

August 23, 2022

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

Re: Comments on proposed rulemaking 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”) July 8 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 requires 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. However, the Agency has indicated that the regulations will not be finalized until the third or even fourth quarter of 2022, leaving businesses with very little time, if any, to comply. While we understand this rulemaking process is complex and appreciate the Agency’s work and consideration of comments throughout the process, we believe a delayed effective date and enforcement date are necessary. The proposed rules would require numerous updates to existing operational systems, including changes to contracts with third-party service providers, website changes and training staff. Therefore, we request that the final rules include a delayed effective date of at least January 1, 2024, and a delayed enforcement date of at least July 1, 2024, which will allow affected financial institutions adequate time to implement the required changes.

§ 7002. Restrictions on the Collection and Use of Personal Information.

Under the proposed regulations, businesses have to obtain the consumer’s *explicit consent* before collecting, using, retaining, and/or sharing the consumer’s personal information for purposes unrelated to, or incompatible with, the purposes for which the personal information was originally collected or processed. The CPRA requires businesses to give consumers notice at the point of personal information collection regarding the categories of information to be collected and the purposes for which this

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.

information will be used. In addition, a supplementary notice to consumers is required if any additional categories of personal information will be collected, or if the collected personal information will be used for purposes incompatible with the ones initially disclosed. The requirement for explicit consent, in addition to the other notices and requirements, will make it more difficult for businesses to evolve and improve their products and services over time. Businesses should not have to obtain an additional consent from the consumer if they fully disclosed all of the potential purposes for which the information may be used, retained or shared (so long as they are not incompatible with the purposes for which the information was originally collected). Developing and marketing new products or improving and marketing existing products would not be feasible.

§ 7004. Consumer Consent.

Section 7004(b) states that activities that do not comply with specific guidelines proposed in the rules constitutes a “dark pattern” and that businesses using “dark patterns” should not be considered to have obtained consumer consent. Section 7004(c) further states that a “user interface is a dark pattern if the interface has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business’s intent.” As written, the draft regulations subject businesses to strict liability regarding the development and implementation of their user interfaces. As a consequence, the Agency or Attorney General could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that may accidentally cause a substantial subversion or impairment of a user’s autonomy, decisionmaking, or choice. It is common for businesses of all sizes to experience problems with their websites, online user interfaces, and mobile applications. Moreover, these problems can occur without the business’s negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminal actors can alter or disrupt a business’s online presence despite the business’s use of state-of-the-art security measures. A business should not be punished for something it did not intend or cause nor could have prevented. We request that the agency drop the strict liability in exchange for a more-measured approach that considers the business’s intent, knowledge, and other relevant factors, such as information security practices. Alternatively, if the regulations retain strict liability, we request that they also establish a safe harbor provision that protects businesses from liability for violations that could not have been prevented or expected.

§ 7011. Privacy Policy.

Section 7011(e) requires a business’s privacy policy to include content not mentioned in the statute. For example, Section 7011(e)(1) requires “a comprehensive description of the business’s online and offline practices regarding the collection, use, sale, sharing, and retention of personal information.” However, the statute does not mention any requirement that the privacy policy contain a “comprehensive description” of a business’s “online and offline practices.” We request that the regulations align with the statute and provide additional guidance or clarity, not create unanticipated requirements with undefined terms such as “comprehensive description.”

§ 7012. Notice at Collection of Personal Information.

Section 7012(e)(4) requires the notice at collection to include the “length of time the business intends to retain each category of personal information,” or if that is impossible, the “criteria used to determine the period of time” the personal information will be retained. Prescriptive data retention notice requirements

are difficult to comply with because of the various and numerous factors that could come into play, such as duration of the relationship with the consumer, duration of the transaction, legal requirements, or in anticipation of defending against legal claims or litigation. We respectfully request that this provision be stricken or amended to allow greater flexibility.

Section 7012(e)(6) requires a business that allows third parties to control the collection of personal information to include in the notice at collection, “the names of all third parties; or, in the alternative, information about the third parties’ business practices.” The statute requires only disclosure of “categories” of third parties, never names or business practices, in the privacy policy, the notice at collection, and in response to the right to know/access. We ask that the agency modify this section to track with the statute requiring categories of third parties, not names or business practices.

Section 7012(f) would require that the notice at collection, if provided online, link to a privacy policy and that the link would take the consumer directly to the applicable section of the privacy policy. This is extremely burdensome and technologically challenging to accomplish. We would suggest, instead, requiring a privacy policy to have sections outlined at the beginning of the privacy policy which enable the consumer to click on the section and be taken to that section of the privacy policy. This flexibility would provide consumers with easy access to the information but would be much more technologically feasible.

Under Section 7012(g)(2), if a business allows third parties (i.e., not service providers or contractors) to control the collection of personal information, the consumer needs to be informed of these third parties’ names or business practices in the privacy notice that they receive at the time of collection of their personal information. Similar to the issue with Section 7012(e)(6) outlined above, the requirement for a business to name or describe the third parties with which it shares personal information would require privacy notices to contain long lists of company names or descriptions that are prone to becoming outdated over time. A lengthy notice prone to including outdated information could end up being so voluminous as to become meaningless to consumers. Accordingly, we request this requirement be removed from the regulations.

§ 7013. Opt-Out Notice.

Section 7013(e) requires a business that “sells or shares” person information provide a notice of right to opt-out of “sale/sharing.” Under current statute and Attorney General regulations, a business that does not “sell” personal information is not required to post a “Do Not Sell My Personal Information” link. Under the proposed draft regulations, if a business “shares” but does not “sell” personal information, the regulations require a business to post a “Do Not Sell or Share My Personal Information” link or the alternative link. If a business “shares” but does not “sell,” or vice versa, the business should be able to post the relevant link and not both links. For example, the business that does not “sell” but “shares” should be permitted to post a “Do Not Share My Personal Information” link without the inclusion of “sell.”

§ 7022. Requests to Delete. & § 7023. Requests to Correct.

Section 7022(b)(1) requires businesses to delete a consumer’s personal information from its existing systems with exceptions for “archived or back-up systems,” indicating that requests to delete do not

trigger a requirement to delete personal information on archived or back-up systems. However, 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 respectfully request that the Agency clarify if a business is never required to delete personal information stored on archived or back-up systems (as long as it says on such archived or back-up systems), or a business has a requirement to delete personal information on archived or stored systems; however, that requirements are not triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose. Additionally, we would like clarification if the definition of “access” includes 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.

Section 7022(f)(1) and Section 7022(f)(2) would require a covered entity to provide a factual, detailed explanation that gives the consumer a meaningful understanding of the disproportionate effort that prevented compliance with a request to delete or correct. The reasons for disproportionality are complex, and some would require a comprehensive understanding of the business’ technical internal processing platform that the consumer does not have. Without this understanding, a detailed explanation would likely confuse, rather than inform, the consumer’s understanding of the process, and the requirement to provide a detailed explanation should be stricken from the rules.

Similarly, the CPRA provides numerous reasons that allow businesses to decline a request to delete or correct. For example, for a consumer request to delete, a financial institution may be able to retain data due to the Gramm Leach Bliley Act (GLBA) exemption, if the account is still open, if the legal records retention period has not expired, etc. Each of these would need to be captured for each individual request and detailed further in the individual consumer response. The complex response required for such a response would be burdensome for the company and may overwhelm or confuse a consumer. Additional complexity exists for other types of requests beyond this specific example. Accordingly, we respectfully request that the requirement to provide a detailed explanation be removed from the rules.

§ 7024. Requests to Know.

Under the CPRA, when a business receives a verifiable consumer request to access their personal information, the disclosed information should cover the 12 months preceding the request. The CPRA allows the regulations to extend this 12-month look-back period unless doing so proves impossible or would involve disproportionate effort on behalf of the business. Accordingly, the proposed regulations impose a look-back period back to January 1, 2022, and also extend the scope of requests to personal information in the hands of the business’s service providers and contractors. This broadening of personal information that is subject to consumer requests will make honoring requests more burdensome for businesses. The regulations should not broaden the personal information that is subject to consumer requests, if it is not explicitly stated in the CPRA.

§ 7025. Opt-Out Preference Signals.

The CPRA provides businesses with different options regarding how businesses can enable consumers to exercise their opt-out rights, for instance by providing opt-out links, or by honoring opt-out preference signals received from consumers' devices or applications. However, the proposed regulations require that opt-out preference signals need to be complied with regardless of whether a business has chosen to provide the opt-out links. This requirement has no basis in the CPRA and exceeds the Agency's authority. Taking away a business's option between providing opt-out links and honoring preference signals is overly burdensome, and the regulation should retain a business's choice between providing opt-out links and honoring preference signals, as provided by the CPRA.

§ 7027. Requests to Limit Use and Disclosure of Sensitive Personal Information.

In a number of sections, the regulations contravene and narrow the scope of the statutory language. This effectively disregards Section 1798.121(a)-(b) of the statute, which permit a business to use a consumer's sensitive personal information 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(l), the seven 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."

We believe that the rules' narrow scope has significant adverse effect. As an example, in Section 7014(h), the Regulations purport to impose a springing consent requirement with respect to any use, outside the seven limited uses defined by Section 7027(l), of Sensitive Personal Information collected at a time when a business did not have a notice of right to limit posted. As written, since a notice of right to limit is not required until January 1, 2023, any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the seven purposes defined by Section 7027(l). Similarly, in Section 7027(g)(1), the Regulations require that, upon receipt of a request to limit, a business must cease to use and disclose Sensitive Personal Information for any purpose other than the seven purposes listed in Section 7027(l); a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services." We believe that these inconsistencies are extremely problematic for constructing a compliance program. Furthermore, the seven use cases identified in 7027(l) do not contemplate a use of Sensitive Personal Information to comply with a legal or regulatory obligation or otherwise address any use case that relates to uses of employee information. Accordingly, we respectfully request that the Agency reconsider such narrowly defined uses or add an additional section 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."

CPRA Section 1798.121(d) states that the requirements in the CPRA related to limiting usage of sensitive personal information and providing a usage limit link don't apply if sensitive personal information is collected and processed without the "purpose of inferring characteristics about a consumer." The proposed regulations do not include this exception. Instead, the regulations may be subjecting all businesses to the CPRA's usage limitation and link requirements, including those who do

not use sensitive personal information for the purpose of inferring characteristics. The regulations should be revised to reflect the exception under Section 1798.121(d), and be revised to provide guidance and examples of what it means to use sensitive personal information to infer and not infer characteristics about a consumer.

§ 7050. Service Providers and Contractors.

The proposed regulations are very prescriptive about the exact provisions that need to be in any contract with a third party that is considered a service provider. These burdensome provisions will make compliance exceptionally difficult, and we believe additional flexibility would provide the desired protections while easing the compliance burden.

§ 7051 Contract Requirements for Service Providers and Contractors. & § 7053 Contract Requirements for Third Parties.

The proposed regulations limit the CPRA's safe harbor for businesses based on their due diligence of their service providers and other parties. Under the proposed regulations, if a business fails to enforce contractual terms and fails to audit or test its service providers', contractors', or third parties' systems, the business might not be able to claim that it did not have reason to believe that its service providers, contractors, or third parties intended to use the personal information in violation of the CPRA. This erodes the safe harbor that would otherwise protect a business whose service provider fails to comply with the CPRA despite its contractual and statutory duties to do so. The limit to the CPRA's safe harbor for businesses based on their due diligence of their service providers and other parties should be removed from the regulations.

The proposed regulations require similar contractual provisions in agreements between businesses and their service providers or contractors as the required contractual provisions between businesses and other third parties. Since the nature of a relationship between a business and its processor is fundamentally different from its relationship with another controller, having the same contractual provisions, such as purpose limitations and oversight provisions, in both kinds of agreements is unlikely to accurately reflect the true relationship and allocation of responsibilities of the two parties. Additionally, new contractual requirements put additional burdens on businesses that need to negotiate and update potentially hundreds or thousands of agreements. This is time consuming and costly to the business and ultimately the consumer if reflected in the price of products and services. The regulations should automatically bind the required contractual provisions to service providers, contractors and third parties. If the contract includes a compliance with laws representation, the relevant provision of the CPRA would be included by reference into the contract. This is more efficient and will considerably reduce the cost to update contracts.

§ 7063. Authorized Agents.

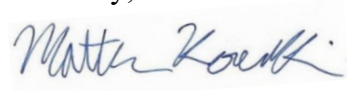
The requirements in Section 7063(b) should remain unmodified, as an opportunity for fraud is created by allowing a consumer to authorize an agent to manage their personal information based on a simple signature without a requirement for the agent to be registered or for the consumer to provide a power of attorney or a notarized signature.

Extension of Employee and B2B 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 leave employees, job applicants, employers and individuals serving other businesses in a service provider context confused regarding the interplay between the CPRA and employment laws because most of the rights under the CPRA either are already addressed or do not make sense in the employment or B2B context. We recommend that in future rulemakings 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.

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