sifma

Invested in America

November 8, 2021

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

Re: Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21)

Dear Ms. Castanon:

The Securities Industry and Financial Markets Association ("SIFMA")[1] welcomes the opportunity to respond to the California Privacy Protection Agency ("CPPA") Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 ("CPRA").[2] SIFMA previously provided comments on the Attorney General's rulemaking under the California Consumer Privacy Act of 2018 ("CCPA").[3] SIFMA and its members are strongly committed to the protection of consumer data, privacy, and security, and its members have operated for years under the well-established protections of the Gramm-Leach-Bliley Act. SIFMA is responding to several of your specific requests but is also providing some additional thoughts on what other areas may be ripe for additional guidance from the CPPA.

1. Audits and Risk Assessments

SIFMA members perform audits and risk assessments for many purposes – including privacy and data protection – under various federal and state mandates. SIFMA believes that any additional rulemaking or guidance provided on when a covered business meets the "significant risk to consumers' privacy or security" standard for initiating a risk assessment should focus on factors that should be considered in making this determination, which may align with triggers for other audits or risk assessments. Further, internal audits should satisfy the requirements so long as they meet the audit industry standards, thus balancing the need to provide or obtain relevant information without placing an undue burden on businesses, especially small businesses. In further developing any guidance on audits and assessments, the CPPA should consider implementing requirements similar to the requirements adopted by the New

[1] SIFMA is the leading trade association for broker-dealers, investment banks, and asset managers operating in the U.S. and global capital markets. On behalf of our members, we advocate for legislation, regulation, and business policy affecting retail and institutional investors, equity and fixed income markets, and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

[2] Invitation for Preliminary Comments on Proposed Rulemaking under the California Privacy Rights Act of 2020 (Proceeding No. 01-21) (September 22, 2021), https://cppa.ca.gov/regulations/pdf/invitation_for_comments.pdf

[3] Letter from Melissa MacGregor, SIFMA to The Honorable Xavier Becerra (December 6, 2019), https://www.sifma.org/resources/submissions/proposed-california-consumer-privacy-act-regulations-ccpa-rules/.

York State Department of Financial Services ("NYDFS") under 23 NYCRR Part 500 or Europe's General Data Protection Act ("GDPR") audit requirements. Many SIFMA members are currently complying with such audit and reporting requirements thus making compliance with a similar requirement in California more seamless and efficient in both jurisdictions. Further the NYDFS rules provide sufficient flexibility based on a company's industry, size, locations, activities, etc.

SIFMA does not believe that additional rulemaking is necessary for assessing risks to consumer privacy versus benefits of businesses processing data, but additional guidance may be beneficial for further clarifying how the CPPA expects firms to make those assessments.

2. Automated Decisionmaking

a. Activities deemed to constitute "automated decisionmaking technology" and/or "profiling"

Automated decisionmaking technology has evolved and grown to become an important part of how some companies do business. In regulating the use of that technology, the CPPA should ensure that the CPRA is no more onerous than, and does not conflict with, equivalent requirements under GDPR as these are well-established requirements. The CPPA should limit the scope of the definition to cover only the processing of personal information solely by automated means, without human intervention, that may negatively impact a consumer's legal rights. The definition should not include automated processes that do not impact a consumer's legal rights such as the use of algorithms to flag suspicious transaction activity.

The existing definition of "profiling" under the CPRA does not require additional rulemaking as it is sufficiently clear, but additional guidance on the term may be helpful for covered businesses in interpreting the requirements.

b. Consumer access to information about businesses' use of automated decisionmaking technology and processes consumers and businesses to facilitate access

The CPPA should consider, for ease of consumer use and efficiency, using the same online method for making requests regarding automated decision-making, that the CCPA and CCPA regulations currently provide for regarding access and deletion requests for consumer information.

c. Responding to consumer access requests

When responding to consumer access requests, the CPPA should consider allowing firms to use a consumer-friendly brief description of the logic involved including, for example, the categories of personal information or factors considered and relative consideration given to such categories or factors. The CPPA should also consider allowing covered businesses to use the same categories of personal information as provided for in the CCPA and CCPA regulations, if the covered business determines that it would be helpful for consistency and the consumer's general understanding.

d. Scope of consumer opt-out rights for automated decisionmaking and processes to facilitate opt-outs

In drafting regulations to govern consumers' "access and opt-out rights with respect to businesses' use of automated decision-making technology," care should be taken to narrowly capture the activities within scope of definition of automated decision-making technology. Automated decision-making that is based upon the consumer's consent or is necessary to perform a contract between the business and the consumer should be excluded from the opt-out requirement. This approach is consistent with Article 22 of the GDPR where similar exceptions to the right of a data subject to opt out of automated processing are included. One example of how this exception would operate is where an individual gives their express consent for a loan application which results in a decision that uses automated decision-making technology. Additional areas that should be outside the scope of the consumer's right to opt-out with respect to automated decision-making are fraud and network security concerns, as businesses should be enabled to prevent system attacks and harm to individuals. This exception is also recognized in the GDPR under Recital 71 which permits automated decision-making for fraud purposes as permitted by law.

3. Audits Performed by the CPPA

Audits performed under the CPRA should be reasonably designed to assess a covered business' compliance with the CPRA and should be risk-based. The CPPA should take a principles-based approach including sampling the covered businesses policies, standards and procedures with associated evidence. The CPPA should give ample advance notice to covered businesses including all information requests. Audits should not be performed more frequently than once every three years unless the CPPA has reason to believe the subject company is not complying with the law. The CPPA's information requests should be narrowly tailored such that they are not unnecessarily burdensome to comply with but still provide adequate information to assess the company's compliance with the law, and the CPPA should remain open to a constructive dialog with the business about refining the scope of such requests where appropriate. Such audits should not include reviews of underlying personal information or reviews of any privileged communications or conversations. Further, covered businesses should not be required to give CPPA auditors unfettered access to company systems or data collection applications. Audits should be done in coordination with other regulators whenever possible to avoid duplication. Finally, any findings by the CPPA should be kept confidential and not subject to public information requests as they may contain sensitive information that may put consumers or the covered business at risk.

4. Consumers' Right to Delete, Right to Correct, and Right to Know

The CPRA amended the CCPA to allow consumers to request correction of inaccurate personal information held by covered businesses. Although SIFMA agrees that consumers should have the right to request material corrections of inaccurate information, covered businesses must have the ability to request sufficient information to authenticate the identity of the requesting party to prevent fraud or accidental or unnecessary to changes to information. Further, consumers should only be able to request a correction of their information up to two times per year.

Covered businesses should also be permitted to take any steps necessary to prevent fraud including the misuse or misappropriation of personal information. The CPPA should not set a threshold time period for

a covered business to respond as not all businesses or types of information are the same or as easily accessible. Covered businesses should be granted a reasonable amount of time to respond which would afford businesses the necessary flexibility to triage requests that require immediate attention without sacrificing responsiveness to consumer needs. A business should be permitted to treat a request for correction as a request to delete personal information, particularly where the information is not maintained for critical business operations or the information has been provided via a third-party source.

Additionally, the CPPA might consider limiting the right to correct to only that personal information which the business has collected directly from the consumer or generated through its interactions with the consumer. Finally, covered businesses should have the right to object to or reject a request because the request is impossible, is without basis, or requires a disproportionate effort. Any additional guidance should include examples or circumstances for when covered businesses can lawfully reject those requests or require consumers to provide additional information before complying with those requests. A business that lawfully and appropriately rejects a request for correction should not be required to accept from the consumer a written addendum to the consumer's record. There is simply no reason to require a business to flag a record that the business has determined in good faith (and in compliance with the CCPA) need not be amended.

5. Consumers' Rights to Opt-Out of the Selling or Sharing of Their Personal Information and to Limit the Use and Disclosure of their Sensitive Personal Information

The CPPA should take into consideration the efforts and investments that covered businesses have made to comply with the existing rules and regulations adopted under the CCPA. Any requirements and technical specifications must be reasonably supported by the platforms through which a business collects personal information to avoid covered businesses having to entirely redevelop their existing system. Businesses should not be required to embrace particular technological solutions that introduce unknown reputation, compliance or security risks without (a) safe harbor protections from the CPPA and (b) being afforded ample time to study these solutions and their potential implications for the business.

6. Consumers' Rights to Limit the Use and Disclosure of Sensitive Personal Information

The CPRA includes the right to limit the use and disclosure of sensitive personal information by covered businesses if the sensitive personal information is collected or processed to infer characteristics about a consumer.[4] The scope of "inferences" and the processing of sensitive personal information that can be limited by consumers should be narrowly drawn toward discriminatory, harmful, and unexpected uses of sensitive personal information. Using and disclosing sensitive personal information for purposes that are reasonably foreseeable, or necessary to ensure that a product or service being offered to consumers is operating as intended, is secure, and complies with law, is not inferring information about a consumer and should not be interpreted as such. Moreover, the CPPA should consider refining the otherwise broad scope of "sensitive personal information" to encompass only those elements that are susceptible to inferences and exclude elements that are used for purposes such as identification and verification. For example, the processing of passport numbers, financial account numbers and account credentials is

[4] *See* 1798.121(d)(noting that "[s]ensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is *not* subject to this section.")(emphasis added).

unlikely to give rise to any inferences that cause material harm to consumers. This provision is intended to be narrow in scope, but if the scope is deemed to be broader, then there are various exemptions that may be necessary for covered businesses to be run effectively including responding to court orders or information that be necessary for the security of the covered business.

7. Information to Be Provided in Response to a Consumer Request to Know (Specific Pieces of Information)

In considering regulations implementing how covered businesses must respond to consumer requests for information, the CPPA should take several things into account. First, businesses should not be required to disclose information not accessed by a business during its normal operations (e.g., information recorded on a storage device not readily accessible by the business during its regular operations or encrypted information to which the encryption key is not accessible by the business in its regular course of business). Businesses should also not be required to disclose information that is unreasonably voluminous or requires extraordinary cost.

8. Definitions and Categories

SIFMA and its members believe that "defining the business purposes for which businesses, service providers, and contractors may combine consumers' personal information" is best left to the discretion of businesses and their service providers. In any event, it is important that any definition or guidance put forth by the agency emphasize that the mere act of combining personal information in the same database is not prohibited if the proper access controls are in place. By way of example, the FACTA Affiliate Marketing rule[5] (which prohibits the "use" of eligibility information received from affiliate for marketing purposes) establishes a framework whereby there is no violation of the rule if the affiliate receives the information through a common database but does not use it to make the solicitation. In short, putting personal information in the same place is not (and should not be) a problem. Rather, problems may arise when the holder of the information starts treating the entire data set as one consolidated mass for the holder to do with as it pleases.

* * *

SIFMA appreciates the opportunity to provide these comments to the CPPA. If you would like to discuss this further, I can be reached at mmacgregor@sifma.org.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director and Associate General Counsel

cc: Kim Chamberlain, Managing Director & Associate General Counsel, State Government Affairs, SIFMA

[5] 12 C.F.R. § 41.20 *et seq.*