March 8, 2019

California Department of Justice
ATTN: Privacy Regulations Coordinator
300 S. Spring St.
Los Angeles, CA 90013

Re: CCPA preliminary rulemaking process

On behalf of the American Financial Services Association ("AFSA"),[1] thank you for the opportunity to provide comments and participate in public forums as part of the Attorney General's Office's ("AGO") preliminary rulemaking process for the California Consumer Privacy Act ("CCPA"). We appreciate AGO's efforts to provide guidance to businesses for how to comply and clarify the law's requirements through the implementing regulations.

Though AFSA members share the state's goal of protecting the privacy of consumers, we have significant concerns about the CCPA, as passed by the legislature, due to vague terms and definitions and the substantial burden it places on covered entities.

Vague Terms and Definitions
Throughout the Act, multiple sections fail to provide a definition for a "verifiable customer request" for information. Notably, the term is referenced in sections 1798.100, 1798.105, 1798.115, and 1798.130. The law offers no framework or guidelines under which a covered business may attempt to verify an individual's identity, particularly in the cases of individuals with no formal customer relationships. Will a covered business be punished if its identity verification requirements for requesters are too lax or too stringent? The law also offers no guidance whether a consumer's request for information on behalf of another individual is a "verifiable customer request," or whether a covered business must comply with a request for a minor's information from a parent or guardian. We request that rulemaking clearly defines a "verifiable customer request" for information and outlines the process to verify a customer's identity.

The Act is also vague on how specific the disclosures provided to an individual must be regarding personal information collected and the purposes for which it will be used. The Act does not make clear whether business must disclose only the "categories" or the "specific pieces" of Personal Information about an individual. We request that the rulemaking require only that businesses disclose the categories of Personal Information collected. Such a requirement would be the most helpful way for consumers to understand what information is being collected and would not require the business to aggregate otherwise-segregated or anonymized data and associate it with a specific individual.

1798.105 – Requests for Deletion of Personal Information
This section is vague with respect to the extent of the following deletion exceptions: "reasonably anticipated" within the context of the ongoing business relationship; the "reasonably aligned with the expectations of the

[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.

(individual) based on the consumer's relationship with the business" exception; the "compatible with the context in which the (individual) provided the information" exception; and instances when a requested deletion of Personal Information by a business triggers the no violation of the freedom of speech provisions of the law. Each of these exceptions should be interpreted broadly to ensure minimal disruption of existing customer relationships. Further, the section does not adequately address concerns with the deletion of data used to detect and prevent fraud, which would have troubling consequences for consumers and the economy.

The deletion requirement raises serious concerns regarding information that a business has previously legally acquired in accordance with existing law. Can a state require that a business destroy informational property it has legally acquired that may be of ongoing value to the business? Is this a permissible "taking" of that business asset? If it is permissible, is the business entitled to just compensation from the state for that taken business asset?

1798.115 – Disclosure of Sold Personal Information and Third Party Notice
We request that the rulemaking allow for disclosure using a public website to meet the notice requirements as the categories disclosed are not specific to an individual consumer. Additionally, the section prohibits a third party from selling personal information unless the consumer has received "explicit" notice and is provided an opportunity to exercise the CCPA right to opt-out. Third parties may not have a direct relationship with consumer and may not be able to provide direct notice. As a result, the law may unnecessarily affect the flow of data. As the law is silent to how a third party should receive notice in order to comply with the requirement, we request that the rulemaking allow a third party to rely on its own privacy policy statements or written assurances from first party data providers.

1798.125 Discrimination Based on Exercise of CCPA Rights
The law sets no standard for determining if an extra charge to an individual who exercised CCPA rights is "reasonably related to the value provided by the individual's data." The law fails to define an "unjust, unreasonable, coercive or usurious" financial incentive practice. What happens if an individual who provides the required opt-in to a financial incentive later revokes that consent after he/she has received the financial incentive benefits?

Businesses are required to provide individuals with a clear website opt-out link, but the law fails to specify whether this is the only means by which an individual may opt-out. Would a business be required to honor an opt-out request if an individual contacts any part of a business, anywhere in the world, and makes a request? Could a California resident stop a seasonal sales associate in a Portland, Maine retail store and give her/his opt-out request for Personal Information held by that company? Like other privacy law opt-outs, the individual should be required to use the designated communication process described in the notice given to the customer.

1798.135 – Internet Home Page
The law requires that a business "respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale of the consumer's personal information." If a business changes its financial incentive offerings pursuant to 1798.125, would the business be allowed to provide notice of the new incentives to an individual within 12 months of the decision to opt-out?

1798.140 Definitions
(c) Business
Nonprofit organizations, including political parties and campaign organizations, are excluded from the definition and the law's requirements. The definitions used for commonly controlled businesses typically use a 25 percent threshold (e.g., the federal Bank Holding Company Act), but this law defines control using 50

percent. The controlled entities provision only brings in other entities that have at least 50 percent common ownership AND also share a common brand.

(d) Business Purposes
Are the seven listed examples a comprehensive list of the activities within the definition and its triggered exemptions?

(g) Consumer
This is a misleading term, as the definition is any individual, and is not limited to the type of interaction with a business—ex. personal, family or household use (consumer) or business (commercial)—and the individual need not be a customer of the business. The definition of "Consumer" should not include employees, who already have extensive personal data protection under state and federal employment laws.

The definition incorporates the California income tax definition of a California income taxpayer, which creates numerous problems and fails to consider several situations. What if the individual is a California taxpayer but all the interactions between the individual and the business take place in another state? (ex. a Massachusetts business has an account with a student at a Massachusetts college who provided a Massachusetts address, but is a California taxpayer) What if the individual was not a California taxpayer in the last completed tax year and the tax analysis for the current year, which is based on actions in the entire current year, cannot yet be completed? What if the individual was a California taxpayer in the last completed tax year and moved out of state right after that tax year ended? What if the individual was not a California taxpayer in the last completed tax year and moved to California immediately after that tax year ended? What if the individual believes they are not a California taxpayer and the California income tax authority later establishes they were a California taxpayer? In this same situation, what if the California taxpayer appeals that decision in court? A better test would be an individual who has provided a California mailing address to the business, similar to the federal Gramm-Leach-Bliley law.

(h) Deidentified
What does "cannot reasonably identify" mean?

(j) Device
This definition should not include an object that is capable of being connected to another object, but not connected to the internet (ex. a keyboard attached to a computer with no internet connection).

(o) Personal Information
This definition includes any information connected to a "household," but that term is not defined. Do household members have to be related? Does it include a college dormitory or multiple tenants cohabitating in an apartment?

The definition broadly includes information that is "capable of being associated" to a person or household, even if the business has never contemplated making that connection. Would this make information that a business never associated with a specific individual, and never intends to try and associate with an individual, but which could possibly, with some effort, be associated with a specific individual, within the definition of that individual's Personal Information? Personal Information should be limited to information associated with an identified individual and not a device, a household or a family.

The exclusion from the protected Personal Information definition for "publicly available information" is limited to government record information. Vast amounts of public information that can readily be obtained—from the

internet or a phone book, for instance—is covered by this law. This exemption should include information readily available to the general public, like other California privacy laws and federal privacy law.
Personal Information should be limited to information collected from an individual and should not include any information related to that person collected from any other source.

(t) Sell, Selling, Sale or Sold
The definition fails to further define "other valuable consideration." Other valuable consideration is vague and could be interpreted to include every mutually beneficial exchange of Personal Information by covered businesses (ex. a community bank gives another small bank a credit reference for no charge, anticipating that they may someday ask that other bank for a credit reference). The definition should be limited to information being provided for monetary consideration.

1798.145 CCPA Limits
(a)(6) Conduct Outside of California
Without access to geolocation data a business cannot determine if information collected via mobile phone or a portable personal computer was collected while the individual was in California. If an individual in California attempts to shield their location from the business (ex. through use of a virtual private network (VPN)), and the business has no other indication the individual is in California, will the business be in violation of the law if it collects or sells that information? This also raises questions over whether it is constitutionally permissible for California to regulate business that occurs in other states or as part of interstate commerce.

(d) Federal FCRA Exception
The exemption for the Fair Credit Reporting Act exemption only applies to the "sale" of personal information. The term "sale" is defined under the law and requires "monetary or other valuable consideration." "Valuable consideration" is not defined under the law and, as a result, the exemption may not be complete to cover the transfer of personal information from a lender. The furnishing of credit data is not sold to a consumer credit reporting agency. If the CCPA were to be interpreted to not apply to the furnishing of data to a consumer credit reporting agency, it would have significant economic impacts to the credit reporting system. The Attorney General should provide clarification that the "sale of" requirement in the FCRA exemption would apply to the furnishing of information that is not made for monetary consideration.

(f) Federal Driver's License Law Exception
It is not clear exactly what information is covered by this exception. Is it just information that is protected by that law, or does it include any information related to a driver's license that is subject to the law?

(g) Allowed Response Exceptions
The law allows a business up to 90 additional days to respond "where necessary," but the scope of this exception is vague. It is also vague as to what qualifies as a "manifestly unfounded or excessive" request by an individual that allows a business to charge a fee or refuse to comply with the request.

(h) Service Provider Violations
The law does not create a clear standard for when a business hiring a service provider has "reason to believe," but no actual knowledge, that a service provider intends to violate this law, thus making the business liable for that violation.

1798.150 Civil Damages
The civil damages authorized by the law are unreasonably burdensome and guarantee at least $100 to individuals whose personal information was part of an unauthorized access, exfiltration, theft or disclosure, who suffered no harm. These damages would add up very quickly in the event of a large breach or a class action suit

that could involve millions of customers. There are concerns about the constitutionality of imposing automatic punitive damages when there was no harm to the plaintiff(s). For instance, should the unauthorized disclosure of any Personal Information, like a phone number that is publicly available in a phone book, create these rights to an automatic windfall? This allows a court to award an individual up to $750, as well as undefined "other relief the court deems appropriate," despite the individual suffering no harm.

The law fails to define what "cure" is required from the business within 30 days of notice from the individual to avoid liability. Further changes to the law and future regulations should describe what is required to be a sufficient notice to cure and how it should be provided to the business. A cure typically cannot involve undoing the data breach, so the only reasonable interpretation of "cure" would be a fix of the conditions that allowed the unauthorized access, exfiltration, theft or disclosure. We request that the rulemaking verify this interpretation.

There is no express standard or duty regarding what a business has to do to reasonably protect Personal Information, just a penalty for any unauthorized access, exfiltration, theft or disclosure of any Personal Information, regardless of the effect or lack of effect of that event. The California Attorney General has created standards for personal data protection, and compliance with those standards should protect a business from liability, particularly when individuals were not harmed by the unauthorized access, exfiltration, theft or disclosure. This law should use compliance with commonly accepted data security "best practices" standards to protect a business from liability for unauthorized access, exfiltration, theft or disclosure of Personal Information, like Ohio recently enacted with House Bill 220.

1798.155 Attorney General Provisions
As with the previous, this section fails to define what "cure" is required from the business within 30 days of notice from the Attorney General to avoid liability. Since that cure often cannot involve undoing all the effects of a violation, is the required "cure" a fix of the conditions of that violation? We also request that regulations verify that the $7500 amount is a cap on actual damages not an automatic punitive damage award.

1798.185 Attorney General Regulations
The law requires the attorney general adopt regulations to explain how to comply with this new law by July 1, 2020. It allows the attorney general to start enforcement actions beginning six months following adoption of regulations or July 1, 2020, whichever is sooner. This does not allow enough time for businesses to implement the complicated disclosure processes AFTER they are defined by the Attorney General, which could be as late as July 1, 2020, the date businesses are required to be in compliance. The compliance date should be the *later of* six months following adoption or July 1, 2020.

1798.192 No Waiver
It is unclear whether a binding arbitration provision specifically allowed by the Federal Arbitration Act (FAA) violates this prohibition by being an effective waiver of the express right in the law to have court awarded statutory punitive damages. The federal preemption under the FAA requires that the CCPA not limit such binding arbitration provisions.

1798.198 January 1, 2020, Effective Date
Private rights of action for any unauthorized access, exfiltration, theft or disclosure of any Personal Information are allowed on and after January 1, 2020, even if the Attorney General has not yet issued interpretive regulations. Such actions should not be allowed any sooner than the later of six months following adoption or July 1, 2020.

The law does not specify whether businesses will be expected to provide Personal Information pursuant to Section 1798.130(a) for the 12 months preceding January 1, 2020, or if the requirement to track and provide the various categories of Personal Information begins as of January 1, 2020.

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 me at 202-469-3181 or mkownacki@afsamail.org.

Sincerely,

Matthew Kownacki
Director, State Research and Policy
American Financial Services Association
919 Eighteenth Street, NW, Suite 300
Washington, DC 20006-5517