AFSA
Protecting Credit Since 1916
American Financial Services Association

California Financial Services Association
1127 11th Street, Suite 400
Sacramento, CA 95814
Phone: 916-485-1554
E-Mail: cfsacfl@aol.com
www.californiafsa.org
CFSA

December 6, 2019

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: CCPA proposed regulations

On behalf of the American Financial Services Association ("AFSA")[1] and the California Financial Services Association ("CFSA"),[2] thank you for the opportunity to provide comments on the regulations proposed by the Office of the Attorney General ("OAG") to implement the California Consumer Privacy Act ("CCPA"). We appreciate your consideration of our comments during the preliminary rulemaking process and reiterate our previous concerns about vague terms and the substantial burdens these regulations place on covered entities.

We appreciate the OAG's efforts to provide guidance to businesses on how to comply and to clarify the law's requirements through the implementing regulations. However, though our members share the state's goal of protecting the privacy of consumers, promoting understanding by consumers of the personal information about them that is collected, sold, and shared for a business purpose, and guarding personal information from unauthorized access, we have significant concerns about the regulations as proposed. There are certain areas where we believe consumers and the business community would benefit from increased clarity and certainty.

Enforcement Delay

Although the effective date and issues of enforcement are not addressed directly in the proposed regulations, our members believe that some clarity in this area is warranted. The CCPA was largely effective on September 23, 2018, and will be operative on January 1, 2020, and enforceable by the OAG on July 1, 2020. It appears that the OAG intends for the regulations to also be enforceable on July 1, 2020, which is likely to be the earliest date that the regulations could be made effective. A delayed enforcement date would give affected businesses the opportunity to evaluate the specific requirements set forth in the regulations and implement new systems and processes needed to be fully in compliance with the law.

---

[1] Founded in 1916, the American Financial Services Association (AFSA), based in Washington, D.C., is the primary trade association for the consumer credit industry, protecting access to credit and consumer choice. AFSA members provide consumers with many kinds of credit, including direct and indirect vehicle financing, traditional installment loans, mortgages, payment cards, and retail sales finance. AFSA members do not provide payday or vehicle title loans.

[2] The California Financial Services Association is a non-profit trade association representing major national and international corporations and independent lenders with operations in the State of California to provide a broad range of financial services, including consumer and commercial loans, retail installment financing, automobile and mobile home financing, home purchase and home equity loans, credit cards, and lines of credit.

In addition, we request that the OAG include in the final regulations a statement to the effect that any enforcement actions will be based on conduct that takes place after the statutory enforcement date of July 1, 2020, or such later date as the regulations may become enforceable. In making this request, we note that the proposed regulations address all the major aspects of the CCPA: how to provide notices, content of the privacy policy, the process for handling submitted requests, verification, and calculating the value of consumer data. Without having final regulations in place to govern compliance, businesses lack clarity that the solutions they are readying for January 1, 2020, will, in fact, meet regulatory requirements. We request that businesses have all the applicable rules and requirements, in final form, with a reasonable timeframe to achieve compliance, before their actions can be determined to be unlawful. Recognizing the time necessary for the OAG to draft and implement comprehensive regulations, we believe that the outlined enforcement delay would be consistent with the legislature's intended delayed enforcement date.

§ 999.301. Definitions

Section 999.301(h) broadly defines "household" as *a person or group of people occupying a single dwelling*. Such a broad definition based merely on temporary occupancy of a dwelling rather than a requirement that persons be related and domiciled, as defined in Section 17014 of Title 18 of the California Code of Regulations, would sweep in groups in living arrangements who should not have access to the personal information of others, such as multiple roommates linked by mutual tenancy, a landlord and tenant, persons using a house sharing app for the weekend, and at the most extreme end, all the residents of a college dormitory. Because this broad access would be contrary to the purpose of the CCPA, we recommend striking the requirement that businesses accept requests from household members—except those from a parent or guardian on behalf of a minor—or, at the very least, that persons whose only relationship is that they share a housing unit should not be included in the definition of household. Instead, we recommend that the OAG consider adopting a definition of household similar to the definition of "family group" used by the U.S. Census Bureau, which defines a family group as "any two or more people (not necessarily including a householder) residing together, and related by birth, marriage, or adoption." [3]

Section 999.301(n) provides a definition of "request to know" that includes *any or all of* six categories of information. Section 999.313 describes different processes depending on whether a consumer is requesting specific pieces of information or categories of information. Providing this kind of flexibility was not envisioned in the statute, and many of our members have already started building solutions that do not afford multiple choices of this kind. We request that the OAG clarify that this multi-tier approach is not mandatory and confirm that businesses that build their process to meet the more conservative requirements associated with a request for specific pieces of information will be in compliance with the law.

§ 999.305. Notice at Collection of Personal Information

This section describes a comprehensive, detailed consumer notice, which suggest there may be a specific form notice the OAG might want covered entities to use. If the OAG intends to be more

[3] https://www.census.gov/programs-surveys/cps/technical-documentation/subject-definitions.html#familyhousehold.

prescriptive regarding the notice requirements, then we request it release a sample form and that the use of such sample form of notice provide a safe harbor for compliant businesses. As many covered entities are likely already working on their own notice in advance of the impending compliance date, we request that notices substantially similar to the sample form notice also be deemed compliant.

Both the statute and the proposed regulation require a collecting business to notify consumers of the categories of personal information to be collected and the purposes for which they will be used. The statute specifies that disclosures required by section 1798.100 must be provided in accordance with the requirements of section 1798.130. The only part of section 1798.130 that a business can look to for instruction on providing the advance notice is section 1798.130(a)(5), which specifies the information that must be in the online privacy policy. Accordingly, businesses that rely on their online privacy policies to provide advance notice should be considered in compliance with the statute. We request that the OAG remove any language from the draft regulations that suggests otherwise.

Section 999.305(a)(2) requires a business present a notice that is "understandable to an average consumer."[4] While we support the goal of clear communications to consumers, the proposed standard is vague and requires additional guidance. If the OAG does not intend to provide a sample notice, we request a clearer and more measurable standard.

Section 999.305(a)(3) requires a business to obtain explicit consent from the consumer to use personal information for a new purpose that may not have been originally disclosed. This requirement goes beyond the existing statutory requirements, which require only notice, and as noted above, could be provided through changes to the online privacy policy. Further, a requirement to obtain explicit consent for new uses would unnecessarily encourage covered entities to draft broad disclosure language that would cover as wide a range of uses as possible. Such disclosures would be longer and less meaningful for consumers seeking to truly understand how their personal information may be used.

Section 999.305(d) restricts the sale of personal information collected from a source other than the consumer unless the business provides a notice at collection to the consumer or contacts the source, but this requirement has no statutory basis in the CCPA and is overly burdensome for businesses that share any information with third parties.

§ 999.306. Notice of Right to Opt-Out of Sale of Personal Information

Section 999.306(a)(1) arguably suggests that a business that does not currently sell personal information must, nevertheless, build an intake function to collect opt outs from consumers who would like to prevent their personal information from being sold in the future.[5] This is an unreasonable outcome for businesses that do not sell and could create a perverse incentive for businesses to decide to sell since they must build the opt-out infrastructure regardless of their

[4] This same terminology is repeated in §§ 999.306, .307, .308, and the comment applies equally to each section.

[5] Stating that "the purpose of the notice of right to opt-out of sale of personal information is to inform consumers of their right to direct a business that sells (or may in the future sell) their personal information to stop selling their personal information, and to refrain from doing so in the future."

current practices. Further, recognizing that the statute does not speak to such a requirement, the OAG should remove from the proposed regulations all such forward looking obligations.

Section 999.306(b)(2) requires a business that *substantially* interacts with consumers offline to also provide the opt-out notice by an offline method. This vague standard does not define what qualifies as substantially offline to trigger the offline notice requirement.

§ 999.307. Notice of Financial Incentive

We request confirmation that businesses that do not offer financial incentives or a price or service difference in exchange for retention or sale of a consumer's personal information do not have to provide the Notice of Financial Incentive or related information in the privacy policy.

§ 999.308. Privacy Policy

Section 999.308(b)(1)(c) requires that the privacy policy include a description of "the process the business will use to verify the consumer request." For security reasons, this requirement should be removed. Describing the process for verification invites fraudsters to circumvent the measures that businesses must put in place to protect consumers. There is minimal additional consumer benefit to publishing the details of how the verification process works when businesses have a legitimate concern that providing too much information in a publicly facing document will put consumer security at risk.

We recommend removing Section 999.308(b)(1)(d)(2), which requires that the privacy policy include for each category of personal information collected, the categories of sources from which each category was collected, the business or commercial purpose for collecting each category, and the categories of third parties with whom the business shares each category of personal information. This disclosure requirement is overly burdensome, requiring businesses to specifically tie source, use, and recipients to each category of personal information collected, to no good effect, and attempts to impose a requirement on all personal information collected when the statute specifies that this degree of granularity only applies to personal information that the business has sold.[6]

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. Section 1798.115(a)(2) specifically states with regard to the personal information sold 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 collection or sharing for a business purpose, a lower level of granularity will provide a less complex and more meaningful disclosure to the consumer.

[6] Section 1798.110 of the statute lists four categories of information that a business must provide regarding personal information the business has collected. Unlike Section 1798.115, this section does not require that the categories be cross-referenced against each other. In fact, cross-referencing the categories would create a lengthy and confusing document.

Section 999.308(b)(3) requires that the privacy policy for all covered entities disclose that a consumer has a right to opt-out of the sale of their personal information. If a business does not currently sell personal information, it should not be required to include such a disclosure in its privacy policy. The exemption provided in 999.306(d)(1) only applies if the business's privacy policy states that the business "does not and will not sell" the personal information. Without the forward-looking statement, a business that does not currently sell personal information would be required to provide the notice of opt out. This disclosure would be unnecessary, irrelevant to the business, and may lead consumers to wrongly believe that the business does in fact sell personal information when it does not.

Section 999.308(b)(5)(a) requires that a privacy policy explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf, but the proposed regulations do not make clear the level of information that a business must provide regarding the designation. For example, it is not clear whether a business must describe the requirements regarding agent request verification found at § 999.326, or whether they may be covered when a request is made. It is also unclear whether businesses may require particular forms or indicia of authority, such as powers of attorney.

§ 999.312. Methods for Submitting Requests to Know and Requests to Delete

Section 999.312(f) assigns to businesses the responsibility for redirecting responses that are not submitted through established channels and for advising a consumer how to remedy a deficient request. The section raises practical questions regarding the requirements for timing and tracking and should be removed.

The statute requires that a business implement at least two methods for submitting requests and, importantly, provide notices to consumers explaining how to make requests. Requests submitted outside of the options provided cannot be addressed in an efficient fashion, creating risk that the business cannot meet the deadlines established by the statute. For example, a request e-mailed to a local branch may not be timely routed to the appropriate location for response, but a business has limited options when it cannot provide a response within the 45 days allowed under the statute.[7] Without the ability to control how requests are submitted, businesses may be challenged both to provide the extension notice within 45 days and to provide the response within 90 days.

§ 999.313. Responding to Requests to Know and Requests to Delete

§ 999.313(c)(5) requires a business, when a request to know is denied based on a conflict with federal or state law, to disclose to the consumer the basis for the denial. There may be times when the precise legal basis cannot be provided to the consumer because such a disclosure would itself violate law. To avoid this potential scenario, we suggest that the OAG include language in this paragraph clarifying that disclosing the existence of the conflict, without detailing the particular law or exception at issue, will be an adequate response under the regulation.

[7] The regulation specifies that a business must respond to a request within 45 days, beginning on the day the business receives the request. If necessary, the business "may take up to an additional 45 days to respond to the consumer's request, for a maximum total of 90 days from the day the request is received." § 999.313(b).

Section 999.313(c)(6) requires a business to use reasonable security measures when transmitting personal information to the consumer. Our member companies recognize the importance of protecting personal information when it is being transmitted, and we request that compliance with this requirement constitute a safe harbor to any cause of action that alleges that the transmission resulted in unauthorized access, acquisition, destruction, modification or disclosure of personal information. Understanding that some consumers may choose to have their personal information delivered by mail, we request that the OAG confirm that delivery through the mail at the request of the consumer absolves the business of liability for any unauthorized access, acquisition, or disclosure of personal information that may occur after the personal information is placed in the mail. Moreover, we request that the OAG confirm that using security measures that the business uses in standard operating procedures, such as e-mail encryption and Secure Message Delivery, will meet this requirement and constitute reasonable security procedures and practices under the CCPA.

Section 999.313(c)(7) states that if a business maintains a password-protected account with the consumer, it may comply with a request to know by using a secure self-service portal. We request verification that while a financial institution subject to the Gramm-Leach Bliley Act (GLBA) may use the secure portal for this purpose, it would not be required to deliver non-GLBA data through the consumer's GLBA account portal.

Section 999.313(d)(1) requires that if a business cannot verify the identity of a requestor seeking deletion it shall instead treat the request as a request to opt out of sales. This requirement has no statutory basis, and, in fact, runs counter to the CCPA's principles by giving control over consumer data based on unverified requests. The CCPA treats the right to delete and the right to opt out of sale of personal information as separate requests, with different statute sections and different exceptions. There is no legal basis to convert a deletion request to an unrequested, unrelated action because the requestor's identity could not be verified. If an identity cannot be verified, the only required action should be to inform the requestor of that fact.

Section 999.313(d)(3) allows a business to delay compliance with a request to delete, where personal information is stored in an archive or backup, until the archive or backup is next accessed. This requirement fails to recognize the technological complexity of database systems and the purpose of archives and backups. Information is generally archived with an established destruction date, determined by the type of data, when a business needs to retain it to meet business or legal requirements and maintain compliance with other state or federal laws. Backups, primarily used for disaster recovery, may never be accessed but may be overwritten on a regular schedule to retain current information. Without more clarity around the word "access," this language could require deletion when unrelated information is automatically added to the database or the database is accessed for purposes of maintenance or recovery.

A requirement to delete triggered by any access to the archive or backup is overly burdensome for businesses, as the next access to the archive or backup may be for unrelated information and not for the specific personal information requested. Accessing the archive or backup for other business needs wholly unrelated to the data subject to CCPA should not trigger a deletion requirement. We request that the deletion requirement for personal information in an archive or

backup system only trigger in the event that the business accesses such data with the intent to use it in the course of its day to day functions.

Section 999.313(d)(4) requires that a business specify the manner in which it has deleted the requestor's personal information. This requirement is burdensome, vague, and has no statutory basis. Deletion of information, especially in large businesses, can be complicated, involving several systems and business units, and a detailed description of this process does not serve the consumer. We recommend that this section only require a business to inform a consumer that the personal information has been deleted, or if it cannot be deleted, the reason why, consistent with the requirements of Section 999.313(d)(6).

§ 999.318. Training; Record-keeping

Section 999.317(g) requires a business that alone or in combination, annually buys, receives for the business's commercial purposes, sells, or shares for commercial purposes, the personal information of 4,000,000 or more consumers to compile certain metrics regarding consumer requests and publish these metrics in the business' privacy policy. This section provides no further guidance as to how the 4,000,000 consumer threshold is calculated. We request that the OAG provide such guidance and that the guidance clarify that the calculation should not include consumers whose information is exempt from the CCPA's disclosure and deletion requirements, such as information subject to the Gramm-Leach Bliley Act, as including such information would skew the results and make the data effectively meaningless. Additionally, the public disclosure of these metrics would not further the purposes of the CCPA and could present fraud or cybersecurity risks. Instead, we recommend that these metrics be provided to the OAG upon request.

§ 999.318. Requests to Access or Delete Household Information

Section 999.318(b) requires a business to disclose or delete personal information for all members of a household if jointly requested. Businesses will not, however, be able to verify whether all members of a household agree to the request, particularly because the business has no practical way to know who all the members of the household are and to verify whether a request was actually received from all members. The broad definition of household members, in that it includes individuals of all ages and physical or mental capacity, regardless of relationship, means that a business can never be certain that a request to disclose or delete is made with appropriate authority. As a result, businesses cannot respond affirmatively to such a request, and this provision should be removed from the regulations.

§ 999.325. Verification for Non-Accountholders

Sections 999.325(b)-(d) require different tiers of authentication for right to know requests depending on the specific categories of personal information requested, but most identity verification techniques do not know how many data points will be needed for verification ahead of time, and most third party verification services do not provide this level of differentiation. The multiple verification tiers could increase the potential for mishandling consumer information. The regulations should allow businesses to instead set their own verification standards based on the business' own assessment.

Section 999.325(c) requires that consumers must submit a signed declaration under penalty of perjury to submit a request for specific pieces of personal information. We request further clarification regarding standards for these declarations, including whether the declaration must be notarized.

Accessibility and Language Requirements
The regulations require throughout—999.305(a)(2)c-d; 306(a)(2)c-d; 307(a)(2)c-d; 308(a)(2)c-d—that notices and privacy policies be accessible to customers with disabilities and available in the languages in which the business provides contracts, disclaimers, notices, sales, or other information. For businesses to have more certainty, the OAG should provide some additional clarity on the requirements for accessibility. For example, the regulations should clarify that if the documents are provided on a website that meets accessibility standards such as Web Content Accessibility Guidelines (WCAG) 2.0, it meets this requirement. We further request that the OAG provide additional clarity regarding how to apply the language requirement. For example, financial institutions may take assignment of installment sales contracts negotiated in other languages. Such contracts should not drive the languages for the financial institution's notices and policies, particularly if the underlying contracts are subject to the GLBA exemption.

Deletion Requests in a 12-month Period
The CCPA, in providing consumers with the right to request their personal information, recognized that identifying and supplying personal data to the consumer places a burden on businesses. The statute requires the business to provide the information not more than twice in a 12-month period.[8] The information must be provided at no charge to the consumer.[9] If, however, the consumer makes more than two requests, the business can opt to charge the consumer for the administrative costs of fulfilling the request or refuse to take action if the requests are manifestly unfounded or excessive.[10] This language suggests that more than two requests in a 12-month period can be considered excessive, and a business is not required to take action.

The CCPA does not expressly state that a consumer can only make two deletion requests in a 12-month period. However, for a business, the process of validating a consumer request, searching for personal information, evaluating whether the information is subject to an exception, deleting or destroying data, and responding to the consumer is not less burdensome than the effort that a business must put into responding to a disclosure request, and may actually be more burdensome. Accordingly, we request that the OAG clarify in the regulations that delete requests should be treated in the same manner as disclosure requests, and no more than two in a 12-month period should be required.

Look Back Period
The CCPA provides that a response to a disclosure request "shall cover the 12-month period preceding the business's receipt of the verifiable request."[11] A business also must include in its

[8] 1798.100(d), 1798.130(b).
[9] 1798.100(d); 1798.130(a)(2).
[10] 1798.145(g)(3).
[11] 1798.130(a)(2).

online privacy policy "the categories of personal information it has collected about consumers in the preceding 12 months."[12] This reference to a 12-month look back period is repeated in several other sections of the CCPA as well.

As noted above, the CCPA provides that the law is generally "operative" on January 1, 2020, notwithstanding that many sections became effective immediately upon enactment. The enforcement date adds additional confusion. The various dates for implementation raise questions about how the look back period should be treated when the law becomes enforceable. The OAG's regulations should clarify that the look back period will not extend farther back than the effective date of the regulations because businesses will not have final and binding guidance for complying with their requirements until that date.

For example, a business is only required to respond to a disclosure request after receiving a verified request. A business cannot receive a verified request until the OAG regulations specify how businesses will determine that a request is valid. Additionally, in response to a disclosure request, a business must identify the information collected in the past 12 months by reference to the definition of personal information.[13] However, the OAG's final regulations may modify or expand the definition of personal information and unique identifiers.[14] As a result, businesses will not be able to fully identify and categorize information until final regulations are published. Accordingly, businesses should not be required to look back beyond the effective date of the regulations to respond to a disclosure request.

Thank you in advance for your consideration of our comments. If you have any questions or would like to discuss this further, please do not hesitate to contact Matt Kownacki at AFSA at (202) 469-3181 or mkownacki@afsamail.org.

Sincerely,

/s/ Matthew Kownacki
Matthew Kownacki
Director, State Research and Policy
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006

/s/ David Knight
David Knight
Executive Director
California Financial Services Association
1127 11th Street, Suite 400
Sacramento, CA 95814

[12] 1798.130(a)(5)(B).
[13] 1798.130(a)(3)(B); 1798.130(c).
[14] 1798.185(a).