November 21, 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") Modified Text of Proposed Regulations dated November 3, 2022 (the "Modified Proposed Regulations") that modifies the previously proposed regulations published on July 8, 2022 as required under the Consumer Privacy Rights Act of 2020 ("CPRA").[2] SIFMA previously commented on the initial proposed regulations dated August 18, 2022 ("Initial Letter")[3] and the comments below reflect some of those same comments as well as comments on the Modified Proposed Regulations. SIFMA appreciates the continued work 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.[4]

---

[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] SIFMA Letter to California Privacy Protection Agency (August 18, 2022) (available at https://www.sifma.org/wp-content/uploads/2022/08/California-Privacy-Regulation-Letter.pdf).

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

SIFMA urges the CPPA to carefully consider the costs associated with potentially overly prescriptive regulations both for businesses and ultimately for customers. As we did previously, the below comments highlight several of the proposed requirements which may do little to protect investors, but would be costly to comply with. We are only about one month away from the January 1, 2023, the compliance date for the CPRA, thus making any new obligations inordinately costly at this late date. As such, SIFMA urges the Commission to consider eliminating any requirements that exceed the CPRA mandate from the Modified Proposed Regulations.

SIFMA continues to remain concerned about the 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). The most recently proposed regulations do not address requirements for responding to requests from employees and B2B contacts. Without specific guidance, 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. **The required business purpose disclosures in agreements and related requirements are impracticable. (Sections 7051(a)(2), 7051(a)(7) and 7053)**

SIFMA continues to be concerned about the provisions that unnecessarily expand on the requirements of the CRPA including Section 7051(a)(2) of the Modified Proposed Regulations which requires businesses to identify in each service provider or contractor agreement the specific business purpose for which personal information is disclosed. The draft regulations would require an impracticable amount of contract remediation to update executed contracts with this information. Further, Section 7053 of the Modified Proposed Regulations requires the same information for third party agreements, which also goes beyond the statute's requirements and is an impracticable task.

Also Section 7051(a)(7) states that "Reasonable and appropriate steps may include ongoing manual reviews and automated scans of the service provider's system and regular internal or third-party assessments, audits or other technical operational testing at least once every 12 months." The ability to do this has significant impacts on license agreements and contractual provisions, intellectual property and security with service providers, much less the ability to create such testing program. SIFMA urges the CPPA to consider require an annual certification of compliance in lieu of an audit.

2. **The Modified Proposed Regulations disregard the statutory language allowing businesses to use Sensitive Personal Information (SPI) for specific purposes. (Section 7027)**

In some sections, the Modified Proposed Regulations contravene and narrow the scope of the statutory language, effectively disregarding CPRA Section 1798.121(a)-(b), which permits a business to use a consumer's SPI 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. The impact of this overreach will have significant adverse effects on businesses and impair a company's ability to establish a strong compliance program. The CPPA should amend this language to coincide with the CPRA.

The following examples demonstrate these challenges:

- In Section 7014(h), the draft regulations purport to impose a springing consent requirement with respect to any use, outside the eight limited uses defined by Section 7027, of SPI 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 (and only if the business is collecting SPI for the purposes of inferring characteristics), any personal information collected prior to January 1, 2023, absent consumer consent, may not be used for any purpose other than one of the eight purposes defined by Section 7027.

- Similarly, in Section 7027(g)(1), the draft regulations require that, upon receipt of a request to limit, a business must cease to use and disclose SPI for any purpose other than the eight purposes listed in Section 7027.

- This is 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."

3. **The requirement to take consumers to a specific section of a privacy policy is unworkable and should be deleted. (Section 7012(f))**

Section 7012(f) of the Modified Proposed Regulations requires a business that collects personal information 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.

This requirement is overly prescriptive, burdensome, and impracticable. The notice at collection must contain a link to the privacy policy. Additionally, the notice at collection is more tailored to the products or services requested by the consumer, thus seems to require every notice of collection to contain different links to varied sections of the privacy policy which would be confusing for consumers and extremely challenging for businesses. This requirement should be deleted.

4. **Downstream notification of opt-out requests to all third parties is operationally challenging or impossible. (Section 7026(f)(2))**

Section 7026(f)(2) requires a business to notify all third parties to whom the business has sold or shared a consumer's personal information of a consumer's 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 requirements of the statute 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).

Further, the requirement to forward a consumer's request to any person with whom the person has disclosed or shared the information does not 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. These requirements go beyond the statute and are operationally difficult or impossible due to technological and practical limitations.

In addition, the CPPA has still not addressed situations where a prospective customer becomes a customer. Businesses need clarity on how to transition customer preferences in these cases. Consent should not be required where an individual becomes a customer under the Gramm-Leach-Bliley Act ("GLBA") and the exception applies.

5. **The requirement to delete personal information from archived or back-up system is expressly excluded from the CPRA. (Sections 7022(b) and (d))**

Section 7022(b)(1) of the Modified Proposed Regulations requires businesses to delete a consumer's personal information from its existing systems except "archived or back-up systems," seemingly indicating that requests to delete do not trigger a requirement to delete personal information on archived or back-up systems. To the contrary, Section 7022(d) states that a business that stores any personal information 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."

SIFMA requests that the CPPA clarify whether (1) a business is never required to delete personal information stored on archived or back-up systems (as long as it remains on such archived or back-up systems), OR (2) a business has a requirement to delete personal information on archived or stored systems; however, that requirement isn't triggered unless, or until, a business activates that system or accesses, sells, discloses, or uses such data for a commercial purpose.

Additionally, the CPPA should clarify that "access" does not include *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 personal information outside of the limited purposes mentioned.

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

6. **The provisions that unnecessarily shift liability away from service providers. (Section 7051(c) and Section 7053(b))**

Section 7051(c) and Section 7053(b) of the Modified Proposed Regulations state 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 personal information in violation of the CCPA/CPRA. Further, 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 personal information in violation of the CCPA.

These provisions go beyond the CPRA and shift nearly all service provider, contractor, and third-party liability to the business. Moreover, the provisions do not discuss what level of due diligence is required to prevent the shifting liability. As a result, these provisions should be struck or amended and clarified such that businesses know what level of due diligence is required to prevent the shifting liability.

7. **CPPA should expressly allow self-service portals for all types of requests. (Section 7024(g))**

Section 7024(g) allows businesses with password-protected accounts to use a self-service that allows consumers to access, view, and receive a portable copy of their personal information. This section should be expanded to also expressly allow consumers to request to delete or request information.

8. **The consumer opt-in provisions are unnecessarily onerous on businesses. (Section 7028).**

Section 7028(a) would require a two-step process for sharing/sale and requests to opt-in for use and disclosure of sensitive personal information. This could potentially be an onerous requirement depending on what is required as a second confirmation step. The CPPA should confirm that the requirement is satisfied if, for example, the consumer clicks a button or check box and then clicks submit.

9. **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. Such requirements should only apply to data collected on or after the compliance date to ensure that firms have adequate systems and controls in place to comply with the new requirements. 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 these requirements. 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