3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
f: 703.524.1082
nafcu@nafcu.org | nafcu.org

National Association of Federally-Insured Credit Unions

December 5, 2019

The Honorable Xavier Becerra
Attorney General
California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

RE: Proposed Regulations for the California Consumer Privacy Act of 2018

Dear Mr. Becerra:

On behalf of the National Association of Federally-Insured Credit Unions (NAFCU), I am writing in response California Department of Justice's request for comments regarding proposed regulations under the California Consumer Privacy Act of 2018 (CCPA) (Proposed Regulations). NAFCU advocates for all federally-insured not-for-profit credit unions that, in turn, serve over 118 million consumers with personal and small business financial service products. NAFCU's member credit unions support a uniform federal standard, not a patchwork of state privacy laws, to protect their member-owners' data. NAFCU opposes the application of the CCPA to credit unions as they are already subject to the requirements of the *Gramm-Leach-Bliley Act* (GLBA) and are responsible stewards of sensitive consumer data.

State data privacy requirements, including the CCPA, are already creating confusion and leading to daunting compliance considerations for credit unions. In particular, the proposed CCPA regulations create challenging and expensive new obligations and varying standards that will undoubtedly present unnecessary burdens for credit unions and could, in turn, increase costs for consumers. Credit unions already comply with privacy requirements under the GLBA, yet the Proposed Regulations add overlapping and confusing requirements that would result in substantial additional compliance costs. NAFCU supports a comprehensive federal data privacy standard that builds on existing requirements under the GLBA, preempts state privacy laws, and protects consumers' information instead of a patchwork of state laws that could establish conflicting requirements, cause confusion, and significantly increase compliance costs for credit unions.

General Comments

The mounting uncertainty and rising compliance burdens related to data privacy protection from state regulators imposes undue burden on credit unions, especially those credit unions that operate across multiple states. Credit unions should not be subject to potentially 50 conflicting state privacy requirements. NAFCU advocates for a uniform federal privacy standard that would better

protect consumers and preempts state laws, including the CCPA, that pose a significant cost and strategic risk to credit unions.

A patchwork of state privacy standards will undoubtedly result in undue burden for credit unions who already comply with federal privacy requirements, such as the GLBA. The impact of privacy laws in varying jurisdictions would also lead to a chilling effect on the products and services credit unions are able to offer to consumers. Accordingly, NAFCU supports a federal privacy law that protects consumers, holds all entities accountable, and recognizes existing federal privacy laws financial institutions follow. NAFCU advocates for the following six principles to be included in a federal privacy law:

1. A comprehensive national data security standard covering all entities that collect and store consumer information.
2. Harmonization of existing federal laws and preemption of any state privacy law related to the privacy or security of personal information.
3. Delegation of enforcement authority to the appropriate sectoral regulator. For credit unions, the National Credit Union Administration (NCUA) should be the sole regulator.
4. A safe harbor from liability for businesses that takes reasonable measures to comply with the privacy standards.
5. Notice and disclosure requirements that are easily accessible to consumers and do not unduly burden regulated entities.
6. Scalable civil penalties for noncompliance imposed by the sectoral regulator that seek to prevent and remedy consumer injury.

Moreover, the Proposed Regulations do not address the numerous compliance issues present in the CCPA. Instead, the Proposed Regulations impose varying procedural requirements for a covered "business",[1] which could include credit unions to follow when making disclosures or handling consumer requests, or complying with the anti-discrimination provisions of the CCPA.[2] In particular, the Proposed Regulations provide procedures for notice of right to opt-out for the sale of personal information (PI).[3] Because credit unions generally do not sell PI, they should not be impacted by the opt-out requirements. Nonetheless, the implementing regulations of the CCPA should clarify the definition of "sale" so that credit unions have a clear interpretation of CCPA compliance requirements. Moreover, the Proposed Regulations fail to address interpretations of unresolved issues, which must be clarified so organizations can work towards compliance, such as the various exemptions contained in the CCPA.

Exemptions Under the CCPA

Despite the CCPA's failure to offer exemptions that apply to organizations, NAFCU maintains the position that the CCPA should not apply to credit unions. In the alternative, the California Attorney General should establish implementing regulations that clarify that the requirements of the CCPA and its implementing regulations do not apply to organizations that solely collect GLBA-covered

[1] Section 1798.140(c) of the CCPA.
[2] *See*, Sections 999.312, 999.336 and 999.337 of the Proposed Regulations.
[3] *See*, Section 999.306 of the Proposed Regulations.

information. Further, implementing regulations should clarify that organizations subject to the GLBA that collect CCPA-covered information should be able to comply through a regulatory regime that works in tandem with the GLBA, rather than an entirely separate, parallel framework which will be confusing for consumers and overly burdensome to credit unions.

The Proposed Regulations establish procedures for providing required notices and processing requests from consumers; however, the Proposed Regulations have not addressed a more foundational issue regarding which organizations must comply with these requirements. There is no discussion of how the various exceptions contained in the CCPA will be implemented. The CCPA provides exceptions to certain personal information already subject to state or federal regulation.[4] These exceptions apply to types of information, not types of businesses or industries; as a result, even if a business qualifies for one of the exceptions, it will only be partially exempted for the specific types of information it collects. For credit unions, the CCPA exempts personal information subject to the California Financial Information Privacy Act (CFPA) or the GLBA.

Many credit unions only collect the personal information necessary to provide their members with the products and services they offer. In these situations, all of the information collected by these credit unions would be subject to the GLBA, qualifying for the exemption under the CCPA. It is not clear whether such a credit union would still meet the definition of a "business" in the CCPA as the credit union would not collect any "personal information" that is not excepted from the law. For credit unions in this common scenario, it is unclear whether they must comply with any of the CCPA's requirements.

Because the Proposed Regulations do not discuss any of the CCPA exemptions, credit unions seeking to rely on the GLBA exemption, or any other partial exemptions contained in the CCPA will be forced to specifically request interpretations by the California Attorney General regarding their obligations. As a result, covered credit unions will either suffer unnecessary burden by incurring substantial costs to comply with the CCPA despite the fact that the information they collect is exempt or be forced to request and wait for duplicative clarifications from the California Attorney General's office. NAFCU opposes the application of these requirements to information that credit unions collect that is already subject to the CFPA or the GLBA.

The implementing regulations for the CCPA need to clarify existing exemptions under the CCPA statute. Specifically, for financial institutions, the implementing regulations should recognize the CCPA's exemption for information collected pursuant to the GLBA and clarify how it applies to covered financial institutions. This guidance should separately address compliance for credit unions that do and do not additionally collect information that falls outside of the GLBA's scope.

The Notification Process of a Consumer's Rights

The Proposed Regulations do not establish sufficient rules and procedures for compliance with the CCPA's notice provisions. The privacy policy and notice requirements under the Proposed Regulations create confusion and additional burdens for covered credit unions and their members

[4] *See e.g.,* Section 1798.145(e) of the CCPA.

because the Proposed Regulations: (1) do not address the exceptions for financial institutions under the GLBA, and (2) create multiple notice requirements for information they presently provide under the GLBA.

Disclosure Requirements

The disclosures under the Proposed Regulations would require covered credit unions to provide detailed notice about the information collected on consumers. Credit unions are already subject to federal privacy laws such as the GLBA and have processes in place to inform consumers about the sharing of their data. Under the GLBA, a credit union is already subject to the following privacy requirements:

- Must provide initial and annual notice of its privacy policies to its customers, both members and nonmembers, and any other consumer if his or her data will be shared with nonaffiliated third parties; and
- Must allow the consumer to opt out of the disclosure of the consumer's nonpublic personal information to a nonaffiliated third party if the disclosure occurs outside of certain exceptions in the regulations.

Despite the fact that credit unions already provide detailed notice under the GLBA, Article 2 of the Proposed Regulations imposes an expanded disclosure requirement regarding information collection and privacy policies.[5] The Proposed Regulations do not offer any clarification as to how a credit union which is covered by GLBA that still collects information outside of the GLBA's scope should reconcile the detailed privacy notice required by that law with the additional, detailed notice required by the CCPA. Only information that is not already subject to the GLBA is covered by these notice provisions in the CCPA, therefore, it would appear that a credit union would be in compliance if it were to draft a Privacy Policy that only covered the information that falls outside of the GLBA. However, such a policy could hardly be called a comprehensive description of the credit union's privacy policies. As written, the proposed regulations do not give proper effect to the GLBA exemption in the CCPA and create notice and disclosure requirements that are confusing and ambiguous and will not serve to give consumers easily understandable information.

The CCPA allows the California Attorney General to add "any exceptions necessary" to ensure that notices provided to consumers are easily understood.[6] The Proposed Regulations should exempt credit unions subject to the GLBA from further disclosure requirements if they are in compliance with the GLBA and their existing annual privacy notice is posted on the credit union's website. The distinction between GLBA-covered information and CCPA-covered information is not one that consumers will instinctively identify and providing consumers with multiple, detailed privacy disclosures will only be confusing and frustrating for them.

If the California Attorney General is not willing to provide an exception for these credit unions, it must provide guidance as to how these credit unions can comply without requiring duplicative

[5] Section 999.305(b) of the Proposed Regulations.
[6] Section 1798.185(a)(6) of the CCPA.

notices or unnecessarily burdening the credit union industry. For credit unions already providing detailed privacy policy disclosures, such a requirement should make reference to the inclusion or addition of information to existing notices, rather than requiring separate, free-standing disclosures which will only serve to confuse consumers and place unnecessary compliance burden on credit unions. A separate, free-standing notice would require covered businesses to undertake a separate and new disclosure process, creating additional compliance burdens for entities, like credit unions, that already have to provide privacy disclosures to consumers under the rule.

Moreover, the Proposed Regulations include several subcategories of privacy notices that a business must provide, including notice that must be provided regarding the right of a consumer to "opt-out" of the *sale* of PI.[7] The CCPA exempts from its definition of "sale" the processing of PI in certain specific contexts; however, these exemptions are ambiguous and could likely lead to confusion and higher compliance costs. The Proposed Regulations do not clarify the ambiguities of the definition of "sale" under the CCPA. Although, many credit unions do not "sell" member data information and would not have to comply with the notice requirements for sale of information under the CCPA, those credit unions seeking to rely on the several exemptions would benefit from additional clarification on their operation and application, including on the definition of "sale." Providing such clarification through implementing regulations would allow businesses to rely on clear exceptions they are entitled to under the law, while reducing the risk of erroneous uses of the exceptions.

Handling Consumer Requests

The Proposed Regulations' designated methods for receiving requests is overly prescriptive and not appropriately tailored to the reality of current online systems utilized by businesses. These requirements for methods to submit a request to know or a request to opt-out include a mandatory interactive webform. For requests to opt out, this webform must be accessed through a link entitled "Do Not Sell My Personal Information," or "Do Not Sell My Info" on the business's website or mobile application.[8] Additionally, the Proposed Regulations requires businesses who collect information online to include mandatory user-enabled privacy controls, such as a browser plugin or privacy setting for opt-out of the sale of information collected.[9]

These mandatory, technical requirements for online mechanisms may be appropriate for large technology firms and multinational organizations; however, they are not appropriate for smaller organizations like credit unions. The provision would require a significant number of credit unions to do a complete overhaul of their online or mobile banking platform to include an "interactive webform via the website or mobile application" or "user-enabled privacy controls." Many credit unions have internally developed their online and mobile banking platforms, so such an overhaul would require substantial time and resources and likely disrupt these services for members.

NAFCU is generally opposed to prescriptive technological requirements as opposed to flexible parameters that allow credit unions to choose what works best for their membership and is within

[7] Section 999.305(a)(4) of the Proposed Regulations.
[8] Section 999.305 of the Proposed Regulations.
[9] *Id*.

their budget. Credit unions, as not-for-profit, member-owned financial institutions have very limited resources to make such drastic changes to their digital platforms. NAFCU strongly objects to this portion of the Proposed Regulations.

Further, regarding requests to opt-out, credit unions are already required by the GLBA to provide an opportunity to opt-out of having a consumer's information shared with nonaffiliated third parties. It would be easiest and most streamlined for consumers to make an opt-out request for the sharing or sale of their information at the same time, rather than making such a request at one time and method for GLBA-covered information and at a separate time and method for non-GLBA covered information. It would be less confusing for consumers and less burdensome on credit unions if GLBA-covered institutions could offer the opt-out of sale at the same time and in the same manner as is provided for in the GLBA.

Non-Discrimination Requirements

The Proposed Regulations' anti-discrimination provisions prohibit a business from discriminating against a consumer because they exercise their rights under the CCPA, including denying goods or services, charging different prices or rates, and providing a different level or quality of goods or services.[10] Specifically, the text of the Proposed Regulations require a business to quantify and justify a price differentiation to support that the differing pricing is not a result of consumers exercising or not exercising CCPA rights but rather reasonably related to the value of the data.[11] Credit unions often offer differential pricing for a variety of reasons. Where credit unions collect information beyond what is necessary to offer a good or service to a member, it is often for the purpose of internal marketing, rather than for external sale.

Credit unions that choose to offer differential pricing for the purposes of obtaining information for internal marketing would face undue burden and associated costs to comply with this requirement, including additional research, learning a new market, and obtaining third-party valuations of data being used internally. The requirement of calculating the value of consumer data for differential pricing should not apply where data would only be used internally and with a consumer's informed consent. As such, NAFCU requests that the implementation regulations of the CCPA provide an exception for differential pricing in connection with data that is collected for internal purposes.

Extension of Moratorium

NAFCU understands that, per statute, the CCPA becomes operative on January 1, 2020 and there is a moratorium on enforcement by the Attorney General until the earlier of six months after the publication of the final regulations or July 1, 2020. However, given ambiguities in the law, the need for additional guidance and the significant difficulties associated with reconciling the requirements for GLBA-covered entities, coupled with the need to develop procedures and update disclosures for the new consumer rights (which cannot commence until the regulations are finalized), warrants a delay in enforcement. Although NAFCU objects to the applicability of the

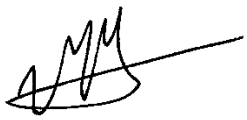
[10] Sections 999.301 and 1798.125 of the Proposed Regulations.
[11] Sections 999.307(b)(5) and 999.308(b)(4) of the Proposed Regulations.

CCPA to credit unions, NAFCU and its member credit unions request an additional delay in enforcement actions by the California Attorney General[12] to help ease the burden of compliance.

Conclusion

NAFCU appreciates the efforts of the California Department of Justice to gather substantive feedback on the Proposed Regulations but opposes the applicability of the CCPA to credit unions. Credit unions are already subject to the GLBA and take great care to safeguard the integrity of their members' personal data and provide notice regarding the sharing of that data. NAFCU cannot support varying state data privacy laws that add potentially conflicting and unnecessary burdens on credit unions. The CCPA and the Proposed Regulations add new obligations and varying standards for compliance that would create mounting and unrealistic compliance obligations for credit unions and confusion for consumers. Moreover, the Proposed Regulations do not address the variety of exceptions under the CCPA statute, including exceptions under the GLBA. Credit unions want to continue to protect their members by following the robust privacy requirements set forth in the GLBA. Ultimately, a comprehensive federal data privacy law that preempts all state privacy laws would better protect consumers and provide more certainty for credit unions.

Sincerely,



Mahlet Makonnen
Regulatory Affairs Counsel

[12] Section 1798.185(c) of the CCPA.