August 18, 2022

Submitted via email: regulations@cppa.ca.gov

California Privacy Protection Agency
Attn: Brian Soublet
2101 Arena Blvd.
Sacramento, CA 95834

Re: CPPA Public Comment for CPRA Regulations

Dear Mr. Soublet,

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to respond to the California Privacy Protection Agency ("CPPA") Notice of Proposed Rulemaking dated July 8, 2022 (the "Proposed Regulations") that will implement regulations required under the Consumer Privacy Rights Act of 2020 ("CPRA").[2] SIFMA appreciates the work that the CPPA has done to bring public attention to consumer privacy issues and work with companies to achieve a higher level of consumer protection.

SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets, including a significant presence in California. SIFMA has 24 broker-dealer and asset manager members headquartered in California. Further, there are approximately 384 broker-dealer main offices, nearly 40,000 financial advisers, and 93,522 securities industry jobs in California.[3]

SIFMA urges the CPPA to carefully consider the costs associated with potentially overly prescriptive regulations both for businesses and ultimately for customers. We highlight below several proposed requirements which may do little to protect investors but would be costly to comply with. Companies that must comply with the CPRA are already engaged in updating their policies, processes, procedures, contracts, and websites to meet the by January 1, 2023 deadline. Any new obligations in the Proposed Regulations that markedly change or expand upon the

[1] The Securities Industry and Financial Markets Association (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 industry's one million employees, we advocate on 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). For more information, visit http://www.sifma.org.

[2] https://cppa.ca.gov/regulations/pdf/20220708_npr.pdf

[3] https://states.sifma.org/#state/ca

CPRA requirements will create significant unnecessary expenditures of resources for all such companies, while not necessarily aligning with the expectations of the California citizens who voted for the law. The CPPA should avoid creating regulatory mandates that far exceed the requirements of the CPRA, which is itself an expansion of the existing privacy law in California.

Also, SIFMA continues to remain concerned about the potential expiration of the employee and business-to-business ("B2B") data exemptions in the CPRA. If, or when, the exemptions expire, the CPRA and its regulations will apply to employee personal information and personal information belonging to an employee or an individual associated with another legal entity involved in a commercial transaction with a business (e.g., B2B contact details). Applying the CPRA and its regulations to employee and B2B data will create unintended consequences and compliance problems which will be compounded by the new obligations that would be imposed by the Proposed Regulations.

1. Priority Issues

Although we provide detailed comments on a wide variety of issues below, we would like to highlight the following priority issues for your consideration:

- **Notice Regarding Third Party Data Collection** (*See #6 below*): The Proposed Regulations expand the notice at collection requirements to include, among other things, the names of all third parties that a business allows to control the collection of Personal Information ("PI") from a consumer (e.g., through analytics cookies) or, as an alternative, provide the consumer with information about the third party's information handling practices.

- **Restrictions on Additional Uses of PI** (*See #2 below*): The Proposed Regulations specify that a business's collection, use, retention and sharing of PI must be "reasonably necessary and proportionate" to achieve the purpose for which the PI was collected or processed and define this standard in relation to what an "average consumer" would expect when the PI was collected. Any uses that are unrelated or incompatible with the original purpose requires prior explicit consent from the consumer.

- **Sensitive PI** (*See #8 and #15 below*): Although the Proposed Regulations list the permissible purposes for processing sensitive PI, unlike Section 1798.121(d) of the CPRA, the Proposed Regulations do not specify that a consumer's right to limit use/disclosure of sensitive PI must be provided only when a business uses the sensitive PI to infer characteristics about the consumer.

- **Overly prescriptive contract requirements for third parties** (*See #16(b) below*): Failure to include all the newly required terms in a vendor contract means that under the CPRA, the vendor cannot be considered to be a service

provider, must be treated as a third party and any disclosure of PI to the vendor may be deemed to be a "sale" or "sharing" of personal information.

- **Business purpose disclosures in service provider/contractor/third party contracts** (*See #18(f) below*): New requirements to identify the specific business purposes and services for which PI will be processed on behalf of the business and specify that the business is disclosing the PI only for the limited and specified business purposes set forth in the contract between the parties - a generic description referencing the entire contract is not acceptable. Identifying these specific business purposes in a contract with a vendor is not a typical practice and complying with this obligation would require businesses to amend all contracts with service providers to include language that is specific and particular to the services that the service provider provides to the businesses. Adding such language in the contract does not serve any practical purpose, would impose significant burdens on businesses to include customized language in their contracts with service providers and ensure that the language in the contracts is kept current as the services provided expand and change over time.

- **Confusing treatment of providers of advertising services** (*See #16(a) below*): Any entity providing cross-context behavioral advertising to a business is considered to be a third party for CPRA purposes and cannot be a service provider or contractor even if the entity otherwise meets all of the CPRA requirements for a service provider or contractor.

2. Restrictions on Use of PI (Section 7002(a))

Section 1798.100(c) of the CPRA states that "[a] business's collection, use, retention, and sharing of a consumer's personal information shall be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose that is compatible with the context in which the personal information was collected, and not further processed in a manner that is incompatible with those purposes." Section 1798.100(a)(1) of the statute permits the collection or use of PI for additional purposes that are incompatible with the disclosed purposes for which the PI was originally collected if the business notifies the consumer of the additional purposes.

Unlike Section 1798.100(a)(1) of the CPRA, Section 7002(a) of the Proposed Regulations requires the business to obtain "explicit consent" from consumers prior to collecting, using, retaining, or sharing PI for "any purpose that is unrelated or incompatible with the purpose(s) for which the personal information [was] collected or processed." However, there is no basis in the CPRA for requiring a business to obtain a consumer's explicit consent in these situations. This new requirement introduced by the Proposed Regulations will remove a business's ability to rely on making updates to the disclosures in its privacy policy to address changes in its practices regarding the collection/use/retention and sharing of PI and the flexibility to respond to evolving business practices. Complying with this new requirement will also result

in material changes to data collection practices, add significant compliance costs, and adversely impact innovation while providing little additional benefit to consumers.

The CPPA should amend the Proposed Regulations to require that in situations in which the business collects, uses, retains or shares any PI for any purpose that is unrelated or incompatible with the purpose(s) for which the PI was originally collected or processed, the business would be required to provide to consumers notice of such new purposes, rather than obtaining the consumers' prior explicit consent.

3. Dark Patterns (Section 7004)

The Section 7004(c) of the Proposed Regulations significantly expands the current definition of "dark patterns" to include any user interface that "has the effect of substantially subverting or impairing user autonomy, decision making, or choice, *regardless of a business's intent*" (emphasis added). Section 7004(a) mandates that "a method that does not comply with subsection (a) may be considered a dark pattern." As a result, any method that does not comply with all of the concepts listed in 7004(a) may be considered to be a dark pattern.

This section potentially subjects businesses to strict liability regarding the development and implementation of their user interfaces, and the CPPA or Attorney General could initiate an enforcement action against a business that experienced technical, software, hardware, or other technology-related issues that accidentally or unintentionally caused a user interface to not meet all of the requirements set forth in subsection (a). It is common for businesses of all sizes to experience problems with their websites, online user interfaces, and mobile applications, particularly since there are an exponential number of combinations of hardware devices, browsers, applications and other hardware and software that users can use to access a business's websites and/or mobile applications, and most businesses at some point encounter situations in which the business's website or mobile application does not operate properly on a particular combination of hardware and software used by a user. Moreover, these problems in other scenarios can occur without the business's negligence, wrong-doing, or intent. Malicious actors, hackers, and other criminals can also alter or disrupt a business' online presence, despite the business' use of state-of-the-art security measures. A business should not be punished for something it did not intend or cause nor could have prevented.

The Proposed Regulations should be amended to align with the CPRA definition of "dark pattern" which does not include "regardless of a business's intent" with substantial subversion or impairment of choice concepts. Removing the phrase "regardless of a business's intent" would eliminate the strict liability consequences and take a more measured approached that considers the business's intent, knowledge, and other relevant factors such as information security practices. The Proposed Regulations should also eliminate the rigid mandate that any method that does not comply with all of the concepts listed in Section 7004(a) may be considered a dark pattern. There should be flexibility in assessing whether a particular practice is in fact a dark pattern and the items listed in 7004(a), as well as others, can be among the factors that are considered when determining whether a particular practice meets the definition of a dark pattern.

4. Additional Privacy Policy Requirements (Section 7011(e))

Proposed Section 7011(e) requires a business's privacy policy to include significantly more than what is required by the CPRA. For example, Section 7011(e)(1) requires "a comprehensive description of the business's online and offline practices regarding the collection, use, sale, sharing, and retention of personal information." The statute does not include any requirement that the privacy policy contain a "comprehensive description" of a business's "online and offline practices." The regulations should track with the statute and provide additional guidance or clarity, not create unanticipated requirements with undefined terms such as "comprehensive description."

The Proposed Regulations would also require businesses to provide details in the Privacy Policy and Notice at Collection on a category-by-category basis in a manner that goes well beyond what the CPRA would require, which is extremely difficult to maintain in an accurate fashion and will lead to long and wordy charts that evade the CPPA's stated goal of ensuring an easily digestible explanation of data processing practices to consumers.

This provision should be deleted because the current requirements under the CPRA are sufficient to protect consumers and should not be expanded.

5. Notice at Collection Online Requirement (Section 7012(f))

Section 7012(f) requires a business that collects PI online to provide the notice at collection by providing a "link that takes the consumer directly to the specific section of the business's privacy policy that contains the information required in subsection (e)(1) through (6)." The section continues by stating that directing the consumer to the beginning of the privacy policy or to any other section without the required information will not satisfy the notice at collection requirement. Not only is this requirement overly prescriptive and burdensome, but it is also impractical. Under the Proposed Regulations, the notice at collection would be required to be customized to the particular product or service requested by the consumer which seems to necessitate that every notice at collection would have different links to different sections of the business's privacy policy. Implementing such an arrangement will be extremely burdensome and may be difficult to implement or unnecessarily cumbersome from a technology perspective.

The Notice at Collection specifications also do not take into account the fact that some companies are global and may have different notice requirements for individuals located in different jurisdictions. Therefore, the Notice at Collection mandated in the Draft Regulations may take all website visitors to the section of a Privacy Policy that applies only to California consumers or perhaps US consumers, but that does not meet the specifications of GDPR (including by specifying the lawful bases for processing). This creates complexity and confusion for consumers, which the CPPA is clearly endeavoring to avoid.

The CPPA should delete this provision from the Proposed Regulations.

6. Notice Regarding Third Party Data Collection (Sections 7012(e) and (g))

Proposed Section 7012(e)(6) requires a business that allows third parties to control the collection of PI from a consumer to include in its notice at collection, "the names of all third parties; or, in the alternative, information about the third parties' business practices." The CPRA requires only disclosure of "categories" of third parties, never names or business practices, including in the privacy policy, other notices at collection, and in response to the right to know/access. This requirement will be burdensome while providing little benefit to the consumer when it is obvious to the consumer that their data is collected by a third party. The Proposed Regulations should track with the statute requiring disclosure of categories of third parties, not names or business practices. Proposed Section 7012(g)(1) further requires that both the business and the third parties provide a notice at collection, which the proposed regulations state can be provided with a link that carries the consumer to the specific section of the privacy policy that discusses such collection.

Section 7012(g)(1) also introduces a new concept also not in the CPRA regarding third parties who "control" the collection of PI, and the imposition of an obligation for such third parties to deliver their own privacy notice at collection. This section goes beyond the statute, creating new obligations not previously contemplated and should be addressed by the service provider, contractor, and third-party contractual requirements and related restrictions, and not by regulation.

The CPPA should clarify whether providing a list of third parties that control the collection of PI is required even when there may be confidentiality provisions governing disclosure of the existence of an agreement between businesses, or where it is obvious to the consumer that their data is collected by a third party; and where, for white labeled products where the identity of the third party is not disclosed, the first party's information handling practices apply and will be presented to the consumer.

The CPPA should also clarify how multiple notices of collection are to be presented to consumers in cases where there are multiple third parties engaged in collection, particularly on websites. Finally, it may be operationally difficult for a business to collect sale/sharing opt-outs for itself and all third parties listed in its notice of collection.

7. Notice of Right to Opt-out of Sale/Sharing (Section 7013(e))

Proposed Section 7013(e) requires a business that "sells or shares" PI to provide a notice of right to opt-out of "sale/sharing." Under the current CCPA statute and CCPA AG Regulations, a business that does not "sell" PI is not required to post a "Do Not Sell My Personal Information" link. Under the Proposed Regulations, if a business "shares" but does not "sell" PI, the regulations require a business to post a "Do Not Sell or Share My Personal Information" link or the alternative link. If a business "shares" but does not "sell," data or vice versa, the business should be able to post the relevant link and not both links. For example, the business that does not "sell" but "shares" should be permitted to post a "Do Not Share My Personal Information" link without the inclusion of "sale."

The CPPA should amend the Proposed Regulations to allow businesses more flexibility around how to tag the link. Labeling the link "Do Not Sell or Share My Personal Information" may be misleading to consumers in those cases where a business does one or the other, but not both. It also arguably contradicts a statement a business may make in its notice of collection that it does not sell information. Also, we note the term "share" as defined in the CPRA is arguably not what the average consumer understands sharing to mean and also conflicts with other "sharing" opt-outs that a business may offer (e.g., GLBA third-party sharing opt outs, FCRA affiliate sharing opt outs). Further, links with mandatory naming conventions are problematic for companies that have to comply with multiple different privacy laws across multiple jurisdictions.

8. Limitations on the Use of Sensitive PI (Section 7014)

Although the Proposed Regulations list the permissible purposes for processing sensitive PI, unlike Section 1798.121(d) of the CPRA, the Proposed Regulations do not specify that a consumer's right to limit use/disclosure of sensitive PI must be provided only when a business uses the sensitive PI to infer characteristics about the consumer.

The Proposed Regulations should be amended to state that sensitive personal information that is collected or processed without the purpose of inferring characteristics about a consumer is not subject to the regulations' requirements pertaining to sensitive personal information. This would align the Proposed Regulations with Section 1798.121(d) of the CPRA. Without the qualifier that is currently in the CPRA, the scope of what constitutes "sensitive information" is increased significantly beyond what is set forth in the CPRA, without any justification in the statute.

9. Permissible Deletion from Backup Systems (Sections 7022(b) and (d))

Section 7022(b)(1) requires businesses to delete a consumer's PI from its existing systems except "archived or back-up systems," seemingly indicating that requests to delete do not trigger a requirement to delete PI on archived or back-up systems. To the contrary, Section 7022(d) states that a business that stores any PI on archived or back-up systems "may delay compliance with the consumer's request" until the archived or back-up system is "restored to an active system or is next accessed or used for a sale, disclosure, or commercial purpose." These provisions open several interpretive questions such as when it may be permissible to delete PI from backup systems and what type of access may trigger the requirement to delete PI from a backup system. For example, "access" should clearly exclude de minimis, temporary, or transient access for maintenance, information security, fraud, system improvement, and other purposes that do not require length or permanent access nor use or disclosure of PI outside of the limited purposes mentioned.

The CPPA should clarify these distinctions and provide better examples of when PI does and does not need to be deleted from backup systems.

10. Documentation to Conduct Correction Assessments (Section 7023)

Proposed Section 7023 requires businesses to undergo an onerous process of looking at the "totality of the circumstances" in deciding to make a correction. This nebulous requirement

leaves firms without adequate guidance on how to perform such assessments and the examples provided are not helpful guides. Similarly, the documentation requirements are burdensome and inappropriate in some cases (e.g., requiring less documentation where there is a high impact to a consumer, such as challenging the appearance of a bankruptcy on their record). Also, the Proposed Regulations do not provide any guidance on how to determine if a request is fraudulent or abusive, leaving businesses that deny a request open to enforcement actions.

Additionally, the responsibility for correcting inaccurate PI should be reallocated, as it is currently overly burdensome for both the consumer and the business. Consumers should be directed to the source of inaccurate information to correct their PI – and that may not be the business in question. Specifically, Section 7023(i) of the Proposed Regulations provides that "[w]here the business is not the source of the information that the consumer contends is inaccurate, in addition to processing the consumer's request, the business shall provide the consumer with the name of the source from which the business received the alleged inaccurate information."

The proposed regulations should be revised to clarify that third-party sources of inaccurate information should be primarily responsible for ensuring that the incorrect PI is corrected in third-party systems. Businesses should only be required to inform the consumer of the name of the source from which the business received the allegedly inaccurate information.

11. Notification of External Parties of Denial of Correction Requests (Section 7023(f)(3))

Section 7023(f)(3) requires a business that has denied a consumer's request either in whole or in part, to notify the consumer that, upon their request, the business will "note both internally and to any person with whom it discloses, shares, or sells the personal information" that the consumer has contested the accuracy of the PI, unless the request is fraudulent or abusive. This requirement goes beyond the statute by requiring a business to notify both internally and to any person with whom it discloses, shares, or sells the PI that the consumer has requested correction, despite the request having been denied. Assuming the denial is lawful, there is no reason a business should have to contact external parties to inform them of a denied request to correct. There is nothing for the external parties to do with this information.

12. The Right to Access Conflicts with the CPRA and Data Minimization Principles

Proposed Section 7024(h) appears to automatically require businesses to provide information they have about a consumer beyond the 12-month period required in the statute, and to provide a detailed explanation if this is not done. This provision conflicts with the CPRA and is unduly burdensome on businesses, as well as in some cases, likely to lead to a conflict with data minimization principles. Further, the requirement to provide information that has been collected by a third party or service provider on the business's behalf requires clarification. For example, background check providers may collect certain information directly from individuals, but never share the details with the business. To require the business to now collect those details to share with a consumer in response to an access request increases breach exposure and constitutes a further violation of data minimization principles.

The CCPA should strike this requirement from the final rules.

13. Opt-out Preference Signals (Section 7025)

Section 1798.135(a) of the CPRA requires businesses to provide links on their websites that enable consumers to limit the sale and sharing of PI and the use and disclosure of sensitive PI. Section 1798.135(b) indicates that businesses are not required to comply with 1798.135(a) "if the business allows consumers to opt-out of the sale or sharing of their personal information and to limit the use of their sensitive personal information through an opt-out preference signal sent with the consumer's consent." Section 1798.135(b)(3) further states that "[a] business that complies with subdivision (a) is not required to comply with subdivision (b). For the purposes of clarity, a business may elect whether to comply with subdivision (a) or subdivision (b)."

Proposed section 7025(e) states the exact opposite, stating that Section 1798.135 "does not give [a] business the choice between posting the above-referenced links or honoring opt-out preference signals. Even if the business posts the above-referenced links, the business must still process opt-out preference signal." Section 7025(c)(6) adds additional confusion by saying a business "should display whether or not it has processed the consumer's opt-out preference signal," which suggests processing preference signals is optional.

The Proposed Regulations do not address what type of signal qualifies as "universal optout preference signal," or the technical limitations in honoring universal opt-out preference signals. Currently, there is no universal opt-out preference signal capable of effectively communicating a consumer's opt-out preferences to all websites, online platforms, or mobile applications. Universal opt-out preference signals should be an optional method that businesses may use to opt-outs as outlined in the statute. Alternatively, the CPPA should clarify how a signal qualifies as one that businesses must recognize.

The Proposed Regulations directly conflict with the CPRA and should be amended to permit businesses the option to honor universal opt-outs. If businesses must recognize opt-out preference signals, there could be significant operational impacts on businesses, including, among other things, implementing technology to recognize and process such signals and applying them to individuals who may use a range of methods to access a business's website.

14. Downstream notification of consumer opt-out requests to all third parties (Section 7026(f)(2))

Proposed Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer's PI of their request to opt-out of sale/sharing and to forward the consumer's opt-out request to "any other person with whom the person has disclosed or shared the personal information." Both requirements go beyond the CPRA and would be technically challenging at the device level whether in connection with a one-off device interaction or in response to a global privacy control. Furthermore, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the PI doesn't take into consideration lawful disclosures to service providers, contractors, law enforcement,

government agencies, or disclosures to other businesses or individuals pursuant to an explicit request or direction from the consumers to make the disclosure.

The CPPA should amend these requirements because they go beyond the statute and are operationally difficult or impossible due to technological and practical limitations.

15. Sensitive PI (Section 7027)

Section 1798.121(d) of the CPRA states 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 [Section 1798.121 on requests to limit use and disclosure of sensitive personal information], as further defined in regulations…and shall be treated as personal information for purposes of all other sections of this Act, including Section 1798.100." Notably, the draft regulations do not clarify when sensitive PI is considered collected or processed for purposes other than inferring characteristics about a consumer. According to the statute, collecting or processing sensitive PI for purposes other than inferring characteristics about a consumer is exempt from the right to limit the use and disclosure of sensitive PI. However, the draft regulations read as if this exemption does not exist, and any collection or processing of sensitive PI is subject to the right to limit use and disclosure. The regulations should be amended to track the statute.

Also, in a number of sections, the Proposed Regulations contravene and narrow the scope of the statutory language, effectively disregarding Section 1798.121(a)-(b), which permit a business to use a consumer's sensitive PI for uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services," even after receipt of a consumer's request to limit. While the Regulations attempt to define permissible uses of sensitive PI in Section 7027(l), the seven use cases listed most certainly do not encompass all those uses of sensitive PI that may be "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services." The impact of this overreach by the Proposed Regulations will have significant adverse effects. As an example, in Section 7014(h), the Proposed Regulations purport to impose a springing consent requirement with respect to any use, outside the seven limited uses defined by Section 7027(l), of sensitive PI collected at a time when a business did not have a notice of right to limit posted. As a notice of right to limit is not required until January 1, 2023, any PI collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the seven purposes defined by Section 7027(l).

Similarly, in Section 7027(g)(1), the Proposed Regulations require that, upon receipt of a request to limit, a business must cease to use and disclose sensitive PI for any purpose other than the seven purposes listed in Section 7027(l); a restriction that conflicts with the language in 7027(a) and in 1798.121(a)-(b) that allows uses that are "necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services." These inconsistencies are extremely problematic for constructing a compliance program. The above notwithstanding, the seven use cases identified in 7027(l) don't even contemplate a use of sensitive PI to comply with a legal or regulatory obligation or otherwise address any use case that relates to uses of employee information.

The CPPA should revise the Proposed Regulations to limit overreach and resolve inconsistencies in the Proposed Regulations and with the CPRA.

16. Service Provider, Third-Party, and Contractor Relationships (Sections 7050, 7051 and 7053)

The combined effect of the service provider/third party/contractor provisions in the proposed regulations is confusing and could, in their present iteration, greatly impact any business that combines information from various sources. Section 1798.140(v) of the CPRA defines service providers as a person or entity, operating in a for-profit capacity, that processes PI on behalf of a business. Section 1798.140(w) defines third parties as people or organizations that is not: (1) a business that collects PI from consumers, nor (2) a person or entity to whom the business discloses a consumer's PI.

a. Confusing treatment of providers of advertising services

Proposed Sections 7050(a) and (c) expand the definition of "service provider" to include "contractors," while treating vendors that provide cross-context behavioral advertising services (services for online advertising where a business provides information about its own customers to a vendor to perform advertising on behalf of the business) a list of its own customers' email addresses to a vendor as "third parties." Specifically, under proposed Section 7050(c), any entity providing cross-context behavioral advertising to a business is a third party and cannot be a service provider or contractor. A business should have the right to contract with a vendor to provide cross-context behavioral advertising services to the business and if the vendor meets all the other requirements to qualify as a service provider, the arrangement should not result in the business being deemed to engage in selling and/or sharing PI and thus required to offer an opt-out to consumers.

The CCPA should delete the new restriction.

b. Overly prescriptive contract requirements for third parties

The Proposed Regulations also impose new contract terms a business must include in its agreements with service providers and contractors. Under proposed Section 7053, failure to include all the required terms in an agreement with a firm that is acting as a service provider/contractor means that under the CPRA, the firm must be treated as a third party to which the business may be deemed to "sell" or "share" PI. The Proposed Regulations do not conform to the requirements in Section 1798.100(d) of the CPRA and cover obligations already addressed in the CPRA with respect to both businesses and service providers. There is no value in requiring businesses and service providers to restate these obligations as contract terms. Furthermore, a business's failure to comply with the new requirement to include all the prescribed terms in agreements with service providers/contractors would result in a harsh consequence on the business and the service providers – the business would be required to treat those services providers as a third party and if the business provides PI to such parties, that sharing would need to be treated as a sale or sharing of PI. Both consequences would have a significant compliance impact for both businesses and service providers.

The Proposed Regulations should be amended to mirror the requirements in Section 1798.100(d) of the CPRA.

c. Notice and Consent

Proposed Section 7053(a) imposes new contract requirements for third parties including, among other things, that third parties, authorized to collect PI from consumers through a business's website, check for and comply with a consumer's opt out preference signal to not sell or share their PI. Any third-party involvement in the collection of PI must be communicated to consumers with notice, and a failure to have an agreement in place forbids a third party from processing PI received from the business. The Proposed Regulations would require an impractical amount of contract remediation to updated executed contracts with this information and goes far beyond what was contemplated by the CPRA.

The CPPA should clarify whether a person could be acting as both a business and a service provider with respect to the same personal data. Additionally, the CPPA should clarify whether explicit consent from a consumer could make restrictions on the use of PI originally obtained in the service provider context moot. The CPPA should also clarify the meaning of "third parties," as it remains undefined compared to the term "service providers."

d. Audit and Due Diligence

Proposed Section 7051(e) explains that "[f]or example, depending on the circumstances, a business that never enforces the terms of the contract nor exercises its rights to audit or test the service provider's or contractor's systems might not be able to rely on the defense that it did not have reason to believe that the service provider or contractor intends to use the personal information in violation of the CCPA and these regulations at the time the business disclosed the personal information to the service provider or contractor." The CPPA should provide guidance regarding what "circumstances" would justify a business not exercising its right to audit. For example, would certification or representation that the service provider's parent/affiliates are a GLBA-regulated entity be a sufficient circumstance?

Proposed Section 7051(e) and Section 7053(e) states that "[w]hether a business conducts due diligence of its" service providers, contractors, or third parties "factors into whether the business has reason to believe" the service provider, contractor, or third party is using PI in violation of the CCPA/CPRA. Furthermore, both provisions cite an example where a business that never enforces the terms of its contract nor exercises its rights to audit or test might not be able to rely on the defense that it did not have reason to believe that the service provider, contractor, or third party intended to use the PI in violation of the CCPA.

A business's right to avail itself of the CPRA liability shield for violations committed by a service provider, contractor, or third party should not be conditioned on its due diligence of that service third party, but on whether the business had actual knowledge or reason to believe that the violation would be committed *consistent with the CPRA*. A business may not be able to secure the contractual right to periodically audit or test the systems of each service provider,

contractor, or third party to which it discloses PI and should instead be permitted to rely on independent assessments or audit reports prepared by a third parties (e.g., SOC 2).

e. Business purpose disclosures in service provider/contractor/third party contracts (Section 7051(a)(2) and Section 7053)

Proposed Section 7051(a)(2) requires businesses to identify, in each service provider or contractor agreement, the specific business purpose for which PI will be processed on behalf of the business and specify that the business is disclosing the PI only for the limited and specified business purposes set forth in the contract between the parties. The Proposed Regulations note that a generic description referencing the entire contract is not acceptable, which goes beyond the CPRA's obligations.

The CCPA should remove this requirement because specifying the business purpose for each PI processing activity is impractical. Large companies with thousands of vendors would have to spend significant time and resources to identify and list in its contracts with every service provider each specific business purpose for which the business discloses PI to the service provider. Furthermore, many businesses enter into master agreements with vendors and service providers and the details of the specific products or services that are provided under the agreement are specified in other documents (such as purchase orders or statements of work) or other communications between the companies (such as emails). Failure to specify the specific business purposes and services in an agreement with a vendor should not disqualify the vendor. from being a service provider/contractor under the CPRA

17. Authorized Agents (Sections 7001 and 7063)

The Proposed Regulations would also loosen safeguards for requests from authorized agents which would allow requests from those who are not acting as a power of attorney for the customer. SIFMA believes that eliminating these safeguards will encourage fraudulent activity.

The CCPA should reinstate these safeguards and the requirement that authorized agents be registered California business entities.

18. CPPA Audit (Section 7304)

Section 7304 of the Proposed Regulations states that the CPPA "can conduct an audit if the collection or processing of PI presents a significant risk to consumer privacy or security, or if the subject has a history of noncompliance with CCPA or any other privacy protection law."

This provision is extremely broad and potentially outside of the scope of the CPPA's authority under the CPRA and therefore should be struck from the Proposed Regulations.

19. The Effective Date for the Rule Should be No Earlier Than January 2024

SIFMA encourages the CPPA to delay the effective date and enforcement of any final CPRA rules until January 2024. To date, only a portion of the CPRA regulations have been proposed and some critical and potentially complex regulations including automated

decisionmaking are still forthcoming. The operational challenges highlighted in this letter clearly indicate that additional time will be needed for companies to fully and responsibly implement new requirements given the complexity of the Proposed Regulations. Requiring businesses to attempt to comply prior to that time will lead to confusion and sloppy execution that will only harm businesses and consumers alike.

* * * * *

SIFMA and its members appreciate the opportunity to provide these comments and welcome further discussion. Please reach out to Melissa MacGregor at mmacgregor@sifma.org with any questions or to schedule a meeting.

Sincerely,

Melissa MacGregor

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Kim Chamberlain, Managing Director, State Government Affairs, SIFMA