California
CREDIT UNION LEAGUE

August 22, 2022

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

Re: **CPPA Public Comment**
Proposed Regulations to Implement Changes to the California Consumer Privacy Act of 2018 (CCPA), as Amended by the Consumer Privacy Rights Act of 2020 (CPRA)

Dear Mr. Soublet:

I am writing on behalf of the California Credit Union League (League), one of the largest state trade associations for credit unions in the United States, representing the interests of approximately 230 California credit unions and their more than 11.6 million members.

On July 8, 2022, the California Privacy Protection Agency (CPPA) began its formal rulemaking activities in connection with the administration and enforcement of the California Consumer Privacy Act of 2018 (CCPA), as amended by the California Privacy Rights Act of 2020 (CPRA) (collectively, CCPA/CPRA).

The League has significant concerns with a number of aspects of the CCPA/CPRA and the proposed regulations, including: (1) several areas in the proposed regulations that appear to exceed the requirements of CCPA/CPRA; (2) the potential audits to be performed by the CPPA; (3) the effective date; (4) the enforcement date; (5) a lack of clarity around the exemption for personal information collected pursuant to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA); and (6) the lack of model notices to facilitate compliance.

We respectfully offer the following comments.

1. Proposed Regulations Exceed Statute Requirements

Many areas in the proposed regulations appear to exceed the requirements of the statute—requiring more detailed levels of explanation to the consumer, written confirmations beyond what the statute indicated, and additional steps. While the CPPA was given broad statutory authority to establish rules and procedures to implement and further the purposes of the CCPA/CPRA, some of these additional proposed requirements create an unnecessary burden on businesses and should be reconsidered.

The following outlines our specific concerns:

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

Under Calif. Civil Code §1798.100, businesses need to provide notice to consumers at the point of collection regarding the categories of personal information collected and the purposes for which the information will be used. Before a business collects additional categories of personal information or uses personal information for additional purposes that are incompatible with the disclosed purposes, a consumer must receive a supplementary notice.
Section 7002(a) of the proposed regulations would require a business to obtain the consumer's "explicit consent" before collecting, using, retaining, and/or sharing the consumer's personal information for any purpose that is unrelated or incompatible with the purpose(s) for which the personal information collected or processed.

This exceeds the statutory requirement and creates a new "opt-in" requirement. We recommend replacing this requirement with a new notice to the consumer along with a 30-day opportunity to opt-out, which is more consistent with the statutory intent.

B. §7023. Requests to Correct

The CPRA has amended the CCPA to add a new right: the Right to Request Correction of Inaccurate Personal Information (Calif. Civil Code §§1798.106 and 1798.130).

Section 7023(f) adds additional layers of notice requirements when a consumer submits a request to correct inaccurate information. Not only must the business provide specific notices and explanations to the consumer with regard to its response, §7023(f)(3) of the proposed regulations now requires businesses that receive a consumer request to correct inaccurate information to also inform any person with whom it discloses, shares, or sells the personal information that the consumer contests the accuracy of the information, adding yet another notice requirement on the business not established under the statute. Moreover, it does not afford the business a reasonable opportunity to investigate the validity of the claim or the accuracy of the information before it is under an obligation to notify third parties.

In addition, §7023(i) of the proposed regulations requires businesses, when they are not the source of the inaccurate information, to provide consumers with the name of the source from which the businesses receive the alleged inaccurate information. This exceeds the original statute and may create significant compliance and technological challenges for a credit union without a data inventory or data mapping program.

C. §7024. Request to Know

Under Calif. Civil Code §1798.130(a)(2)(B), a business is required to respond to a request to know with specific pieces of personal information that the business has collected about the consumer for the 12-month period preceding the business's receipt of the request and beyond pursuant to a regulation.

Under the proposed regulations, §7024, a business ***must provide*** the consumer "[a]ll the personal information it has collected and maintains about the consumer on or after January 1, 2022, including beyond the 12-month period preceding the business's receipt of the request, unless doing so proves impossible or would involve disproportionate effort."

This requirement proposed in the regulation contradicts the current requirement under the statute, which states that a business is only required to provide personal information from the prior 12 months ***unless the consumer requests*** that the business provide information beyond the 12-month period. We believe that the regulation's more expansive requirement is problematic and would create an additional burden on businesses.

D. §7025. Opt-Out Preference Signal

Calif. Civil Code §1798.135(b) provides that a business that sells or shares consumers' personal information or uses or discloses consumers' sensitive personal information for purposes other than as expressly authorized shall not be required to provide opt-out links on its website *if* the business allows consumers to opt out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal.

However, under §7025 of the proposed regulations, a business that sells or shares personal information would *always* be required to process a consumer's request via an opt-out preference signal, although if it posts the opt-out links, it may process opt-out preference signals in a non-frictionless manner.

Because the CCPA/CPRA has been interpreted to give businesses the *option* to process and comply with opt-out preference signals instead of implementing Opt-Out Links or Alternative Opt-Out Links, we believe that the proposed regulations contradict this interpretation and may create significant compliance and technological challenges, especially for our smaller credit unions.

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

Calif. Civil Code §1798.121 gives consumers the right to request a business to limit its use and/or disclosure of their sensitive personal information.

The proposed regulations, at §7027(l), set forth a list of purposes for which a business may use or disclose sensitive personal information without offering the right to limit the use or disclosure of such information (e.g., to perform the goods or services requested, to detect security incidents, to prevent fraud, etc.). However, the proposed regulations do not clarify when sensitive personal information is to be considered "collected" or "processed" when the business is inferring characteristics about the affected consumer. We believe the lack of clarity in this area could potentially create confusion and possible unintended violations of CCPA/CPRA.

F. §7050. Service Providers and Contractors

Section 7050 of the proposed regulations cites the following example to help clarify when a business that provides services to a person or organization that is not a business, as defined, might be deemed a "service provider" or a "contractor":

"[A] cloud service provider that provides services to a non-profit organization and meets the requirements and obligations of a service provider under the CCPA and these regulations, i.e., has a valid service provider contract in place, etc., shall be considered a service provider even though it is providing services to a non-business."

The example stated above is confusing. Is it the CPPA's position that services rendered to a non-profit entity would be subject to the CCPA/CPRA requirements even though CCPA/CPRA exempts non-profits from its application? We respectfully ask that the final regulations clarify whether the exemption applies to or excludes non-profit entities.

2. Burden of Potential Agency Audits to Highly Regulated Businesses

Calif. Civil Code §1798.199.65 gives the CPPA the authority to audit businesses' compliance with the law. The proposed regulations (§7304) would allow the CPPA to perform audits in three situations: (1) to investigate possible violations of the CCPA/CPRA; (2) if the subject's collections or processing activities present significant risk to consumer privacy or security; or (3) if the subject has a history of noncompliance with the CCPA/CPRA or any other privacy protection laws. Moreover, these audits maybe announced or unannounced, and a business's failure to cooperate with an audit could lead to enforcement action against that business.

Pending further clarification regarding the definition of a "business" as discussed in Section 7 below, credit unions may be subject to the CCPA/CPRA and therefore to audits performed by the CPPA. Moreover, the CPPA's enforcement authority could extend to both state and federally chartered credit unions.

As financial institutions, credit unions are already among one of the most highly regulated industries. California's state-chartered credit unions are licensed and regulated by the California

Department of Financial Protection and Innovation (DFPI), and the National Credit Union Administration (NCUA) regulates federal credit unions as well as federally insured state credit unions. Additionally, credit unions are subject to federal Consumer Financial Protection Bureau (CFPB) oversight, among other agencies. Credit unions currently undergo robust examinations by their regulatory agencies, which includes their compliance with applicable state and federal privacy and data security laws and regulations. We are concerned that potential audits conducted by CPPA would be not only duplicative of existing examination requirements, but unjustifiably intrusive, burdensome, and overreaching for credit unions. The burden of these additional audits on smaller financial institutions could be especially significant in terms of disruption to staffing and operations. Therefore, we believe that a clear exemption is warranted.

However, if the CPPA is unwilling to provide such an exemption for credit unions, then it must provide guidance as to how credit unions can comply without unnecessarily burdening the credit union industry. At a minimum, coordination with state and federal primary regulators would be warranted.

3. Effective Date

The CCPA/CPRA is effective January 1, 2023. However, the proposed regulations were not issued until July 8, 2022, and they expanded the compliance obligations over that of the current CCPA in a number of areas. Given the detailed and technical nature of the proposed regulations, as well as the extensive technical and operational steps that will be required to ensure full compliance, it is only fitting that the CCPA/CPRA effective date should be extended.

Covered businesses need adequate time to understand the requirements of the statute and the final regulations prior to designing and implementing comprehensive compliance solutions appropriate to the size and scope of their operations, as well as the time and financial resources to actually design and implement those solutions and adequately train staff. The Leagues recommend that the CCPA delay the effective date by two years, until January 1, 2025.

4. Enforcement Date

The CCPA/CPRA provides that the CPPA can bring enforcement action six months after publication of the final regulations or July 1, 2023, whichever is sooner. That means the CPPA could literally adopt final regulations on June 30, 2023, and enforce the law and the regulations the next day, on July 1, 2023.

While we understand that this is not the most likely scenario, it is still a serious concern. As stated above, covered businesses should have adequate time to understand the requirements of the statute and the final regulations, and sufficient time to design and implement comprehensive compliance solutions before being subjected to enforcement actions. Due to the complexities of the

CCPA/CPRA, we urge the CPPA to delay enforcement until no less than six months after publication of final regulations.

5. GLBA and CFIPA Exemptions

The CPRA revised the CCPA's financial information exception to apply to "personal information collected, processed, sold, or disclosed ***subject*** to the federal Gramm-Leach-Bliley Act . . . , or the California Financial Information Privacy Act…" (emphasis and revision added).

Regardless of this change, there is still significant confusion regarding the exemption for personal information collected, processed, sold, or disclosed subject to the federal Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (CFIPA). The confusion arises because the CCPA/CPRA uses terms that are inconsistent with the GLBA and CFIPA.

- The GLBA and CFIPA both use the terms "nonpublic personal information" and define that term to mean "personally identifiable financial information."
- The CCPA/CPRA uses the term "personal information," which is defined in Calif. Civil Code §1798.140(o) and is much broader than the GLBA/CFIPA's definition of "nonpublic personal information."
- In addition, the GLBA pertains to "personally identifiable financial information" collected in the course of a transaction or providing a financial product or service, etc. The CCPA/CPRA pertains to personal information collected in basically any manner, including when there is no transaction.

Because of the inconsistent terminology, the exemption provided in Calif. Civil Code §1798.145(e) is unclear and can be interpreted several ways. It is essential that the CPPA provide clarification in the regulations.

Moreover, for financial institutions that are only subject to the CCPA/CPRA notice requirements to the extent not covered by an exemption, guidance with regard to the appropriate response to a consumer that recognizes this exemption would be especially useful, given that consumers are unlikely to be familiar with the nature and extent to which the exemption applies.

6. Model Notices Needed

The CCPA and its regulations created several notice requirements for businesses, including:

- Notice at or Before Collection,
- Right to Opt-Out,
- Notice of Financial Incentives, and
- Updated Privacy Notices.

Further, the regulations require specific responses to certain verifiable consumer requests, for which model forms for both the request and the response would be beneficial:

- Verifiable Consumer Request to Know,
- Response to Verifiable Consumer Request to Know,
- Verifiable Consumer Request to Delete,
- Response to Verifiable Consumer Request to Delete,
- Verifiable Consumer Request to Limit the Use of Sensitive Personal Information, and
- Response to Verifiable Consumer Request to Limit the Use of Sensitive Personal Information.

As noted above, the CPRA added the new Right to Request Correction of Inaccurate Personal Information, which would require a specific response to another form of verifiable consumer request. Useful Model forms would include:

- Verifiable Consumer Request to Correct Inaccurate Personal Information, and
- Response to Verifiable Consumer Request to Correct Inaccurate Personal Information.

Additionally, businesses must provide notice of the following consumer requests to third party service providers and contractors:

- Notice to Third Party Service Provider/Contractor that Consumer Contests the Accuracy of Certain Personal Information,
- Notice to Third Party Service Provider/Contractor of Consumer Opt-Out Request,
- Notice to Third Party Service Provider/Contractor of Consumer Deletion Request, and
- Notice to Third Party Service Provider/Contractor of Consumer Request to Limit the Use of Sensitive Personal Information.

For all these required notices and responses, the regulations require the notices be easy to read and understandable by the average consumer and provide some standards to achieve that. This direction is subjective and does not contemplate a method or metric to assess the readability.

Since all businesses need to provide the required notices and responses, uniform model notices would help ensure consumer's understanding of the notices, simplify the requirements for businesses, and create an objective standard of review to determine whether a business' notices comply with the required standards. The Leagues recommend the CPPA draft proposed model notices for public comment and then include a safe harbor in the final regulations for the use of notices substantially similar to the model notices.

The provision of model notices by the CPPA will also help to alleviate some of the initial compliance burden associated with meeting the fast-approaching Effective Date and Enforcement Date.

7. Other Considerations

A. The Credit Union Difference

The League supports the spirit of the law; however, it is important that the CPPA understand the credit union difference. Credit unions, while highly regulated financial institutions, are first and foremost member-owned, democratically governed, not-for-profit financial cooperatives whose purpose is to promote thrift and improve access to credit for their member-owners, particularly those of modest means. As not-for-profit entities, credit union earnings are passed on to their member-owners in the forms of reduced fees, higher savings rates, and lower loan rates. Credit unions exist for the financial benefit of their member-owners, but they are ultimately driven by the philosophy of people-helping-people.

The credit union structure is vastly different than for-profit entities. "Owners" are not proprietors or shareholders in a business whose only goal is that the business maximize individual shareholder profits. Instead, credit union shareholders are members of a not-for-profit cooperative with a volunteer board of directors democratically elected by and from among its members. Each member has one vote, regardless of the number of shares (amount of funds) held in the credit union. Consumer personal information collected by credit unions is the personal information of its member-owner consumers in order to provide them with the products and services they desire.

Credit unions are the original consumer financial protection advocates. In addition, as highly regulated insured depository institutions, credit unions already comply with a plethora of data privacy and security requirements, including GLBA, CFIPA, and NCUA's data security regulations.

B. Definition of a Business

The definition of a "business" subject to the requirements of the CCPA/CPRA requires further clarification.

- *Thresholds*

The CPRA changed the scope of covered businesses. Part of the definition of a business is that it satisfies one or more of the following thresholds:

> (A) As of January 1 of the calendar year, had annual gross revenues in excess of twenty-five million dollars ($25,000,000) in the preceding calendar year, as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.
>
> (B) Alone or in combination, annually buys or sells, or shares the personal information of 100,000 or more consumers or households.
>
> (C) Derives 50 percent or more of its annual revenues from selling or sharing consumers' personal Information.

The application of threshold (B) to the personal information of 100,000 or more "consumers or households" is confusing. A consumer, as defined in the CCPA/CPRA is a natural person California resident. Is the rest of the threshold then related to households of natural person California residents? Additionally, further clarification is needed to determine the method for counting the number of consumers or households toward the 100,000 threshold. For example, if one household has five individual residents/consumers, would they be counted as one (household), five (consumers) or six (five consumers plus one household) toward the 100,000 threshold? For smaller credit unions, these distinctions are essential to the determination of whether they are subject to the requirements of the CCPA/CPRA.

- *Doing Business in California*

Another part of the definition of a business is that the entity "does business in the State of California." There is no clear definition under the CCPA/CPRA or the regulations of what it means to "do business" in the State of California. Clarification is needed.

For credit unions based outside of California, members may live in or relocate to California while maintaining a relationship with their out of state credit union through ATMs or a shared branching network. (A shared branching network allows a member of one credit union to walk into the local branch of another credit union of which they are not a member and perform a range of transactions.)

At what point does the non-California credit union become subject to the CCPA/CPRA despite the lack of a physical presence? "Doing business" in a state should mean something more than isolated or incidental transactions. There should be a clearly defined standard that contemplates intentional repeated and successive transactions that clearly indicates a pattern or practice of choosing to do business with California consumers, and not one-time or occasional transactions.

Final Comments

Ultimately, the League supports the spirit of the law and the need to protect the personal information of its members, but we continue to have significant concerns with the practicality and implementation of the proposed regulations.

We thank you for the opportunity to comment. We trust you will carefully consider our views and recommendations. If you have any questions regarding our comments, please contact me.

Sincerely,

Diana R. Dykstra
President/CEO
California Credit Union League