November 8, 2021

California Privacy Protection Agency
Attn: Debra Castanon
915 Capitol Mall, Suite 350A
Sacramento, CA 95814

Re: PRO 01-21 — Preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020

Dear Ms. Castanon:

On behalf of the American Financial Services Association ("AFSA"),[1] thank you for the opportunity to provide comments on the California Privacy Protection Agency's ("Agency") invitation for preliminary comments on proposed rulemaking under the California Privacy Rights Act of 2020 (PRO 01-21). AFSA 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.

Extension of Employee and B2B Exemption

The California Privacy Rights (CPRA) extends the CCPA's partial exemption of employee and business contact data until January 1, 2023. The partial employee exemption specifically exempts personal information that is collected by a business about a person in the course of the person acting as a "job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of" the business to the extent that the personal information is collected and used solely within the employment context. The exemption also applies to personal information used for emergency contact purposes, as well information that is necessary to administer employment benefits. Under the exemption, employers are still required to inform employees and applicants, at or before the time of collection, of the categories of personal information to be collected and the purposes for which the information will be used (i.e., a "notice at collection"). Further, employers are not exempt from the "duty to implement and maintain reasonable security procedures and practices," and employees and applicants retain the private right of action in the event that certain of their personal information is subject to a data breach.

Under the business-to-business exemption, businesses are not required to provide certain notices or extend certain consumer rights to their business contacts. Specifically, the exemption applies to information "reflecting a written or verbal communication or a transaction" between the business and an employee or contractor of another organization (i.e., a business, non-profit or government agency), where the communication or transaction occurs in the context of (1) the business conducting due diligence on that other organization, or (2) the business providing or receiving a product or service to or from such organization.

[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.

The expiration of the exemptions will leave employees, job applicants, employers and individuals serving other businesses in a service provider context confused regarding the interplay between the CPRA and employment laws because most of the rights under the CPRA either are already addressed or do not make sense in the employment or B2B context.

We request that the regulations make the exemptions permanent or extend them to allow for additional time to comply. This would be in line with the approach of other states such as Colorado and Virginia who chose to exclude human resources data from the scope of their privacy laws, along with proposed legislation (e.g., New York and North Carolina) not including employee or B2B data within their purview. It is no surprise these states chose not to include employee or B2B data within their scope because most privacy rights are either already addressed under other existing laws or do not apply in the employment or B2B context. For example, in California, employees already have the right to access their payroll records, their employment agreements and broadly their personnel file. Additionally, under California law, an employer may not "discriminate, retaliate, or take any adverse action against an employee" if the employee decides to correct his or her data by updating or changing "name, Social Security number, or federal employment authorization document." Job applicants may also challenge an employer's decision to deny employment that was erroneously based on a conviction history report. And as a general matter, it is an unlawful practice under California employment laws to discriminate against an employee for opposing any unpermitted practices or exercising his or her rights under the law.

Furthermore, other rights under the CPRA (e.g. right to opt out of the sale or sharing of data and the right to limit the use of sensitive personal information) do not apply in the employment or B2B context. Businesses do not sell employee or service provider data and do not track employees or service providers for targeted advertisements, so there is no need to opt out of selling or sharing. Also, there is no need to limit the use of sensitive personal information because it is collected solely for human resources functions or tax compliance purposes.

If the exemptions are not permanently extend the regulations should align employment and privacy rights in the CPRA regulations by: (1) defining "professional or employment-related information" to mean an employee's personnel file or in a case of a B2B interaction the individuals personal contact information (business information such as work email address, business location, title, etc. should be excluded); (2) clarifying that the right to correct is limited to rectifying objective personal information that can be verified through official documentation, such as correcting a name, an address or other data generally maintained under official government records; and (3) ensuring the CPRA's deletion right does not contradict legal retention obligations under employment or other laws (e.g. California Labor Code § 1198.5 Equal Employment Opportunity Commission regulations, Age Discrimination in Employment Act and Fair Labor Standards Act) requires employers to maintain a copy of each employee's personnel records for a period of no less than three years after termination of employment .

Processing that presents a significant risk to consumers' privacy or security, including cybersecurity audits and risk assessments performed by businesses.

Section 1798.185(a)(15) of the California Privacy Rights Act (CPRA) involves issuing regulations requiring businesses to conduct annual cybersecurity audits and "regular" risk assessments if the business's "processing of consumers' personal information presents significant risk to consumers'

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

privacy or security." In determining whether the processing "may result in significant risk to the security of personal information," the CPRA identifies two factors to be considered: (1) the size and complexity of the business; and (2) the nature and scope of processing activities.

The CPRA's risk assessment requirement is similar to the EU General Data Protection Regulation. Article 35 mandates a data protection impact assessment be carried out in consultation with the data protection officer for processing "likely to result in a high risk," but unlike the CPRA, it does not require DPIAs to be filed with a regulatory authority. While Article 35 identifies particular circumstances where DPIAs are necessary, it also calls for guidance regarding what kind of processing is subject to the DPIA requirement. Both the European Data Protection Board and individual countries, like the U.K. Information Commissioner's Office, have issued such guidance. Such guidance can be instructive to the CPPA as they develop regulations. However, as discussed below, financial institutions are already subject to sufficient regulatory requirements for the protection of consumer data.

The Gramm-Leach-Bliley Act Safeguards Rule (16 CFR 313.1 *et seq*) already sets forth standards for covered financial institutions for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. Additionally, the Safeguards Rule already requires that covered financial institutions routinely audit, test and monitor the risks in order to evaluate and adjust their information security program. Such safeguards ensure that data that presents a heighten risk to the privacy of consumers is appropriately protected. Requiring covered financial institutions to comply with the audit and risk assessment provisions of the CPRA is over-burdensome and unnecessary. Duplicative regulatory burdens resulting in increased costs to consumers without a tangible benefit.

Consumers' right to delete and right to correct.

Right to Delete. Under the CPRA, the "right to delete" seems to remain largely the same except for one notable change—in addition to directing service providers to delete consumer's personal information from their records upon receiving a verifiable consumer request, businesses will also be required to notify "contractors" to do the same, "and notify all third parties to whom the business has sold or shared such personal information, to delete the consumer's personal information, unless this proves impossible or involves disproportionate effort."

What qualifies as "disproportionate effort" is not defined. We request that the regulations provide clarification and guidance regarding what is needed to establish whether deletion is impossible or involves disproportionate effort. At the very least, data that is not stored in a structured database (unstructured data) be explicitly excluded from the requirement to delete.

Right to Correct. Under the CPRA, consumers have a new right to request a business that maintains inaccurate personal information about the consumer correct such inaccurate personal information, taking into the account the nature of the personal information and the purposes of the processing of the personal information. Financial institutions are subject to laws and regulations such as GLBA and the Fair Credit Reporting Act (FCRA), which would exempt much of the information that financial institutions hold from the right to correct. However, we would suggest that the CPRA regulations further clarify and define that the right to correct non-exempt data be limited to data that is not subjective (e.g.

name, address, SSN, etc.). Any type of data that is subjective or cannot be independently verified as true and correct should not be subject to the right to correct.

Consumers' rights to opt out of sharing of their personal information

Sharing. "Sharing" is a new defined term under the CPRA and means "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party *for cross-context behavioral advertising*, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged. The CPRA imposes several additional responsibilities on business that "share" personal information. They must disclose the "sharing" to consumers in their privacy policy, give consumers a way to opt out, and post a "Do Not Share My Personal Information" link on their homepage.

The addition of "sharing" seems directly targeted at online advertising but it is unclear on how it will impact the activities of businesses that use cookies on their websites to track consumers. When consumers use or direct a business to "intentionally interact" with third parties, it is not considered a "sale" or the "sharing" of personal information. Deliberate interactions such as visiting an entity's website or purchasing goods or products from a party may constitute "intentional interactions" as defined in the CPRA. We request that the regulations further clarify and define what the types of intentional interactions that would not be considered "sharing." For example, if a consumer visits a lender's website to view their rates and terms is that an intentional interaction. If that information is shared with Google to display loan ads to the customer, would that be considered "sharing"?

Look-Back Period for Consumer Requests

Although the CPRA does not come into effect until January 1, 2023, consumer requests to access data can "look back" at data collected by a business on or after January 1, 2022. Moreover, for any personal information collected starting January 1, 2022, the CPRA gives consumers the right to make a request to know beyond the CCPA's standard one-year look back. The exception to this expanded right is if such a look-back request would be "impossible" or require "disproportionate" effort. We request that the CPRA regulations define a specific look-back period (e.g. 12 to 24 months) or at the least clarify that business that have purged or cannot otherwise retrieve data using reasonable effort be exempt from a longer look-back period. The Section 1798.145(j)(2) of the CPRA does state that nothing in the CPRA requires businesses to keep personal information for any specified length of time or to retain personal information about a consumer if it otherwise would not in its "ordinary course of business," so the regulations should clarify that businesses are not required to provide information that has been purged or is otherwise not retrievable without unreasonable effort (e.g. data stored in back-up servers).

Sensitive Personal Information

Pursuant to the CPRA, consumers have the right to restrict a business's use of sensitive personal information to, among other things, that use which is necessary to perform the services or provide the goods or services requested; to certain "business purposes" identified in the CPRA; and as otherwise authorized by CPRA regulations. Examples of such business purposes include verifying consumer

919 18th Street NW, Washington, DC, 20006 ▲ 202.296.5544 ▲ www.afsaonline.org ▲ @AFSA_DC

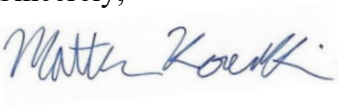
information, fulfilling transactions, providing financing and payment processing, providing advertising and marketing, except for cross-context behavioral advertising. Businesses that use sensitive personal information for purposes other than those specified in the CPRA are also required to provide consumers notice of such use and inform them of their right to limit the use or disclosure of their sensitive information. As with the right to opt out of the sale of personal information under the CCPA, businesses may opt to providing such right through a new, separate link titled "Limit the Use of My Sensitive Information" posted on the business's internet homepage, or, at the business's discretion, utilizing a single, clearly-labeled link that allows a consumer to both opt out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information.

We ask that the regulations clarify that the requirements to allow customers to limit the use of sensitive information and provide customers with an opt-out link be limited to consumer data that is not subject to the GLBA. Furthermore, the rights regarding sensitive information should not be extended to employees or information provided in the B2B context.

Additionally, we request that the regulations exclude employee, job applicant and B2B information form the rights relating to sensitive personal information. Those rights do not apply in the employment or B2B context. Businesses do not sell employee, job applicant or service provider data and do not track those individuals for targeted advertisements, so there is no need to opt out of selling or sharing. Likewise, sensitive personal information is collected solely for human resources functions or tax compliance and not for any other purpose, so there is no need to "limit" the use of such data.

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