February 25, 2020

Ms. Lisa B. Kim, Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013
privacyregulations@doj.ca.gov

RE: California Consumer Privacy Act of 2018 – Revised Rulemaking Comment Letter

Dear Ms. Kim:

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 revised rulemaking undertaken by the California Department of Justice pertaining to the California Consumer Privacy Act of 2018 (CCPA). We appreciate revisions that have been made to the initial draft regulations released on October 11, 2019, that are responsive to the comments we submitted in our December 6, 2019, letter.

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. While our letter makes several specific observations regarding the revised regulations, as a general matter, we urge that final regulations avoid inconsistencies with the CCPA, such as the provision in Section 999.315, requiring companies to provide a method of consumer opt-out that does not exist within the current law, and, moreover, that businesses not be required to provide notifications that may confuse consumers and obfuscate relevant information.

The requests outlined below should not be considered an effort to undermine the CCPA but are rather intended to assist in clarifying aspects of the law to better facilitate compliance by financial institutions.

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

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

Revised regulations in Section 999.305(a)(4) require that when a business collects personal information from a consumer's mobile device for a purpose that the consumer would not reasonably expect, the business must provide the consumer a just-in-time notice summarizing the categories of personal information being collected and a link to the full notice at collection. We request this provision be removed or that the regulations clarify when the collection is for purposes a consumer would not reasonably expect.

Pursuant to Civil Code Section 1798.100(b) of the CCPA, a business must inform consumers, at or before the time of information collection, as to the categories of personal information that will be collected and the purposes for which that information will be used. Should this change—i.e. the business wishes to collect a different category of personal information or use information collected for a different purpose—the business must provide consumers with an updated notification that reflects the change before information collection. As currently proposed, Section 999.305(a)(5) of the draft regulations require much more than the updated notification required by statute. Specifically, under Section 999.305(a)(5), a business that seeks to use

previously collected personal information for a purpose materially different from the purpose previously disclosed must first obtain the consumer's explicit consent for the new purpose.

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.

In addition, the revised regulations have further confused the notice at collection requirements. Section 999.305(a)(3) has been revised to require that the notice be made "readily available" and it is unclear what the new language means. The proposed regulation does not specify that the notice must always be given in the same location and manner that the information is being collected, but the "illustrative examples" suggest that this may be the case, which is extremely difficult, if not impossible, to comply with.

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

Revised regulations in Section 999.308(c)(1)(e)(2) require a business to match each category of personal information collected with the categories of third parties to whom information was disclosed or sold. This requirement is excessive and does not meaningfully aid transparency.

Civil Code Section 1798.115 treats information that the business collected and sold differently from personal information the business simply collected or personal information the business collected and disclosed for a business purpose. Under the CCPA, cross-referencing is only required for personal information that is collected and sold.

Specifically, 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 category of third parties 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. The same cannot be said for a business's information collecting or sharing activities given that a consumer's right to opt-out does not extend to these activities. Applying the same level of granularity to information that is collected and shared needlessly complicates the disclosure. This is likely to cloud the facts that are most relevant to the consumer, such as, the categories of third parties to whom the personal information is sold.

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)(3), as proposed in October 2019, provided that a business shall not provide a consumer with specific pieces of information if the disclosure created "a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks." The revised regulations have deleted this requirement. We request that the deleted language be reinserted.

Without the ability to withhold specific pieces of particularly sensitive information, like usernames and out-of-wallet information, sending responses, for example, in plain text via postal mail as the CCPA allows consumers to request, puts customers and their financial records at risk if a hacker or other bad actor makes the request fraudulently or intercepts the response. Credential stuffing and identity theft is already a security problem, and businesses need the ability to withhold actual data where necessary to protect consumers from fraud.

In the place of the requirement to withhold information that could present a security risk, the revised regulations propose a new exception to the requirement to fulfill consumer requests. While this new exception in Section 999.313(c)(3) is helpful, we are uncertain whether a business will ever be able to satisfy all the conditions in (a)-(d), particularly the requirement in Section 999.313(c)(3)(c) that the business does not use personal information for any commercial purpose. In addition, Section 999.313(c)(3)(b), does not permit a business to retain personal information for internal record-keeping purposes, analytics or quality assurance. We request additional clarity as to these new provisions.

Further, in retaining section 999.313(c)(3) and subsections (a)-(d), we request clarity on how the provision would apply. As written, the revised provision would excuse a business from requiring it to provide or delete information if the information is not, "in a searchable or reasonably accessible format." We appreciate that the Attorney General recognizes that we cannot provide or delete the information if a business cannot search for it. It further provides, however, in the conjunctive, that all conditions must be met, meaning the business maintains the information only for legal or compliance reasons, does not sell or use it for commercial purposes, and describes for consumers the categories of records that were not searched. What is not clear is, if the information is not searchable, how the other conditions will apply. Perhaps applying this in the disjunctive "or" would resolve this ambiguity, or otherwise further explanation of how this would apply is needed.

Revised regulations proposed in Section 999.313(d)(6) pertain to cases where a business denies a consumer's request to delete personal information. New language added to Section 999.313(d)(6)(a) is confusing and onerous. Proposed language requires that a business inform the consumer that it will not comply with the consumer's request to delete and that the business

must describe the basis for the denial, including when the business has applied an exception to the CCPA or where there is a conflict with federal or state law.

This new language in Section 999.313(d)(6)(a) conflates two concepts: (1) the application of the statutory exceptions and (2) the actual denial of a request to delete, for instance because a request cannot be verified. If a business deletes information that does not fall into one or more exceptions, but keeps information it is permitted to retain under the CCPA, it has complied with the request. Similarly, if a business after a review of searchable databases, determines that it does not hold personal information of the consumer in such databases, the business has not denied the request. In these situations, a business should not be subject to new and onerous response requirements.

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.

- **Service Providers. (Section 999.314).**

The revised rule now provides at section 999.314(c)(3) that a service provider may retain, use, or disclose personal information obtained in the course of providing services for "internal use by the service provider to build or improve the quality of its services, *provided that the use does not include building or modifying household or consumer profiles, or cleaning or augmenting data acquired from another source.*" (emphasis added). This may be inconsistent with CCPA section 1798.140(v) (definition of "service provider") whereby a service provider is permitted to use the personal information to fulfill the terms of the contract, and where a contract may allow or require a service provider to use the information to clean or augment the data acquired from another source. We ask that the language in this subsection allow for a service provider to use the information in accordance with its contract.

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

Section 999.315(f) 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 business 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 business 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 extended to 45 days.

Section 999.315(f) also requires a business that sells a consumer's personal information to notify those third parties to whom it has sold the personal information that the consumer has exercised their right to opt-out and instruct them not to sell that consumer's information. 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. Under the CCPA, the business in not required to take the additional, burdensome step of contacting third parties and instructing them to cease selling the consumer's personal information. 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 proposed regulations.

The proposed regulations have introduced a method for consumers to opt-out that is not included in the CCPA. The concept of "user-enabled global privacy controls" in Section 999.315(g) is entirely new. In this regard, the regulations recognize the use of "user-enabled privacy global controls, such as a browser plugin or privacy setting, device 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 includes robust provisions establishing how a business must communicate a consumer's right to opt-out and provides acceptable methods to evidence the consumer's intent to opt-out. It is unclear why these carefully considered provisions should be augmented by adding new, largely unproven opt-out channels without first assessing their effectiveness and consumer value. In addition, businesses may not be able to comply with this new requirement without the 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 and test the effectiveness of user-enabled controls, and should it be necessary an opportunity to make adjustments to ensure they are positioned to comply with the provision.

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

Revised regulations pertaining to record-keeping proposed in Section 999.317(e) include an express prohibition on sharing information maintained for record-keeping purposes with any third party. This new requirement directly conflicts with a central goal of the regulations, which is to permit record sharing with regulators. Particularly for highly regulated financial institutions, a prohibition on sharing records with third parties, such as state and federal regulators, agencies, and other parties who request them via lawful process is untenable. We request this new provision be removed.

Section 999.317(g) of the proposed regulations expand record-keeping obligations for businesses that buy, receive, sell or share the personal information of ten million or more consumers. For companies that meet this threshold, the regulation requires publishing consumer request metrics in the business's privacy policy or website. This mandate is not derived from the CCPA and does not benefit consumers. Nor do the regulations provide any guidance relating to the calculation of the ten million consumers. We urge that this provision be removed from the regulations or alternatively that the requirement to publish these metrics be replaced with a requirement that they be provided to your office upon request.

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

Revised regulations in Section 999.318 reflect improvements for requests to know or delete personal information for "households." We continue to have significant concern with these requirements. Operationally, it will be impossible to ascertain who occupies a residence on a given date, how to identify an intent to submit a joint request and whether anyone age 13 or younger is a household member.

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.

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 to verify the consumers identity 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.

Further, the new requirement added in Section 999.323(d) that businesses not charge consumers for proper identity verification is overbroad and needs refinement. Paired with the example highlighted in the revised regulations, this new language effectively discourages the use of notaries, which is a commonly accepted legal method for authenticating the identity of an individual. The Uniform Statutory Form Power of Attorney (California Probate Code Section 4401) even references the attachment of a required notary certification.

When read in tandem with Section 999.326(b), which explicitly references the Probate Code's requirements as a means for businesses to streamline the verification of authorized agents, the new text in Section 999.323(b) creates an unnecessary barrier to consumer choice and a direct conflict with Section 999.323(e)'s requirement that businesses "implement reasonable security measures to detect fraudulent identity-verification activity and prevent the unauthorized access to or deletion of a consumer's personal information."

Businesses required to ensure the security of the personal information they are tasked with disclosing or deleting should not be penalized for employing a separately required method for authenticating legal affidavits signed by consumers. We recommend that the regulations make clear that use of a notary to verify the identity of the consumer does not trigger a monetary penalty to businesses looking to secure personal information when a consumer chooses to exercise his or her rights under the CCPA.

Section 999.325(b)-(c) appears to identify two potential distinct 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 approach imposes additional burdensome implementation requirements beyond the statute. We request that this two-tiered system be optional or removed from the regulations.

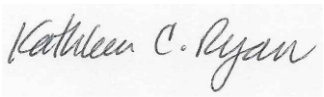
Section 999.326(a) outlines procedures for verifying a request sent by an authorized agent. The revised proposal states that the business may require the consumer to provide "written and signed" permission to the agent. The regulations should clarify what is meant by "written and signed." Additional clarity is need regarding verification. Specifically, the proposal states that a business may also require the consumer to verify their own identity directly with the business. If the business requires the consumer to verify their own identity, the regulations should clarify that the 45-day period to respond to the request does not begin until the business makes contact with the consumer (and not from the date the request is received from the authorized agent).

CONCLUSION

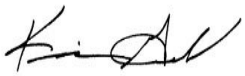
We appreciate the opportunity to comment on the proposed revisions to the draft regulations released in October 2019. With this comment letter endeavoring to focus on the revised provisions to the draft regulations, we respectfully wish to redraw your attention and underscore comments we included in our letter dated December 6, 2019. In addition to the comments provided herein, we urge that the final regulations: provide sample notification forms; clarify that the 12-month lookback period in Civil Code Section 1798.130 applies from January 1, 2020; exempt from the Act trade secrets and intellectual property, including data that, if disclosed, would impede the prevention and detection of fraud or the authentication of an individual; and, grant an 18-month implementation period for the final regulations.

Thank you again for the opportunity to comment. We welcome any questions you may have regarding our letter.

Sincerely,



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



Kevin Gould
SVP/Director of Government Relations
California Bankers Association

Susan Milazzo
Chief Executive Officer
California Mortgage Bankers Association

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