CALIFORNIA BANKERS ASSOCIATION

August 23, 2022

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Boulevard
Sacramento, CA 95834
regulations@cppa.ca.gov

RE: Comments on Proposed Rulemaking Implementing the California Privacy Rights Act of 2020

Dear Mr. Soublet:

The California Bankers Association (CBA) appreciates the opportunity to submit comments to the California Privacy Protection Agency (Agency) on the proposed rulemaking to adopt regulations to implement the California Privacy Rights Act (CPRA) of 2020. CBA is one of the largest banking trade associations in the United States advocating on legislative, regulatory, and legal matters on behalf of banks doing business in California.

The importance of protecting consumer data and privacy are not new concepts for banks who have operated for decades under protections established by laws like the Gramm-Leach-Bliley Act and California Financial Information Privacy Act. As the Agency works toward adopting regulations in accordance with the CPRA, we appreciate the opportunity to provide input.

Section 7002: Restrictions on the Collection and Use of Personal Information.

Section 7002(a) requires "explicit consent" to collect, use, retain, or share personal information for "any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed." To the contrary, Civil Code Section 1798.100(a)(1) permits the collection or use of personal information for additional purposes that are incompatible with the disclosed purposes as long as the business notifies the consumer of the additional purposes. Accordingly, we believe requiring "explicit consent" goes beyond the statute. We urge that the regulations be consistent with the statute by requiring notice, not explicit consent.

Section 7004: Requirements for Methods for Submitting CCPA Requests and Obtaining Consumer Consent.

Section 7004(a)(5) requires that California Consumer Privacy Act (CCPA) requests submitted by consumers be easy to execute. While understandable, making technical issues like broken links a violation of the regulation is excessive and unduly burdensome. We request that this language be removed or that a willful or malicious intent standard be included when imposing liability for a broken link.

Section 7004(c) 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." The proposed regulations subject businesses to strict liability regarding the development and implementation of their user interfaces. As such, the Agency could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that are accidental.

Businesses may experience problems with their user interfaces. These problems may occur without the business's negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminals can alter or disrupt a business's online presence despite the business's best efforts. A business should not be punished for something that was unintentional, that it did not cause, nor for something it could not prevent. Instead of strict liability, the regulations should consider the business's intent, knowledge, and other relevant factors, such as information security practices. The proposed regulations also fail to make it clear what qualifies as substantial.

Section 7010: Overview of Required Disclosures.

Section 7010(b) of the proposed regulations require a "business that controls the collection of a consumer's personal information shall provide a notice at collection." The proposed regulations delete the reference to collecting personal information "from a consumer" suggesting that the notice must cover personal information obtained from third parties as well as from consumers.

Conversely, Section 7012(a) indicates that the "purpose of the notice at collection is to provide consumers with timely notice, at or before the point of collection, about the categories of personal information to be collected from them". (Emphasis added). For consistency with Section 7012(a), the draft regulations should avoid deleting "from a consumer" in Section 7010(b).

Section 7012: Notice at Collection of Personal Information.

Section 7012(e)(4) requires the notice at collection of personal information to include the "length of time the business intends to retain each category of personal information identified in subsection (e)(1), or if that is not possible, the criteria used to determine the period of time it will

be retained." We urge that this provision be removed or that it allow flexibility. Aside from being difficult to comply with, a lengthy and complicated notice is less likely to be read by consumers compared to a more basic notice that indicates how personal information is collected and used.

Section 7012(e)(6) requires a business to include in its notice at collection if the "business allows third parties to control the collection of personal information, the names of all third parties; or, in the alternative, information about the third parties' business practices." Conversely, Civil Code Section 1798.110(c)(4) requires a business that collects personal information about consumers shall disclose the "categories of third parties to whom the business discloses personal information." As such, the statute doesn't require a business to disclose the names of third parties nor the third party's business practices as proposed by the regulations. The proposed regulations go beyond the statute. Accordingly, we urge that the regulations be consistent with the statute by requiring disclosure of the categories of third parties, not the names or business practices of third parties.

Section 7022: Requests to Delete.

Section 7022(c)(4) requires a service provider or contractor, upon notification by a business, to notify any other service providers, contractors, or third parties to delete the consumer's personal information unless it is impossible or involves disproportionate effort. If the service provider or contractor claims that such a notification involves a disproportionate effort, "the service provider or contractor shall provide the business a detailed explanation that shall be relayed to the consumer that includes enough facts to give a consumer a meaningful understanding as to why the notification was not possible or involved disproportionate effort."

We urge that the requirement to provide a detailed explanation be removed given that this requirement is not derived from the statute and considering the complexity and the resource intensive nature that would be involved in determining whether providing a notification involves a disproportionate effort.

Section 7023: Requests to Correct.

The proposed regulations create new requirements around requests to correct that make compliance operationally and technically infeasible. More specifically, the proposed regulations in Section 7023(c) require that a business must ensure that personal information remain corrected, which could require a business to establish mechanisms ensuring that corrected personal information is not overridden by inaccurate personal information subsequently received. Another example is in Section 7023(i) of the proposed regulations, which requires that a business must not only correct personal information, but it must provide the consumer with the name of the source of the alleged inaccurate information where the business itself is not the source of the information.

When responding to a request to correct, Section 7023(f)(2) requires a business that claims complying with the request to correct is impossible or would involve a disproportionate effort to provide the "consumer a detailed explanation that includes enough facts to give a consumer a meaningful understanding as to why the business cannot comply with the request."

We urge that the requirement to provide a detailed explanation be removed given that this requirement is not derived from the statute and considering the complexity and the resource intensive nature that would be involved in determining whether complying with the request to correct involves a disproportionate effort.

Section 7023(f)(3) requires a business that has denied a consumer's request to correct in whole or in part, to inform "the consumer that, upon the consumer's request, it will note both internally and to any person with whom it discloses, shares, or sells the personal information that the accuracy of the personal information is contested by the consumer", unless the request is fraudulent or abusive. This requirement goes beyond the statute, and we request that the provision be removed. Further, if the denial is lawful, it is unclear what the person will do with this information.

Section 7023(h) requires a business that determines that a request to correct is fraudulent or abusive must "inform the requestor that it will not comply with the request and shall provide an explanation why it believes the request is fraudulent or abusive." This provision should be removed from the proposed regulations as it raises a security risk for consumers by potentially revealing anti-fraud protocols to potential wrongdoers.

Section 7025: Opt-Out Preference Signals.

Section 7025(b) states that a "business shall process any opt-out preference signal that meets the following requirements as a valid request to opt-out of sale/sharing", which is inconsistent with Civil Code Section 1798.135(b)(3), which states that a "business that complies with subdivision (a) is not required to comply with subdivision (b)." Civil Code Section 1798.135(a) outlines the requirements for businesses that provide opt-out links on its internet homepage.

Civil Code Section 1798.135(b)(3) states for "the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)." Accordingly, the statute grants businesses the choice of whether they want to provide opt-out links on their internet homepage or honor universal opt-out preference signals.

Conversely, the proposed regulations require businesses to provide opt-out links on their internet homepage and to honor universal opt-out preference signals. We urge that the regulations align with the statute, thereby permitting businesses the option granted in statute.

Section 7026: Requests to Opt-Out of Sale/Sharing.

Section 7026(f)(2) requires a business to comply with a request to opt-out of the sale or sharing of personal information by notifying "all third parties to whom the business has sold or shared the consumer's personal information" of the consumer's request to opt-out of the sale or 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 of these requirements go beyond the statute and should be deleted.

Furthermore, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information doesn't 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 consumer to make the disclosure.

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

Civil Code Section 1798.121(d) states that sensitive personal information "that is collected or processed without the purpose of inferring characteristics about a consumer, is not subject to this section, as further defined in regulations adopted pursuant to subparagraph (C) of paragraph (19) of subdivision (a) of Section 1798.185, and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100."

The proposed regulations focus on the request to limit the use and disclosure of sensitive personal information but do not offer clarity on when sensitive personal information is considered collected or processed. According to the statute quoted above, collecting or processing sensitive personal information for purposes other than inferring characteristics about a consumer is exempt from the right to limit the use and disclosure of sensitive personal information. However, the proposed regulations imply this exemption does not exist and any collection or processing of sensitive personal information is subject to the right to limit its use and disclosure. The regulations should be amended to align with the statute.

In addition, the draft regulations provide seven permissible uses of sensitive personal information. However, these permissible uses should be clarified and expanded to include uses of sensitive personal information to comply with legal or regulatory obligations.

Section 7050: Service Providers and Contractors.

The proposed regulations provide a limited view of the types of advertising services that may be provided by service providers and contractors. Under the proposed regulations and illustrative examples, a social media company that acts as a service provider or contractor cannot use a list

of a business's customer email addresses to identify users on the social media company's platform to serve advertisements to them.

The proposed regulations do not address a circumstance where the social media company agrees to use personal information solely for the business's benefit, in which case the social media company would be operating as a service provider or contractor. Without further clarification in the regulations, situations where businesses disclose personal information to an entity solely to provide services to the business could constitute sharing under the CPRA when no cross-context behavioral advertising occurs.

Section 7051: Contract Requirements for Service Providers and Contractors.

The proposed regulations in Section 7051(a)(2) require that agreements between a business and service provider or contractor identify specific purposes for which personal information is disclosed, which cannot be described in "generic terms, such as referencing the entire contract generally." This provision requires businesses to take a highly customized approach to every engagement that utilizes a standard addendum to address data usage restrictions in compliance with the law. Requiring businesses to take a customized approach to every engagement is overly burdensome to businesses without providing a commensurate benefit to the consumer and we believe that the provisions go beyond statutory requirements.

Section 7051(e) states that whether "a business conducts due diligence of its service providers and contractors factors into whether the business has reason to believe that a service provider or contractor is using personal information in violation of the CCPA and these regulations." The section offers 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 or contractor intended to use the personal information in violation of the CCPA.

This provision goes beyond the statute and shifts service provider and contractor liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent this shift in liability. We urge the striking of these provisions or clarifying them such that businesses have clear guidance on what level of due diligence is required to prevent liability.

Section 7053: Contract Requirements for Third Parties.

Similar to the comments offered previously in Section 7051, Section 7053(a)(1) of the proposed regulations require that a business identify, in each agreement, the specified purpose for which personal information is sold or disclosed, which goes beyond the statutory requirements.

Section 7053(e) states that whether "a business conducts due diligence of the third party factors into whether the business has reason to believe that the third party is using personal information in violation of the CCPA and these regulations." The section offers 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 third party intended to use the personal information in violation of the CCPA.

This provision goes beyond the statute and shifts third party liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent this shifting of liability. We urge the striking of these provisions or clarifying them such that businesses have clear guidance on what level of due diligence is required to prevent liability.

Section 7063: Authorized Agents.

Civil Code Section 1798.185(a)(7) requires rules and procedures to facilitate a consumer's authorized agent to make various CCPA-related requests taking into consideration, among other things, security concerns.

We continue to underscore our concerns that the regulations pertaining to authorized agents may provide an opportunity for fraud by allowing a consumer to authorize an agent to manage their personal information based on a signature and without a requirement for the agent to be registered or for the consumer to provide a power of attorney or a notarized signature.

Section 7304: Agency Audits.

With respect to the Agency's authority to audit businesses' compliance with the law, we urge the Agency to exempt banks which are highly regulated and subject to ongoing supervision and frequent examination by banking regulators.

State and federally chartered banks have at least three independent regulators. For example, state-chartered banks are presently regulated by the California Department of Financial Protection and Innovation, the federal Consumer Financial Protection Bureau, and the Federal Deposit Insurance Corporation (FDIC). This level of oversight includes frequent, routine examinations by regulatory agencies of not only the safety and soundness of these organizations but of their compliance with various laws whether focused on consumer protection or otherwise.

Bank examinations are comprehensive and require a bank to dedicate significant time and resources in advance of the exam commencing. Banks are required to gather and compile significant amounts of records, data and information in preparation for an examination. While examiners may conduct some portion of an exam off-site it is typical that the regulator conducts

a portion of the examination on bank premises. Examinations conclude with the regulator communicating findings to the bank through meetings with management and an exam report.

With respect to the adherence to state and federal laws, banking regulators are granted broad authority when conducting compliance exams. As an example, the FDIC's Consumer Compliance Examination Manual requires the examiner to review the bank's compliance with the Gramm-Leach-Bliley Act. In this regard, the examiner is considering the bank's notices, privacy policies, internal controls, information sharing practices, complaint logs, administration of opt-out requests, etc. Similarly, the California Department of Financial Protection and Innovation examines a bank's compliance with the California Financial Information Privacy Act.

In furtherance of our request that banks be exempt from audit, the Agency may wish to familiarize itself with the comprehensive processes and systems developed by bank regulators surrounding routine examinations, including the detailed examination manuals that are publicly available. We urge the Agency to consider the robustness of bank examinations, the well-developed structure that has been established around exams, the extensive scope of the review covered in an exam, and the routine and frequent nature in which these exams are conducted.

Enforcement Deadline.

Understanding that final regulations will not be adopted by the statutorily mandated deadline of July 1, 2022, as required by Civil Code Section 1798.185(d), we request that the regulations not be enforceable until one year from the date of final adoption of this rulemaking. Businesses subject to the CPRA would have been given one year to implement the requirements of the regulations before enforcement of the regulations began. Accordingly, we request that the regulations become enforceable one year after the date the regulations are finalized.

####

Thank you for the opportunity to offer comments. We welcome any questions you may have.

Sincerely,

Kevin Gould
EVP/Director of Government Relations

KG:la