California
CREDIT UNION LEAGUE

November 15, 2022

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

Re: **CPPA Public Comment**
Modified 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) (Original Proposed Regulations). On November 3, 2022, the CPPA proposed further amendments to the Original Proposed regulations based on initial comments received (Modified Proposed Regulations).

The League has previously provided comments regarding the CCPA/CPRA and respectfully offers the following comments and feedback on the Modified Proposed Regulations for your further consideration.

- **Investigations and Enforcements**

The Modified Proposed Regulations add the following provision (b) to Section 7301:

> "[A]s 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."

The above Modified Proposed Regulation language states that the CPPA ***may*** take the delay in promulgating regulations and good faith efforts to comply into consideration instead of that it ***shall*** take them into consideration.

Given that covered businesses are likely to have six or seven less months to prepare for the July 1, 2023, enforcement start date than initially intended, the League is concerned that the Modified Proposed language is too permissive, leaving businesses at risk of possible enforcement actions despite their best efforts to comply. We believe that the considerations identified in §7301(b) are reasonable and fair and should always be taken into consideration.

- **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.

The League previously provided comments on August 22, 2022, in response to the Original Proposed Rules wherein the League expressed concerns regarding the proposed Section 7304, which concerns persist.

As indicated in our prior comment letter, pending further clarification regarding the definition of a "business" as discussed in 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 strongly reiterate our position 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 and appropriate.

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.

- **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. Despite the language of §7301(b) of the Modified Proposed Regulations regarding possible enforcement considerations, 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, or the threat of enforcement actions. This is particularly true in light of the fact that the temporary exemptions extended to employee and certain business-to-business (B2B) data under Cal. Civil Code §1798.145 (m) and (n) sunsets as of January 1, 2023. The Modified Proposed Regulations remain silent on these specific compliance challenges that covered businesses are currently facing.

Due to the complexities of the CCPA/CPRA, the fact that the Modified Proposed Regulations are missing key guidance on all topics for which regulations are still necessary pursuant to §1798.185 of the CCPA/CPRA, as well as sunsetting of the exemption for employee and B2B transactions, we urge the CPPA to delay enforcement until no less than six months after publication of final regulations. It is essential for effective compliance that the Agency take the time needed to ensure that any regulatory language adopted is comprehensive and complete, and based upon underlying CCPA/CPRA statutes that are fixed and not in a state of impending amendments.

- **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). We are disappointed that neither the Original Proposed Regulations nor the Modified Proposed Regulations clarify this exemption.

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 vague and 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's verifiable request that recognizes this exemption would be especially useful, given that consumers are unlikely to be familiar with the nature of the exemption or the extent to which it applies.

- **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 covered businesses need to provide the required notices and responses, uniform model notices would help to ensure a consumer's understanding of the information being provided, simplify the requirements for businesses, and create an objective standard of review to determine whether a business' notices comply with the required standards.

We are disappointed that neither the Original Proposed Regulations nor the Modified Proposed Regulations included model notices. The League strongly recommends that the CPPA create

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.

- **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

We continue to call on the CPPA to clarify the definition of a business. The Modified Proposed Regulations do not define or further clarify the CCPA/CPRA definition of a business. We strongly recommend the final regulations clarify both the threshold criteria and the phrase "doing business in California."

- *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 Modified 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