November 21, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Re: Comments on modified text of rules implementing the California Privacy Rights Act of 2020

Dear Mr. Soublet:

On behalf of the American Financial Services Association ("AFSA"),[1] thank you for the opportunity to provide comments on the California Privacy Protection Agency's ("Agency") November 3 modifications of proposed rulemaking to implement the California Privacy Rights Act of 2020 (CPRA). AFSA members share the state's goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access. We appreciate the Agency's consideration of our previous comments and look forward to further engagement throughout the rulemaking process.

Enforcement Delay

The CPRA required that finalized regulations be completed by July 1, 2022, to provide businesses with enough time to comply before January 1, 2023, when the CPRA becomes operative, and before enforcement begins six months later, on July 1, 2023. As we discussed in previous comments, the rulemaking timeframe leaves businesses with very little time, if any, to alter operational practices to comply with the law. We appreciate the Agency's recognition of these challenges through its inclusion of § 7301(b):

> As part of the Agency's decision to pursue investigations of possible or alleged violations of the CCPA, the Agency may consider all facts it determines to be relevant, including the amount of time between the effective date of the statutory or regulatory requirement(s) and the possible or alleged violation(s) of those requirements, and good faith efforts to comply with those requirements.

While we believe this section is a step in the right direction, we respectfully request stronger assurances that a company's good faith effort to comply with the regulations will be considered in enforcement decisions. Accordingly, we request that the rules be modified to instead read: "the Agency *must* consider all facts…"

[1] Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

Employee and B2B Data Exemption

The California Privacy Rights (CPRA) extends the CCPA's partial exemption of employee and business contact data until January 1, 2023. The expiration of the exemptions will create unintended consequences and compliance problems as employees, job applicants, employers and individuals serving other businesses in a service provider are left without further guidance and clarity regarding the interplay between the CPRA and employment laws. Most of the rights under the CPRA either are already addressed or do not make sense in the employment or B2B context, and neither the CPPA nor the California Attorney General has provided businesses with any guidance or draft regulations concerning the treatment of such data. We request that the Agency consider making the exemptions permanent or extend them to at least January 1, 2024, to allow for additional time to comply, if the legislature fails to take steps to extend them. Absent this exemption, we request that the Agency issue guidance and provide more clarity regarding CPRA obligations with respect to employee and B2B data.

Business Purpose Disclosures

Section 7051(a)(2) requires businesses to identify, in each service provider or contractor agreement, the specific business purpose for which personal information is disclosed, which goes beyond the statute's obligations. Section 7053(a)(1) of the draft regulations requires the same information for third party agreements, which also goes beyond the statute's requirements and is not feasible. As currently written, this would require an impracticable amount of contract remediation to update executed contracts with this information. We request that these sections be removed from the final rules to align with the content of the statute.

Use of Sensitive Personal Information

In some sections, the draft regulations contravene and narrow the scope of the statutory language, effectively disregarding Section 1798.121(a)-(b) of the CPRA, which permits a business to use a consumer's sensitive personal information (SPI) for uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services," even after receipt of a consumer's request to limit. While the regulations attempt to define permissible uses of Sensitive Personal Information in Section 7027(m), the eight use cases listed do not encompass all those uses of Sensitive Personal Information that may be "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."

For example, section 7014(h) of the draft regulations would require consumer consent to disclose SPI outside collected at a time when a business did not have a notice of right to limit posted, except for the eight uses defined in Section 7027(m). As a notice of right to limit is not required until January 1, 2023 (and only if the business is collecting SPI for the purposes of inferring characteristics), any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the eight limited purposes defined by Section 7027(m). Similarly, in Section 7027(g)(1), the draft regulations require that, upon receipt of a request to limit, a business must cease to use and disclose SPI for any purpose other than the eight purposes listed in Section 7027(m).

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

Accordingly, we respectfully reiterate our request in our last letter that the Agency reconsider such narrowly defined uses or add an additional subsection to section 7027(m) allowing "any other acts or practices that may be necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services."

Notice at Collection Online

Section 7012(f) requires a business that collects personal information online to provide the notice at collection by providing a "a link that takes the consumer directly to the specific section of the business' privacy policy that contains the information required in subsection (e)(1) through (6)." The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement. We believe that this requirement is overly prescriptive, burdensome, and impracticable. For example, the information required in subsection (e)(1) through (6) may not be contained in the same section, and therefore may not be available at a single link, as maintained by the rule. We respectfully request that this requirement to link to a specific section be removed.

Downstream Notification of Opt-Out Requests to All Third Parties

Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer's personal information of a consumer's request to opt-out of sale/sharing and to forward the consumer's opt-out request to "any other person with whom the person has disclosed or shared the personal information." Both requirements go beyond the requirements of the statute and would be technically challenging at the device level (whether in connection with a one-off device interaction or in response to a global privacy control). Further, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information does not take into consideration lawful disclosures to service providers, contractors, law enforcement, government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure. These requirements go beyond the statute and are operationally difficult or impossible due to technological and practical limitations. We respectfully request that the Agency remove this requirement.

Archived or Backup Systems

Section 7022(b)(1) requires businesses to delete a consumer's personal information from its existing systems except "archived or back-up systems," seemingly indicating that requests to delete do not trigger a requirement to delete personal information on archived or back-up systems. To the contrary, Section 7022(d) states that a business that stores any personal information on archived or back-up systems "may delay compliance with the consumer's request" until the archived or back-up system is "restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose." We request that the Agency clarifies its position on deletion of information on archived or backed up systems. Is a business never required to delete personal information stored on archived or back-up systems (as long as it remains on such archived or back-up systems), or does a business have a requirement to delete personal information on archived or stored systems, with the understanding that requirement is not triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose? Additionally, does "access" include de minimis, temporary,

or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of personal information outside of the limited purposes mentioned?

Due Diligence

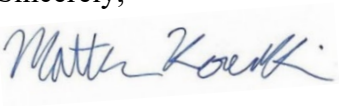
Section 7051(c) and Section 7053(b) state that "[w]hether a business conducts due diligence of its" service providers, contractors, or third parties "factors into whether the business has reason to believe" the service provider, contractor, or third party is using personal information in violation of the CCPA/CPRA. Further, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the personal information in violation of the CCPA. The provisions go beyond the statute and shift nearly all service provider, contractor, and third party liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent the shifting liability. We respectfully request that the Agency strike out or amend and clarify these provisions such that businesses know what level of due diligence is required to prevent the shifting liability.

Topics Unaddressed by the Proposed Rules

Section 1798.185(a)(15) of the California Civil Code requires the Agency to issue rules governing risk assessments that businesses covered under the CPRA must submit to the Agency. The proposed regulations do not provide any guidance on the structure or frequency of these assessments. Additionally, Section 1798.185(a)(16) of the California Civil Code requires the Agency to issue regulations governing access and opt-out rights regarding a business' use of automated decisionmaking technology. Many businesses use automated tools to conduct their businesses efficiently and eliminate bias in decisionmaking. The rules do not provide clarity over the use of these technologies as required by the statute.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact me at 202-469-3181 or mkownacki@afsamail.org.

Sincerely,



Matthew Kownacki
Director, State Research and Policy
American Financial Services Association