Civil Code, § 1798.185(a)(4)(A).*

The CPRA, at Civil Code, § 1798.121(a), limits consumers' right to direct a business that collects sensitive personal information to limit its use of that information by expressly permitting businesses to help to ensure "security and integrity" and to perform services on behalf of the business, including verifying customer information. CDIA urges the CPPA not to place limitations on these permitted uses when it adopts regulations addressing how consumers may limit business' use of their sensitive personal information. In particular, CDIA urges the CPPA not to limit the CPRA's express authorization for businesses to engage in "security and integrity" activities and other business services.

When businesses and their service providers, including CDIA members, engage in efforts to detect fraud and verify identity, they may use elements of sensitive personal information, including social security numbers, other identification numbers, or financial

account numbers, in particular, comparing information provided by the consumer to information made available for verification and fraud detection efforts. Such efforts are critical for businesses to be able to prevent loss and protect consumer privacy.

If consumers were able to limit the use of sensitive personal information for "security and integrity" activities, like fraud detection, or other business services like verifying customer information, businesses would be less able to prevent identity theft and other fraud, and all consumers would suffer because of such increased fraud risks and the potential increase in cost of services resulting from greater losses. CDIA thus urges the CPPA not to limit the CPRA's express authorization for businesses to engage in "security and integrity" activities and other business services.

IV. Business Purposes for which Entities May Combine Personal Information and Use Personal Information on Own Behalf

The Invitation for Preliminary Comments states, in part:

> *8. Definitions and Categories*
>
> *The CCPA and CPRA provide for various regulations to create or update definitions of important terms and categories of information or activities covered by the statute.*
>
> *Comment on the following topics will assist the Agency in deciding whether and how to update or create these definitions and categories:*
>
> *. . .*
>
> *e. Further defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information that was obtained from different sources. See Civil Code, §§ 1798.185(a)(10).*

CDIA strongly urges the CPPA to deem that efforts to security "security and integrity" as that term is defined by the CPRA are a business purpose for which businesses, service providers, and contractors are permitted to combine consumers' personal information obtained from different sources.

CDIA members provide "security and integrity" services, like fraud detection and identity verification services, to their business customers and may do choose to do so under the CPRA's "service provider" or "contractor" models. In order to provide such services, fraud detection and identity verification providers often have a need to combine multiple sets of personal information collected from multiple sources. These vendors provide their services through various data processing methods, including by comparing inquiry data with data available elsewhere, by detecting anomalies in provided data, and by otherwise analyzing

multiple data sets, all with the goal of detecting—and thus preventing—identity theft, fraud, and other illegal actions on businesses. These efforts reduce business costs and protect consumers, whether such consumers are business customers or not, and thus further consumer privacy.

CCPA regulations currently permit service providers to retain, use, and disclose personal information obtained in the course of detecting data security incidents and protecting against fraudulent or illegal activity. See Cal. Code Regs. tit. 11, § 999.314(c)(4). Fraud detection and identity verification service providers need to be able to retain, use, and disclose personal information to provide their critical services and prevent fraud on businesses and on consumers. Without the ability to retain, use, and disclose personal information, such service providers would not be able to offer fraud detection and prevention services because such services necessarily involve verifying the accuracy of personal information provided to businesses. The CPPA should retain this express permission for service providers to use, retain, and disclose personal information in connection with security and integrity functions and expand it to apply to "contractors" under the CPRA.

The CPPA should also expressly include "security and integrity" activities within the business purposes for which businesses and their service providers and contractors may combine personal information obtained from multiple services. Service providers offering fraud detection and prevention services need to be able to combine, and thus compare, personal information obtained from multiple sources and on behalf of multiple business clients to be able to accurately verify personal information and prevent fraud. If fraud prevention services providers are not permitted to combine personal information from multiple sources, or if consumers are permitted to opt out of such processing, fraud prevention services providers will be unable to provide their critical services. By permitting service providers to combine personal information for "security and integrity" activities, businesses will be able to utilize commercial fraud detection and identity verification products and reduce the risk of identity theft and other fraud on both businesses and consumers.

V. Establishing Exceptions Necessary to Comply with State or Federal Law

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is tasked with updating existing regulations and adopting new regulations. See, e.g., Civil Code, § 1798.185.

Civil Code, § 1798.185(a)(3) instructs the:

> *Establishing [of] any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter.*

The goals of the CPRA and CCPA to protect and further consumer privacy emphasize the importance—and the *growing* importance—of fraud detection products. Fraud detection products protect not only businesses against fraud by criminals, but they also protect consumers from identity fraud. These products work by utilizing a large volume of data, and removing one consumer's data from the universe of available data would affect not only that consumer, but all consumers.

The CPRA authorizes the CPPA to establish exceptions necessary to comply with state or federal law as needed. Businesses of various sorts and sizes are required to engage in customer due diligence (CDD), know your customer (KYC), or other identity theft and fraud check expectations by law, regulation, guidance, or other collective standard. Businesses engage identity verification and fraud detection providers like CDIA members to comply with such requirements or expectations. In the context of such varied CDD, KYC, and other fraud detection requirements and expectations, CDIA strongly urges the CPPA to adopt an express exception to CCPA and CPRA requirements that provides that the law is not to be interpreted to prevent or limit a business' efforts to ensure "security and integrity" as the law defines those activities. Such a provision would assist in business' efforts to comply with law and other standards and would further consumer privacy by permitting businesses to engage in appropriate efforts, including through the use of commercial fraud detection services, to combat identity theft, protect consumer personal information, and ensure consumer privacy.

VI. Purpose Limitation Exception for "Security and Integrity" Activities

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is authorized to adopt additional regulations as necessary to further the purposes of the CCPA and CPRA. See, e.g., Civil Code, § 1798.185(b).

CDIA urges the CPPA to clarify that "security and integrity" activities are not purposes for which businesses are required to disclose to consumers under Civil Code, § 1798.100(a)(1) and (2), and that not disclosing such "security and integrity" purposes would not prevent a business from using personal information for such purposes, per Civil Code, § 1798.100(c).

As noted, many CDIA members provide critical fraud protection services. Disclosing the nature of those services any related data collection may compromise the success of such efforts where the disclosure would inform fraudsters as to the type of fraud and identity theft checks engaged in by a particular business. Furthermore, limitations on the ability of fraud detection providers to use crucial data, including in the absence of disclosure to the consumer, will also undermine these important services.

CDIA urges the CPPA to clarify that "security and integrity" activities are not purposes that businesses are required to disclose to consumers under Civil Code, § 1798.100(a)(1) and (2). Furthermore, CDIA urges the CPPA not to apply the purpose limitation requirements in § 1798.100(c) to data used for "security and integrity." Rather, data should be made available for

those purposes regardless of the notice provided at collection in order to maximize available information to protect against fraud and to avoid providing opportunities for fraudsters to avoid detection, uses that further consumer privacy.

VII. Repealing or Delaying the Enforcement of Employment Context and Business to Business Communications Exemptions Sunsets

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is authorized to adopt additional regulations as necessary to further the purposes of the CCPA and CPRA. See, e.g., Civil Code, § 1798.185(b).

The CPRA sunsets these exemptions on January 1, 2023, and businesses lack clear guidance as to how to extend rights to consumers with regard to personal information not processed in the context of providing products or services to those consumers while navigating other laws, like state employment laws. CDIA urges the CPPA to advocate to the legislature the repeal of these sunsets, but in the absence of such action, CDIA urges the CPPA to delay enforcement of the law with regard to personal information processed in these contexts. In the absence of a repeal of these sunsets or a delay in enforcement, we encourage the CPPA to carefully consider the extent to which CPRA rules will apply to personal information currently covered by these exemptions given competing privacy considerations, particularly the privacy of other employees who may be referenced in employee records.

VIII. Urging Uniformity with Similar State Laws

The Invitation for Comments also requests any additional comments in relation to the CPPA's initial rulemaking. The CPPA is authorized to adopt additional regulations as necessary to further the purposes of the CCPA and CPRA. See, e.g., Civil Code, § 1798.185(b).

CDIA urges the CPPA to adopt a policy statement by regulation that it will align its regulatory interpretations with provisions of similar state privacy and data protection laws, including the Virginia Consumer Data Privacy Act and the Colorado Privacy Act, wherever possible. The CPRA instructs the CPPA to cooperate with other similar state agencies to ensure consistent application of privacy protections. See Civil Code, § 1798.199.40(i). Accordingly, CDIA urges the CPPA to endeavor to interpret the CPRA consistently with the laws enforced by those other state agencies.

Businesses subject to these laws are facing an increasingly large and complex landscape of privacy laws relating to consumer data, and consumers across the nation will benefit from similar protections and rights. Accordingly, it would benefit consumers for the CPPA to interpret the CPRA consistently with such other laws. For example, CDIA encourages the CPPA to adopt consistent interpretations to what is considered "personal information" and "deidentified information," and CDIA urges consistent approaches to

interpreting provisions permitting businesses to engage in "security and integrity" activities without limitation. We also urge the CPPA to consider providing businesses right reasonable abilities to cure deficiencies in CPRA compliance, just as other state laws provide. Finally, CDIA urges the CPPA to work with other state agencies to ensure that businesses can provide consistent disclosures to residents of all states.

* * *

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