American Bankers Association
Building Success. Together.

CALIFORNIA BANKERS ASSOCIATION
A DIVISION OF THE WESTERN BANKERS ASSOCIATION

CaliforniaMBA
Advocacy. Education. Connection.

MBa
MORTGAGE BANKERS ASSOCIATION

December 6, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: <u>California Consumer Privacy Act of 2018 – Proposed Rulemaking Comment Letter</u>

Dear Attorney General Xavier Becerra:

The American Bankers Association (ABA), the California Bankers Association (CBA), the California Mortgage Bankers Association (California MBA), and the Mortgage Bankers Association (MBA) appreciate the opportunity to submit written comments in response to the proposed rulemaking undertaken by the California Department of Justice pertaining to the California Consumer Privacy Act of 2018 (CCPA).

ABA is the voice of the nation's $18 trillion banking industry, which is composed of small, regional and large banks. Together, America's banks employ more than 2 million men and women, safeguard $14 trillion in deposits and extend more than $10 trillion in loans.

CBA is a division of the Western Bankers Association, one of the largest banking trade associations and regional educational organizations in the United States. CBA advocates on legislative, regulatory and legal matters on behalf of banks doing business in the state of California.

California MBA is a California corporation operating as a non-profit association that serves members of the real estate finance industry doing business in California. California MBA's membership consists of approximately three hundred companies representing a full spectrum of residential and commercial lenders, servicers, brokers, and a broad range of industry service providers.

The Mortgage Bankers Association is the national association representing the real estate finance industry, an industry that employs more than 280,000 people in virtually every community in the country. Headquartered in Washington, DC, the association works to ensure the continued strength of the nation's residential and commercial real estate markets; to expand homeownership; and to extend access to affordable housing to all Americans. MBA promotes fair and ethical lending practices and fosters professional excellence among real estate finance employees through a wide range of educational programs and a variety of publications. Its membership of over 2,200 companies includes all elements of real estate finance: mortgage companies, mortgage brokers, commercial banks, thrifts, REITs, Wall Street conduits, life insurance companies, and others in the mortgage lending field.

As your office prepares to issue final regulations in accordance with the CCPA, we respectfully urge that you consider the following requests to clarify aspects of the proposed regulations and the CCPA. These requests should not be considered an effort to undermine the CCPA but rather they are intended to assist in clarifying aspects of the law as a means to enhance compliance for financial institutions.

ARTICLE 2: NOTICES TO CONSUMERS. (SECTIONS 999.305-999.308).

➢ **Notice at Collection of Personal Information. (Section 999.305).**

Section 999.305(a)(3) of the draft regulations requires explicit consent to use a consumer's personal information for a purpose that was not specifically included in the required notice provided to the consumer at the time of collection. Pursuant to Civil Code Section 1798.100(b) of the CCPA, the only requirement in these scenarios is to deliver another notice that is compliant with the same notice to provide a consumer when information is first collected. As such, there is no additional statutory requirement that the business obtain the explicit consent from the consumer, as now required in the proposed rule.

Accordingly, we believe that this provision impermissibly amends the statute in place of implementing the intent of the Legislature. Moreover, this requirement creates a conflict between the statute and the regulations. A financial institution that provides notice consistent with the requirements of the law may nonetheless be charged with violating the statute because the regulations provide that a "violation of these regulations shall constitute a violation of the CCPA, and be subject to the remedies provided for therein." Given that this concept of obtaining explicit consent for the use of a consumer's personal information for a new purpose goes beyond the text of the CCPA, we request that it be removed.

➢ **Notice of Right to Opt-Out of Sale of Personal Information. (Section 999.306).**

Section 999.306(d)(2) requires businesses to treat as an opt-out any collection of personal information where a "Do Not Sell My Personal Information" button is not present. Under Civil Code Section 1798.100, a business must notify consumers of the purposes for which their personal information is collected and cannot use the personal information for additional purposes without providing notice.

According to Civil Code Section 1798.120(b), a business that sells consumers' personal information to third parties must provide notice to a consumer before selling that consumer's personal information. Civil Code Section 1798.135(a) requires that a business must add a "Do Not Sell My Personal Information" link to the business's Internet homepage and disclose the potential for sale in its privacy policies. As provided for in Civil Code Section 1798.135(a)(5), once a consumer opts-out of the sale of the consumer's personal information, the business must wait for at least 12 months before requesting that the consumer opt back in. Further, the CCPA provides additional protections to consumers who choose to opt-out of the sale of the consumer's personal information.

The requirements under the CCPA are clear. The regulations, however, make it less clear by imposing a new requirement on businesses that do not sell personal information. Under the CCPA, a business that does not sell information at the time information is collected from a consumer may later sell that information provided the consumer is first provided with a notice indicating that information may now be sold to third parties.

Treating a no-notice exemption at the time of collecting the information as an automatic opt-out, as contemplated in Section 999.306(d)(2), is inconsistent with the intent of the CCPA opt-out provision, and otherwise creates further ambiguity in how those automatic opt-outs should be treated under the CCPA (for example, how the business must treat the 12 month no-solicitation period). Since this provision in the regulation is inconsistent with the corresponding provision in the CCPA, and given that consumers are adequately protected by existing law, we request that these provisions be removed from the regulations.

- **Privacy Policy. (Section 999.308).**

Civil Code Section 1798.130 acknowledges that the online privacy policy constitutes notice at collection. Separately but relatedly, disclosures required by Civil Code Section 1798.100 must be provided in accordance with the requirements contained within that section. Requiring businesses to provide additional forms of individual notice, as described in Section 999.305(a)(2)(e), is inconsistent with the statute. Accordingly, only compliance with the provisions within Civil Code Section 1798.130(a)(5) addressing the online privacy policy can be required for advance notice. Businesses that include the advance notice in their online privacy policies are in compliance with the statute.

The proposed regulations regarding the privacy policy require businesses to match specific pieces of information with their specific uses and disclosures. This requirement is excessive and doesn't meaningfully aid transparency. Under the existing CCPA, cross-referencing is only required for personal information that is sold. Civil Code Section 1798.115 treats information that the business sold differently from both the personal information that the business collected and the personal information that the business disclosed for a business purpose. Further, as it relates to personal information that is sold, Civil Code Section 1798.115(a)(2) states specifically, that the business must disclose "the categories of third parties to whom the personal information was sold, by category or categories of personal information for each third party to whom the personal information was sold." This different treatment is a logical consequence of the fact that the statute gives consumers the right to opt-out of sale. A consumer exercising that right has an interest in knowing which information is sold to which third party. Because there is no right to opt-out of the collection or sharing of personal information for a business purpose, a lower level of granularity will provide a less complex and more meaningful disclosure to the consumer.

ARTICLE 3: BUSINESS PRACTICES FOR HANDLING CONSUMER REQUESTS. (SECTIONS 999.312-999.318).

- **Responding to Requests to Know and Requests to Delete. (Sections 999.313).**

Section 999.313(c)(5) requires that a business must specifically disclose the basis for denying a request to know or a request to delete if the denial was based on a conflict with federal or state laws or an exception to the CCPA. This is understandable. However, Section 999.313(d)(6)(c), applicable to a denial of a request to delete, provides that the business is not permitted to use the consumer's personal information for any other purpose than provided for by that exception. This restriction improperly prevents a business from using the consumer's personal information for other lawful purposes including fighting fraud or even completing a consumer's transaction if that reason was not included in the denial letter. Accordingly, we request that these provisions be removed from the regulation.

Section 999.313(d)(1) requires that where a business cannot verify the identity of a requester seeking deletion, the business shall instead treat the request as a request to opt-out of the business selling the consumer's personal information. This form of automatic opt-out is inconsistent with the CCPA and could have the unintended consequence of opting out consumers who do not wish to opt-out of sales. Further, if the request is not from the named consumer, such a requirement could lead to businesses opting out the wrong consumer infringing on the rights of consumers who have not choosen to opt-out from a sale.

The CCPA goes into great length to explain and reiterate that the consumer's right to opt-out requires an affirmative act by the consumer. Examples of the law's intent may be found in Civil Code Sections 1798.120 and 1798.135. If a requestor's identity cannot be verified, all that should be required is notifying the requestor, stating that more information is needed for verification. Since this provision in the proposed regulation is inconsistent with the corresponding provision in the CCPA and since consumers are adequately protected by existing law, we request that this provision be removed from the regulations.

Section 999.313(d)(2) provides three methods of complying with a consumer's request to delete their personal information: permanently and completely erasing, de-identifying, and aggregating. In complying with Section 999.313(d)(4), a business apparently must specify the manner in which it has deleted personal information by identifying one of these three methods. This requirement is burdensome, confusing, and irrelevant to consumers and we request that it be removed.

- **Requests to Opt-Out. (Section 999.315).**

Section 999.315(e) requires that a business must act on a consumer's request to opt-out of the sale of their personal information in no more than 15 days. This period of time is significantly less than the time period provided to a business responding to a request to know or delete (45 days). Where a consumer makes an opt-out request, particularly a consumer who has authorized another person to opt-out of sale on their behalf, this proposed 15-day deadline fails to provide sufficient time to confirm that the individual making the request has the proper authorization. We request that this provision be removed or the time extended to 45 days.

Section 999.315(f) requires a business to (i) notify all third parties to whom it has sold the personal information of the consumer within 90 days prior to the business's receipt of the opt-out request, (ii) instruct them not to further sell the information, and (iii) notify the consumer when this has been completed. This requirement is inconsistent with the corresponding provisions in CCPA, wherein a business is only required to cease selling the information it has collected from the consumer. There is no corresponding provision in the CCPA that the business takes further action and notify all third parties in this regard. Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this section be removed from the regulations.

Proposed regulations have introduced a new method for a consumer to opt-out that is not included in the CCPA. The concept of "user-enabled privacy controls" in Section 999.315(g) is entirely new. In this regard, the regulations recognize the use of "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information…" This new requirement is inconsistent with the CCPA.

Existing law has established robust provisions on how a business must message the consumer's right to opt-out and provides acceptable methods to evidence the consumer's intent to opt-out. Moreover, there has been no opportunity to assess the meaningfulness of this concept or the value that this may offer to consumers. In addition, businesses may not be able to comply with this new requirement if there is no technological capability to track or respond to such browser plugins or similar mechanisms.

Since this provision in the regulation is inconsistent with the corresponding provision in CCPA and given that consumers are adequately protected by existing law, we request that this provision be removed from the regulations. In the alternative, we request that the effective date of this provision be delayed, thereby allowing businesses the opportunity to investigate the current technological status of the functionality of user-enabled controls, and an opportunity to make adjustments to ensure they can comply with the provision.

- **Training: Record-Keeping. (Section 999.317).**

Section 999.317(g) of the proposed regulations expand record-keeping obligations for businesses that buy, receive, sell or share the personal information of four million or more consumers. For companies who meet this threshold, the regulation requires releasing consumer request metrics in the business's privacy policy or posted on their website. This mandate is not derived from the existing law and does not benefit consumers. Nor do the regulations provide any guidance relating to the calculation of the four million consumers.

We urge that this provision be removed from the regulations or alternatively that these metrics not be released publicly in privacy policies, but instead be provided to your office upon request. Should this provision remain, the regulations should clarify that businesses are required to calculate the 4 million threshold and compile metrics based on consumers who have the right to make requests under the CCPA. Including consumers who are not eligible to make requests, as a result of existing CCPA exemptions, skews the results in a manner that would make the results meaningless.

- **Requests to Access or Delete Household Information. (Section 999.318).**

While the draft regulations in Section 999.318 attempt to offer guidance with respect to requests to know or delete personal information for "households," we remain concerned with these requirements.

While we support the clarification that a business may comply with an individual request for household personal information by providing only aggregate personal information, if the requestor does not have a password protected account, the proposed regulations still expose individuals to the release or deletion of their personal information without their knowledge and consent. Aggregation is helpful but is not sufficient to protect people if the household consists of only two or three people.

Moreover, the proposed regulations do not address how the business should respond if the requestor has a password protected account. The implication is that if the requestor has a password protected account, the business must provide the household personal information to the requestor, or delete household personal information. Likewise, we believe it is virtually impossible for a financial institution to determine whether all members of a household jointly request access or deletion, without a level of investigation into a particular household that would be extraordinarily burdensome—if not impossible. Our members are concerned about the transient nature of households – spouses may separate, or adult children may return or leave the household – and there is no practical method for a financial institution to determine the makeup of the household when a request is received.

For these reasons, we urge the deletion of "household" from the definition of "personal information." We believe the unauthorized disclosure or deletion of personal information by one household member is an unintended consequence of the CCPA.

If the final rule does not delete "household" from the definition of personal information or otherwise exempt businesses from disclosing personal information or deleting personal information for a household, we respectfully request that the final rule create a safe harbor from liability if the business follows the procedures in the final regulation regarding verification of requests for access to or deletion of household personal information.

We would further request additional clarity as to the aggregate data that must be provided to the requesting household. It seems that the household information to be disclosed pursuant to this provision is that which applies to, and subject to inspection by, the household as a whole. It is not intended to include specific categories or pieces of information pertaining to a specific individual consumer residing in that household.

ARTICLE 4: VERIFICATION OF REQUESTS. (SECTIONS 999.323-999.326).

➢ **Provide additional clarity around what is necessary, and what will be deemed in compliance, when authenticating a verifiable consumer request and include a safe harbor. (Sections 999.323-999.325).**

As part of routine transactions with consumers, financial institutions collect personal information in order to facilitate customer requests. Furnishing personal information to consumers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetrate fraud and identity theft.

A business receiving a consumer's request will need sufficient data from the consumer as a safeguard to ensure the information provided in return is associated with the requesting individual. Regulations established by the Attorney General should provide flexibility for a business to decline a consumer's request where the data presented by the consumer is insufficient to authenticate a request. Further, in circumstances where limited information is provided by the consumer, a business endeavoring to authenticate a request should have flexibility, but not be required, to furnish non-sensitive personal information (excluding personal information that if disclosed would otherwise result in a data breach) to the consumer as a means to satisfy its compliance and to protect the consumer against fraud and identity theft.

We believe that a safe-harbor from liability should be granted to businesses that satisfy the criteria adopted pursuant to the promulgated regulations, or situations where the evidence shows the business was justified to use the degree of due diligence it did in verifying the identity of the requestor. Financial institutions generally have been quite capable in identifying false requests for information. Limiting the tools institutions can use to protect consumers' personal information from false requestors will not promote consumer protection.

Section 999.325(b)-(c) requires that businesses provide two tiers of authentication for requests for rights to know, depending on whether the request is for categories or specific pieces of personal information. This two-tiered requirement imposes additional burdensome implementation requirements beyond the statute and we request that this two-tiered system be optional or removed from the regulations.

Section 999.325(c) requires that consumers must furnish a signed declaration under penalty of perjury to submit a request for specific pieces of personal information. We request additional clarity as to the purpose of this requirement and guidance on what will satisfactorily constitute a signed declaration under the penalty of perjury.

REQUESTS FOR CLARITY PRESENTLY NOT INCLUDED IN DRAFT REGULATIONS.

- **Request standardized, uniform disclosures for CCPA-mandated notices.**

Provisions within the CCPA and the proposed regulations require specific disclosures and also require specific information to be included in such notices (i.e. Sections 999.305-999.308). In an effort to promote consumer understanding with the requirements and protections of the CCPA that may lead to informed consumers, we request the Attorney General provide sample disclosures associated with the notices and disclosures required under CCPA that businesses may voluntarily elect to use in order to achieve compliance. Such continuity will allow consumers to more easily gain an understanding of the purpose of the notices, and, more importantly, easily identify the distinctions between businesses in what personal information is collected, retained and how it is treated. Additionally, these model disclosures will assist businesses, particularly smaller businesses, in achieving compliance. Voluntary use of these disclosures should also create a safe harbor to businesses using these template disclosures.

- **The "lookback" period should commence January 1, 2020. (Section 1798.130).**

As currently written, the CCPA appears to apply retroactively by requiring businesses to provide information subject to a consumer's request covering the time period prior to the Act's effective date and prior to publication of implementing regulations. We believe rulemaking should clarify that the 12-month lookback period provided for in Civil Code Section 1798.130 applies from the operative date of the CCPA, thereby precluding its application to activities occurring before January 1, 2020.

- **Affirm that the CCPA does not apply to a covered entity's intellectual property and that a business is not required to reveal data infringing on the rights of others.**

In subdivision (a)(3) of Section 1798.185, the CCPA grants the Attorney General authority to establish "any exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights, within one year of passage of this title and as needed thereafter."

In this regard, we urge rulemaking that establishes an exception from the Act for intellectual property or for data that, if disclosed, would have an adverse effect on the rights or freedoms of others. The CCPA should not apply to information that is the protected intellectual property of a business, including information subject to copyright, patent, service mark and/or trade secret protections. A business should not be required to disclose any information that is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique, or process developed to process or analyze personal information, or any information derived from such process or analysis.

In considering this request, your office may wish to consider the approach taken in the European General Data Protection Regulation (GDPR) which places reasonable limitations on the consumer privacy right it grants. Both the intellectual property exclusion and the avoidance of infringement on the rights of others are embedded in the GDPR. We believe that there should be similar recognition in the CCPA of circumstances where a business' attempt to comply with a consumer's request would place it in the position of violating the rights of others or placing it in jeopardy with its competitors.

Given the authority granted to your office pursuant to subdivision (a)(3) of Section 1798.185, we request that the final regulations affirm that intellectual property should not be disclosed in response to a verifiable consumer request.

- **Grant an 18-month delayed effective date with respect to the regulations.**

We urge your office to specify a later effective date for the regulations, such as 18 months after the final regulations are issued. When the CCPA was enacted, businesses were granted 18 months from the legislation's passage to its effective date. This period of time was granted recognizing the complexity of the CCPA, the potential for additional statutory revisions given the speed for which the CCPA was advanced through the Legislature, and was an acknowledgment of the time necessary for businesses to develop compliance protocols to implement the statutory provisions.

Financial institutions have been actively engaged in due diligence and establishing policies and procedures for compliance with the CCPA. The regulations will require financial institutions to re-evaluate their policies and procedures and adapt where necessary. In order to revise any policies and procedures, financial institutions will require additional time to establish and test compliance procedures.

The authority for such as action may be found in Government Code section 11343.4(b)(2). That section provides that the agency issuing regulations can specify an effective date. In furtherance of this request, Section 11343.4(b)(1)'s limitations on an agency's ability to specify an effective date does not apply and that limitation only applies when the statute specifies an effective date.

Since the CCPA does not specify an effective date for the regulations and simply specifies that regulations should be adopted by July 1, 2020, with no reference to an effective date, we request an effective date for the regulations of no earlier than January 1, 2022.

Thank you for the opportunity to provide commentary on this rulemaking. We welcome any questions you may have regarding our letter.

Sincerely,

Kathleen C. Ryan

Kathleen C. Ryan
Vice President and Senior Counsel
American Bankers Association

Kevin Gould
SVP/Director of Government Relations
California Bankers Association

Susan Milazzo

Susan Milazzo
Chief Executive Officer
California Mortgage Bankers Association

Pete Mills
Senior Vice President, Residential Policy &
Member Engagement
Mortgage Bankers Association