December 6, 2019

VIA EMAIL TO: privacyregulations@doj.ca.gov
The Honorable Xavier Becerra
Attorney General, State of California
1300 I Street
Sacramento, CA 95814

Privacy Regulations Coordinator
California Office of the Attorney General
300 South Spring Street, First Floor
Los Angeles, CA 90013

Re: Proposed California Consumer Privacy Act Regulations

Dear Attorney General Becerra,

The Securities Industry and Financial Markets Association (SIFMA)[1] appreciates this opportunity to comment on the proposed California Consumer Privacy Act (CCPA) regulations.

I. Executive Summary

In promulgating regulations under the CCPA, it is important that the Attorney General's office endeavor to create clear and consistent rules that businesses can meaningfully rely on in their efforts to comply with the CCPA and provide consumers with additional clarity about the collection, use, and sharing of their personal information. To that end, SIFMA requests that the Attorney General's office delay enforcement of the CCPA until January 1, 2022, to allow for businesses to appropriately implement the complex systems of accepting, verifying, and responding to consumers' requests in accordance with the regulations' requirements.

[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 industry's nearly 1 million employees, 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).

In addition, SIFMA recommends that the regulations seek to enhance the clarity of ambiguous language in the CCPA in order to ensure the efforts to increase privacy do not come at the cost of the security of consumer personal data. Within the regulations, SIFMA requests that any requirements related to the disclosure of information take into account dual goals of enhancing clarity for consumers and protecting businesses' free speech interests in the use of data for internal business purposes. In addition, the regulations should seek to provide businesses with flexible options for complying with consumer requests in a way that satisfies both the consumers' interest in protecting their personal information and the business's legitimate business interests. We describe our specific concerns and recommendations in more detail in the sections that follow.

II. Enforcement of the regulations should be delayed until January 1, 2022.

The CCPA states that the Attorney General should "adopt regulations" by July 1, 2020, but does not mandate an effective date for those regulations; instead it states that the earliest date that such enforcement could be brought is "six months after the publication of the final regulations […] or July 1, 2020, whichever is sooner."[2] The Attorney General thus has discretion to delay enforcement of the regulations until a later date. California Government Code sets forth a default timeline establishing when regulations become effective.[3] The default rule states that it does not apply if the "effective date is specifically provided by the statute" or if a "later date is prescribed" in the regulation.[4] As the CCPA does not specifically provide an effective date, the California Attorney General has the authority to provide such a date in the regulations. We encourage the Attorney General to delay that enforcement until January 1, 2022, which would allow for a two-year grace period beyond the CCPA's January 2020 effective date and would provide companies an additional eighteen months to prepare for compliance, after the July 1, 2020 enforcement date. This would be somewhat less than the amount of time that the European Union provided companies to prepare for the EU's General Data Protection Regulation ("GDPR"), which developed from a well-established body of EU data protection law, but it would at least provide businesses with a reasonable opportunity to read the final regulations and develop systems in reliance upon clear guidance. The alternative has forced companies to try to anticipate what the final regulations might require even though the regulations will, at best, be issued days before the CCPA's effective date.

The CCPA itself provided an 18-month period between its passage and its effective date in recognition of the complexity of implementing the statute's numerous requirements. The draft regulations are similarly extensive and detailed in ways that could not reasonably be anticipated from the text of the CCPA. Implementation of many of the provisions in the draft regulations will require businesses to revise back-end processes. For example, the regulations necessitate the redrafting of many disclosures, notices, and

[2] CCPA, CA Civil Code § 1798.185(a).
[3] Cal. Gov't. § 11343.4.
[4] Cal. Gov't. § 11343.4(b).

communications. According to the draft regulations, those redrafted disclosures must include details about data collection and use that will require extensive development work to determine and convey meaningfully to consumers.

In addition, once the regulations are final, businesses will be required to revise, and possibly redraft, and implement additional content training with an expanded target audience and will need to establish channels for distributing information to consumers and accepting access and deletion requests. Attempting to rush this development work could introduce substantial anti-consumer risks, including security, fraud, and identity theft risks. Time is needed to establish and implement procedures for appropriately receiving and verifying requests, and additional personnel may need to be trained in accepting requests and documenting this verification process. If not done properly, this could lead to significant risk that consumer information is released to an unauthorized person who makes an invalid request. Testing and validation of processes is needed before these channels are opened to the public to mitigate the risk of fraud and identity theft. To reduce risk, this testing and validation should not be rushed.

While businesses are establishing robust verification procedures to meet the statutory text's effective date of January 1, 2020, they may need additional time to rework those procedures to comply with provisions in the regulations, such as § 999.325, which requires verifying identity with a high degree of certainty, including by obtaining and maintaining a record of a declaration signed under penalty of perjury, in lieu of—or possibly in addition to— comparable processes already planned. These new processes will take time to implement properly. To allow for that implementation, the Attorney General should either specify a later enforcement date in the regulation text, or, at a minimum, exercise its enforcement discretion by allowing for a grace period that would hold any enforcement actions until at least two years after the effective date of the CCPA and should withhold enforcement for any violations that occur before January 1, 2022.

III. The draft regulations should promote the goal of protecting consumers' personal information.

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 Safeguards Rules. While the industry recognizes that the goal of the CCPA is to provide greater transparency to consumers, no regulations should be issued that would promote transparency at the expense of harming the security of consumer data. The CCPA, Civil Code § 1798.185(a)(7) requires that, when establishing rules and procedures to facilitate consumers' ability to obtain information, the Attorney General take into account security concerns and available technology. Several of the proposed regulations, as drafted, do not properly account for the security risks that they create. These proposed regulations should be revised or struck as described below.

a. The regulations should not require detailed disclosure of the process used to verify consumer requests or the reasons that requests appear fraudulent

The proposed regulations require detailed disclosure of the process a business uses to verify consumer requests for access to or deletion of personal information, including any information the consumer must provide to verify the request.[5] This requirement compromises the security of consumer information by requiring businesses to disclose to potential bad actors the methods that they can use to maneuver through the verification process and fraudulently obtain personal information about another consumer. If businesses are allowed to employ risk-based verification measures as needed, businesses will be better able to protect consumers' privacy and avoid such security incidents.

Similarly, the proposed regulations require that businesses who believe that requests to opt out of sales are fraudulent can deny the request but must inform the requesting party with an explanation of why it believes the request is fraudulent.[6] Providing such an explanation places consumers' personal information at risk for two reasons. First, the group to whom the information provided—parties that have submitted requests that appear fraudulent—is likely to contain a high proportion of bad actors seeking to use deception to gain access to consumers' personal information without the consumers' authorization. Second, the information that the regulations require businesses to provide—an explanation of why the business believes the request is fraudulent—will only serve to educate the potential bad actor on how to create a more convincing request and defraud the verification system in the future.

These requirements should be struck from the final regulation entirely or the regulations should clarify that description of the process of verification and the determination that a request is fraudulent should be limited to a high-level summary.

b. Process for deletion of personal information

With regard to the procedures for accepting and executing requests for deletion of personal information, the regulations provide detailed requirements that are not mandated by the text of the CCPA and could hurt businesses' ability to protect consumer information. Section 999.312(d) of the proposed regulations requires a two-step process for deletion requests. It should be eliminated to allow businesses to make risk-based determinations about deletion requests that would better protect consumer information. Similarly, § 999.313(d)(2) of the proposed regulations limit the methods of deletion that businesses may use to comply with consumer requests. This should be deleted to allow businesses to implement additional measures to address deletion requests that would better meet the consumer protection goals of the statute.

[5] Proposed CCPA Regulations §§ 999.308(b)(1)c, 999.308(b)(2)c, and 999.313(a).
[6] *Id.* § 999.315(h).

Section 999.312(d) of the proposed regulations requires a two-step process for deletion but does not clearly describe what that process should entail. This provision should be deleted or clarified so that no "re-authentication" is necessary for consumers who have already authenticated their identity. If a two-step requirement is included in the regulations, the proposed regulation should state that businesses are not required to authenticate a consumers' identity twice. Instead businesses are required to confirm a second time whether consumers would really like their personal information deleted before deleting the information. The lack of clarity in the current provision could result in both over-deletion—because identity was authenticated twice, but the consumer did not have the opportunity to confirm that they wanted their information deleted before it was erased—and under-deletion—because businesses could not determine a workable method for the double authentication process. Both over- and under- deletion could create a risk to consumers' personal information, either by businesses erasing information that is unrecoverable against the consumers' wishes or by businesses maintaining information that consumers wanted erased that could be involved in future security incidents. Clarifying this requirement would result in more consistent application and better compliance with the consumers' wishes about the handling of their personal information.

In addition, the proposed regulations limit businesses to three prescribed options for handling deletion.[7] Limiting businesses to three options for deletion of information goes well beyond the CCPA requirement that businesses comply with consumer requests to have their personal information deleted. It imposes the three options without consideration of cost or other potential measures that businesses could employ. In addition, it prevents businesses from employing risk-based measures to determine the most appropriate method of deletion on a case-by-case basis. For these reasons, this provision should be deleted.

Finally, the proposed regulations require that information be deleted from archived or backup systems.[8] For financial institutions, such deletion would affect the ability of the business to maintain the necessary systems in a manner that complies with FDIC/FFIEC/SEC requirements for business continuity planning. In addition to such conflict with existing federal requirements, the deletion could create great risk for consumers. This requirement should be eliminated.

c. The regulations should clearly identify when it is too risky to disclose information in response to a data subject request.

The proposed regulations state that businesses "shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, and unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."[9] The terms "substantial" and "unreasonable" create ambiguity that

[7] *Id.* § 999.313(d)(2).
[8] *Id.* § 999.313(d)(3).
[9] *Id.* § 999.313(c)(3).

suggests that, if a business determines that there is an articulable security risk from the provision of certain information, it would still be allowed to provide that information if the business's perception of the risk is insubstantial or reasonable. This ambiguity could lead to second guessing of business decisions and could cause businesses to disclose information in response to requests that could potentially place more consumers' privacy at risk.

We would recommend either (1) striking the terms "substantial" and "unreasonable" (so that the provision reads: "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates an articulable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks."); or (2) replacing the word "and" before unreasonable with "or" (so that the provision reads: "A business shall not provide a consumer with specific pieces of personal information if the disclosure creates a substantial, articulable, or unreasonable risk to the security of that personal information, the consumer's account with the business, or the security of the business's systems or networks.").

IV. The regulations should clarify ambiguous provisions in CCPA.

In an effort to provide maximum transparency and foster smoother and more consistent implementation of the CCPA across businesses, the regulations should clarify certain points of ambiguous text in the CCPA.

First, the regulations should specify that the AB 1355 amendment to Civil Code § 1798.145 (which exempts personal information transferred in the course of certain business communications or transactions, where the consumer is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency) applies in the case of persons engaged in transactions in the role of institutional investors, trustees, partners, employees, beneficiaries, or other natural persons associated with financial accounts that are held in the names of institutions, partnerships, businesses, trusts, and estates. Currently, the CCPA's line between natural persons and estates, trusts, sole proprietorships, partnerships, etc. is ambiguous. The federal Gramm-Leach-Bliley Act as well as several other federal statutes established a clear line that transactions are properly considered consumer transactions when they are "for personal, family, or household purposes." See, e.g., 15 U.S.C. §§ 1692a(5), 2301(1), 6809(9). That same approach is respected in California law, Civil Code § 1791(a)(defining "Consumer goods" as a product ". . . used, bought, or leased for use primarily for personal, family, or household purposes . . . "). The CCPA should reflect this clear, commonsense division between a natural person acting as a consumer and a natural person acting as part of business. Accordingly, all financial information about natural persons gathered by a financial institution for "personal, family, or household purposes" is within Civil Code § 1798.145(e), and all personal information that is gathered by a financial institution for reasons other than "personal, family, or household purposes" should be within the ambit of the AB 1355 amendments for business interactions.

Second, the regulations should provide a non-exhaustive list of situations in which requests from a consumer could be considered manifestly unfounded or excessive, allowing businesses to charge a reasonable fee or refuse to act on the request, under Civil Code § 1798.145. Such examples should include requests that would require the business to expend a disproportionate amount of time, effort, and cost to ascertain the information that the consumer has requested or to provide the information to the consumer in a format that does not inadvertently reveal the personal information of another consumer in the process. In particular, the regulations should clarify that businesses are allowed to charge a reasonable fee or refuse to act on requests for hard copies or unstructured data. Providing clarity on this point would further the goal of protecting reasonable requests and would help protect consumer information from incidental exposure by a business.

Third, the regulations should define revenue, within the definition of "business" in the CCPA, Civil Code § 1798.140, as limited to revenue that is sourced from California. Such a clarification would be consistent with the Impact Assessment that was released along with the proposed regulations, which is calculated based on California Gross State Product and is not based on revenue from other states or international jurisdictions. Companies with small California operations but substantial operations in other areas would not be likely to process material amounts of personal information about California residents.

Fourth, the regulations should exclude from the definition of "sale" that is provided in Civil Code § 1798.140 all of the items that are subject to the general exceptions in 15 U.S.C. § 6802(e), such as disclosures of data related to servicing private label accounts, securitizations, transfers of servicing rights, provision of information to insurance rate advisory organizations, and in connection with the sale, merger, transfer, or exchange of the relevant financial institution. These exceptions are vital to the functioning of the secondary market activity that provides capital for consumer financial products and services and are subject to extensive federal oversight. It will only serve to confuse consumers if these secondary market activities are included within the definition of "sale" because the functioning of these markets can be incredibly complex and is far removed from the privacy interests that the CCPA seeks to protect.

Fifth, the regulations should clarify the definition of personal information for the purposes of data subject access requests ("DSARs"). The CCPA, as amended, defines "personal information" as information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." However, the amended CCPA explicitly excludes from the definition of "personal information" any consumer information that is "deidentified." The CCPA defines "deidentified" information as that which "cannot reasonably identify, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer," with the definition of consumer limited only to natural persons – and not a device. Because device identifier information can only reasonably be linked to a device, it should be excluded from the universe of personal information that businesses are required to provide or delete in response to DSARs. The inclusion of "device" identified information rests on the implicit presumption that devices are

surrogates for persons, but many devices are shared devices. Treating data from a shared device as data from a personal device could harm other unknowing users of that device. This is even more concerning because the users of shared devices are often those who do not have the economic means to own their own devices and may be the least familiar with the privacy and security challenges of using a shared device. Eliminating device identifier information from the universe of DSAR information would protect these shared-device using consumers and enable businesses to feel confident that they are providing information to the correct consumer without infringing on the rights of other individuals. For example, the device or browser in a public library may be used by several different consumers. If one of those consumers requested the "personal information" from a business that was connected to that device identifier, it would return information on several different consumers, which would not serve the purpose of providing consumers with more clarity about how their personal information is being used and indeed could compromise the privacy and security of the other users of that shared device.

V. The regulations should require disclosures that would provide consumers with a meaningful, comprehensible explanation of how their personal information is used and how they can exercise their rights with regard to their personal information without imposing a disproportionate burden on businesses seeking to comply with the regulations.

Several of the proposed regulations impose requirements for what must be disclosed to consumers, both in the privacy policy and in responses to consumer requests, which go above and beyond the requirements spelled out in the text of the CCPA. Many of these requirements will result in disclosures that are longer and more overwhelming and confusing to consumers. These verbose disclosures would frustrate the CCPA's goal of providing consumers with clarity about how their personal information is used and how they can exercise their rights with regard to their personal information. The proposed regulations should be modified to require only the disclosures necessary to provide consumers with meaningful information without otherwise compromising the security of the process or disproportionately burdening businesses who are trying to provide clarity to consumers.

a. Disclosures regarding the collection, use, and sharing of personal information

Sections 999.305(b)(2), 999.308(b)(1)d.2, 999.313(c)(10) address the detail with which businesses must describe the collection, use, and sharing of personal information. Those provisions require that the business specify the categories of information collected from a list provided in the CCPA, along with, for each separate data category, the sources from which the information was collected, the business purposes for which the information is used, the categories of third parties to whom the personal information may be disclosed, and the business purposes for which the information is disclosed. When listing these categories, businesses are instructed to select from eleven categories of personal information, a proposed minimum of three source types, and seven third party types, along with several possible uses of personal information. This information is too dense and detailed to include in a privacy

notice and could result in many dozens or of different combinations of this information, resulting in many additional pages of a privacy notice. This provision would be a large administrative burden on all businesses, and a mechanism by which businesses could be subject to large monetary penalties based on an error in judgment or record keeping, without meaningfully adding to consumers' understanding of how their personal information is used in shared. Rather it could cut against that understanding and cause more confusion.

The text of the CCPA does not require this information be provided in such a detailed fashion. Instead, the text of the CCPA can be interpreted to state that information on the categories of sources, business purposes, and third parties can be provided in the aggregate. The language of the regulations should be adjusted to be consistent with this understanding of the CCPA, which would provide for a disclosure that was much more accessible to consumers, easy to understand, and shorter, resulting in more consumers reading and comprehending from the disclosure how the business collects and uses their information. For example, the CCPA states that businesses should "inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used" but does not state that the purpose must be laid out for each category of personal information.[10] Indeed, pairing purposes of use with the categories of personal information could result in more confusion and lengthy disclosures, especially where certain categories of personal information may be used for more than one business purpose. Such disclosures would be at odds with the proposed regulation's requirement in § 999.305(a)(2) that notice be "designed and presented to the consumer in a way that is easy to read and understandable to an average consumer."

b. Disclosures regarding the business or commercial purpose

Both the CCPA and the regulations require that businesses disclose the business or commercial purpose for collecting or selling personal information.[11] The regulations should clarify that the potential business purposes for collection of the information could go beyond the seven options outlined in the CCPA definitions.[12] Consistent with the U.S. Supreme Court's decision in Sorrell v. IMS Health Inc., 564 U.S. 552 (2011), companies have a commercial free speech interest in their use of data. To balance the free speech interest and the resulting heightened judicial scrutiny, the regulations must use the least restrictive means of accomplishing their goal. Businesses may have legitimate interests in collecting personal information for internal uses that go beyond the seven uses provided in the CCPA definitions. The restriction of those internal uses of data to a limited set of use options does not further the government's interest in preventing the sale of data.

[10] CCPA, CA Civil Code § 1798.100(b).
[11] *Id.* § 1798.110(c)(3); Proposed Regulations § 999.305(b)(2).
[12] CCPA, CA Civil Code § 1798.140(d).

c. Disclosure of the right to request deletion of personal information

Section 999.308(b)(2)(a) of the proposed regulations requires that businesses explain that consumers have a right to request the deletion of their personal information that the business collects or maintains. This language is broader than the CCPA requirement, which states that consumers have the right to request that businesses delete personal information that "the business has collected from the consumer."[13] The regulation language should be revised to comply with the CCPA as follows: "Explain that the consumer has a right to request the deletion of their personal information collected by the business from the consumer."

d. Disclosures in response to consumer requests

Once consumers seek to exercise their rights, the proposed regulations require that businesses provide extremely detailed, personalized information. In response to access requests, businesses providing information must do so in an individualized form,[14] and businesses who do not provide specific pieces of information must explain the basis for that denial.[15] Similarly, in response to deletion requests, the proposed regulations require businesses that delete information to disclose the manner in which they deleted data from among the three options provided in the draft regulations[16] and businesses that do not delete all or some information to inform the consumer of the basis for the business's denial of the deletion request, including any statutory and regulatory exceptions.[17]

The requirement to provide such detailed, individualized information in response to subject requests imposes a significant administrative burden and cost on businesses and conflicts with federal and state laws. We recommend that these provisions be deleted or changed to allow for a more general statement of denial or disclosure of information.

e. Disclosures regarding financial incentives

The proposed regulations also require much more detailed disclosures that the CCPA text contemplates with regard to financial incentives.[18] The CCPA text requires that businesses not discriminate against consumers for exercising their rights under the CCPA, and it states that businesses may offer financial incentives but must notify consumers of the incentives. As a threshold matter, the definition of "financial incentive" in the proposed regulations is overbroad and includes programs, benefits, or offerings for the "disclosure, deletion or sale" of personal information. This definition extends beyond the language in CCPA and should be aligned more closely with the definition of financial incentive in the CCPA. In

[13] *Id.* § 1798.105(a).
[14] *Id.* § 999.313(c)(9).
[15] *Id.* § 999.313(c)(5).
[16] *Id.* § 999.313(d)(4).
[17] *Id.* § 999.313(d)(6)a.
[18] *Id.* § 1798.125.

addition, where financial incentives do exist, the proposed regulations impose significant additional obligations, including requiring that businesses offering financial incentives disclose detailed information about how they determine the value of the consumers' information and how they justify the incentive.[19]

Disclosure of such information could result in the revelation of trade secrets, pricing strategies, or other confidential business information that could result in a host of detrimental competitive impacts. The CCPA, Civil Code § 1798.185(a)(3), states that the Attorney General must adopt regulations that establish, among other things, "exceptions necessary to comply with state or federal law, including, but not limited to, those relating to trade secrets and intellectual property rights." The current proposed draft regulations do not address the protection of trade secrets or intellectual property rights. This oversight should be resolved in future drafts, and provisions like this one, which conflict with those rights, should be removed.

Such a requirement could cause an unconstitutional regulatory taking of trade secrets by forcing their disclosure. Moreover, as this measure was not contemplated by the CCPA text and there has been no study of the costs or implications of such disclosures, this provision should be struck from the proposed regulations.

f. Disclosures regarding CCPA-related metrics

Finally, sections 999.308(b)(8) and 999.317(g)(1) require that businesses that buy, receive, sell, or share personal information of four million or more consumers annually for commercial purposes, compile and share CCPA-related metrics in the annual privacy notice. This obligation is not related to any CCPA provision which would authorize it but instead appears to be original to the regulations. Moreover, the four million trigger has no basis in anything in the CCPA and is not tied to any study of the costs associated with the compilations of these statistics. These provisions are thus arbitrary and beyond the regulatory authority of the Attorney General and would impose a significant administrative burden and cost on businesses. We recommend striking both sections from the proposed regulations.

VI. The regulations should propose workable methods for opting out of the sales of personal information.

a. Treatment of browser settings as opt-out

The proposed regulations, in Section 999.315(c), require that businesses that sell personal information should treat any "user-enabled privacy controls, such as a browser plugin or privacy setting or other mechanism, that communicate or signal the consumer's choice to opt-out of the sale of their personal information as a valid request" to opt out of the sale of their personal information. While SIFMA supports

[19] *Id.* § 1798.125.

the requirement that businesses honor a consumer's request to opt out of sales, this method for opting out does not offer a reasonable approach. First, it is not clear that any browsers currently have a setting that allows consumers to select that they would like to opt out of the sales of their personal information. Instead, various internet browsers have introduced plug-ins that purport to allow consumers to signal their intention that websites not track their information. Browser plug-ins and privacy settings are not consistent across browsers and are difficult to connect to a known consumer. Indeed, a consumer that opts-out with one browser may then use a different device without an opt-out, leaving the company with conflicting and ambiguous indications of intent. For this reason, businesses have found implementation of browser settings like "Do Not Track" difficult and have instead asked consumers to indicate this directly.

The CCPA already provides a clear method for consumers to make that wish known by requiring that any business that sells information post a clear "Do Not Sell My Personal Information" in several key locations. Any user that wants to opt out of such sales will be notified and have the opportunity to do so. They will not, therefore, be deprived of the opportunity to exercise this choice by removing the requirement in § 999.315(c) and the corresponding provision in § 999.315(g), which states that browser settings should be interpreted as direct consumer requests and not requests through authorized agents. For clarity and consistency, these provisions, which were not contemplated by the text of the CCPA, should be removed.

b. Treatment of unverified deletion requests as opt-out

Similarly, Section 999.313(d)(1), which requires businesses that cannot verify the identity of a consumer making a deletion request to treat such requests as requests to opt out from the sale of personal information could have the negative consequence of opting out consumers who do not wish to opt out of sales. The verification process is in place to confirm that the right consumer's personal information is affected. If the consumer cannot be verified, the business cannot reasonably be expected to know which consumer should be opted out of the sale of information. This could lead to businesses opting out the wrong consumer and infringing on the rights of consumers who choose not to opt out from sale, but would prefer to continue to receive the benefits that may come from opting in to the sale of information, such as receiving more relevant advertising. For this reason, this provision should be struck, as it denies consumers meaningful choice about how their information is used and shared.

VII. The regulations should allow for reasonable methods for businesses to inform consumers of uses of information and should not require explicit consent for uses that are compatible with the legitimate interest of the business and are reasonably foreseeable to the consumer.

a. Notice provided at or before collection

The proposed regulations require that businesses do not collect personal information from consumers unless they give the consumer notice of the collection at or before the point of collection.[20] This language overlooks many scenarios in which subsequent notice may be permissible and where delivery of the notice at or before collection is impracticable and would delay meeting the consumer's needs. For example, where a consumer requests and authorizes the collection on a voice call, it may not be possible to provide the consumer with the notice at that time. In such situations, the regulations should allow for collection of personal information with subsequent deliver of the notice where the consumer authorizes such collection.

b. Consent for secondary use of data

In addition, the proposed regulations require business to obtain explicit consent from consumers if the business uses the consumers' personal information for a purpose that was not previously disclosed in the notice that the business provided to consumers at or before the point of collection.[21] This requirement is inconsistent with the text of the CCPA which states that consent for collection and use should be opt out. The language of the regulations should be modified to replace the explicit consent requirement with a requirement to provide consumers with notification of the secondary use of the data. Moreover, such notice should only be required for uses that are incompatible with the business purpose initially disclosed for which the personal information was collected or is not reasonably related to the product or service that the business provides. In such cases, where the new use is not reasonably foreseeable to the consumer, the collection should be allowed after the consumer receives a secondary notice of collection stating the new purposes for collection.

VIII. The regulations should allow for reasonable use of aggregate information by service providers.

The proposed regulations go beyond the provisions in the text of the CCPA that limit how service providers can use the information they receive. The regulations require that service providers do not use personal information that they receive from businesses or from a consumer's direct interaction with the service provider to provide services to any other person or entity.[22] The proposed regulations allow for

[20] *Id.* § 999.305(a)(5).
[21] *Id.* § 999.305(a)(3).
[22] *Id.* § 999.314(c).

service providers to combine personal information from multiple businesses for use on behalf of those businesses, but only "to the extent necessary to detect data security incidents, or protect against fraudulent or illegal activity."[23] The proposed regulations therefore limit the use of aggregate information by service providers.

This provision is incongruent with the law itself. The CCPA definition of "personal information," in Civil Code § 1798.140(o), explicitly states that "aggregate consumer information" is not "personal information." We recommend striking the restriction against service providers' ability to combine information from businesses, as this could have chilling effect on the provision of analytic, data science, or other research, reporting, and innovation that could have a net benefit for the businesses served by the service provider and their consumers. If specific examples are to be given, then the internal use of data to improve products and services and offer aggregated analytics and research should be recognized as a valid use.

All internal uses of aggregate data should be allowed. As explained above, companies have a commercial free speech interest in their use of data, in accordance with the U.S. Supreme Court's decision in Sorrell, 564 U.S. at 552. Consequently, the CCPA regulations are subject to heightened scrutiny and must use the least restrictive means of accomplishing their goal. Restricting internal uses of data by service providers does not further the government's interest in preventing the sale of data.

IX. The regulations should allow for the use of record-keeping information to meet legal obligations.

The proposed regulations require that businesses maintain records of consumer requests under the CCPA and prohibit businesses from using those records for any other purposes.[24] This blanket prohibition could conflict with other laws where businesses are legally required to provide such information. The regulations should be revised to allow businesses to use the information to meet legal obligations, including the use for the purpose of asserting a legal defense or defending against claims.

X. The regulations should protect the personal information of all household members equally.

The proposed regulations require that businesses who receive requests to access or delete information that pertains to a household by providing aggregate household information.[25] This practice was not contemplated by the CCPA. It raises several questions such as how to verify the individuals are in the same household, and it increases consumer privacy risks by potentially exposing information about one member of a household to other member(s) of the household. This is especially true in situations where

[23] *Id.*
[24] *Id.* § 999.317(e).
[25] *Id.* § 999.318.

roommates are unrelated and where one member of the household may wish to keep information secret from the other household member who is making the request. The regulations should clarify that nothing in this section requires or allows companies to violate the privacy of other household members when providing information to one household member.

XI. The regulations should provide clear guidance on your expectations for reasonable security and a safe harbor for those that meet those expectations.

The regulations currently do not address what information security measures are necessary to achieve a "reasonable" level of security. SIFMA suggest that the regulations include guidance about the types of processes and governance that your office would deem to be reasonable. It will be important that this guidance not attempt to dictate particular information security controls, but rather articulate the types of safeguards that are required, in much the same way as the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule. For example, the regulations could specify the following types of safeguards required by the Safeguards Rule, as appropriate to the size and complexity of the business, the nature and scope of the business's activities, and the sensitivity of any personal information at issue:

- Reasonable Administrative safeguards, such as designation of a security program coordinator, identification of risks, assessment of safeguards, training of employees, and appropriate vendor selection and oversight;
- Reasonable technical safeguards, such as risk and threat assessment, detection, prevention, response, and testing; and
- Reasonable physical safeguards, such as proper information storage and disposal, detection and prevention of physical intrusions, and protection against unauthorized access to information.

In order to incentivize corporate compliance, the regulations should also provide a safe harbor against enforcement if an independent auditor certifies the company's compliance with such a control structure. This would encourage companies to develop more robust information security practices and to have them reviewed by independent third parties. Such an expansion of the regulations would directly further the intentions of the CCPA in protecting consumer data.

XII. The regulations should clarify that provisions related to allowing consumers to opt out of the sale of their personal information do not apply to businesses that do not sell personal information.

Sections 999.330 through 999.332 of the proposed regulations relate to the sale of information. The applicability of these sections is not clearly stated in the proposed regulations, which could lead to businesses trying to comply with these regulations even if they do not sell consumer information. In such

cases, consumers may be left even more confused about how their personal information is used and shared. The regulations should clarify that these sections are inapplicable for businesses which do not sell personal information.

* * * * *

SIFMA greatly appreciates your office's consideration of the issues raised above and would be pleased to discuss these comments in greater detail. If you have any questions or need any additional information, please contact me at 202-962-7300 or Edward McNicholas at Ropes & Gray at 202-508-4779.

Sincerely,

Melissa MacGregor
Managing Director & Associate General Counsel

cc: Edward R. McNicholas, Partner, Ropes & Gray
Fran Faircloth, Associate, Ropes & Gray
Kim Chamberlain, Managing Director & Associate General Counsel, State Government Affairs