February 25, 2020

Lisa B. Kim, Privacy Regulations Coordinator  
California Office of the Attorney General  
300 South Spring Street, First Floor  
Los Angeles, CA 90013  
Email: PrivacyRegulations@doj.ca.gov

Re: Revised Proposed Regulations Under the California Consumer Privacy Act

Dear Ms. Kim:

The Bank Policy Institute (BPI)\(^1\) appreciates the opportunity to submit comments on the Attorney General's Revised Proposed Regulations, as modified on February 7 and 10, 2020, under the California Consumer Privacy Act (CCPA) (Revised Proposed Regulations).\(^2\) BPI supports numerous revisions in the Revised Proposed Regulations. For example, BPI applauds the guidance in § 999.302 regarding the interpretation of "personal information." The new language helps clarify the meaning of that important term and appears to be consistent with the intent of the CCPA. BPI also supports the revision in § 999.305(b)(2) to permit businesses to provide the business or commercial purposes for which "the categories of personal information" will be used rather than listing the business or commercial purposes for each individual category of personal information. This change will aid businesses in providing consumers with privacy policies "designed and presented in a way that is easy to read and understandable to consumers," as prescribed in § 999.308(a)(2).

I. Executive Summary

As explained in BPI's prior comment letter, the Attorney General plays a critical role in ensuring that any new requirements under the Revised Proposed Regulations are consistent with the CCPA's terms and are consistent with the intent of the CCPA. The harmonization is critical to allow businesses adequate time to test and implement strong compliance policies and processes to help consumers understand their rights and responsibilities. Financial institutions, in particular, have been required to invest significant time and resources to build compliance programs that align with both the policies set forth in the CCPA and existing federal and state financial laws. The regulations should take these programs into account and ensure that consumer protections are not unintentionally weakened by companies' CCPA compliance efforts. In Part II, we propose several amendments to the Revised Proposed Regulations in order to address these concerns.

---

\(^1\) The Bank Policy Institute is a nonpartisan public policy, research and advocacy group, representing the nation's leading banks and their customers. Our members include universal banks, regional banks and the major foreign banks doing business in the United States. Collectively, they employ almost two million Americans, make nearly half of the nation's small business loans, and are an engine for financial innovation and economic growth.

\(^2\) Cal. Civ. Code § 1798.100 et seq.
II. Proposed Amendments

A. The regulations’ effective date should be at least six months after the final regulations are published in order to account for the imposition of requirements that go beyond the statute, and the Attorney General should not bring enforcement actions for conduct that occurs before January 1, 2021.

As explained in BPI’s prior comment letter, the CCPA is a highly complex statute that requires businesses to invest significant time and resources in compliance. The Revised Proposed Regulations would add additional requirements and so will increase still further the time and resources needed for businesses to design, test, and implement compliant systems and processes. Many of these burdens are not contemplated by the CCPA itself. Thus, businesses have had less than two months to evaluate the implementation requirements of the original proposed regulations, and considerably less time to respond to Revised Proposed Regulations, much less to invest substantial resources into compliance, given the uncertain content of any final and binding rules. Requiring businesses to compress this timeline unreasonably will neither benefit consumers nor advance the goals of the CCPA.

Financial institutions face additional compliance costs given their obligations under state, federal, and international laws. For example, the CCPA does not apply to certain personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (GLBA) and the California Financial Information Privacy Act (Cal FIPA). Banks have been required to invest significant time and resources to build compliance programs that properly determine whether certain personal information falls under the scope of the CCPA and to balance the requirements of the CCPA with the GLBA and Cal FIPA.

The Revised Proposed Regulations would add further complexity to financial institutions’ compliance programs. Additional time is required to meet these compliance obligations. The regulations’ effective date should thus be at least six months after the final regulations are published, and the Attorney General should not bring enforcement actions for conduct that occurs before January 1, 2021.

B. The requirement in § 999.317(g)(2) to publish metrics regarding responses to consumer requests in a business’s privacy policy will not help consumers and may increase the risk of identity fraud. These metrics should instead be provided to the Attorney General upon request.

Subsection 999.317(g)(2) of the Revised Proposed Regulations would require covered businesses to disclose by July 1 of every calendar year “within their privacy policy or posted on their website and accessible from a link included in their privacy policy” several metrics about consumer requests they received under the CCPA and their responses to those requests. At the same time, subsection 999.308(a)(2) would require businesses to make available to consumers a privacy policy “designed and presented in a way that is easy to read and understandable to consumers.” Subsection 999.317(g)(2)’s requirement to publish metrics regarding consumer requests may make privacy policies complex and less readable, cutting against the core goals of subsection 999.308(a)(2). Publication of metrics in businesses’ privacy policies would lengthen and complicate these notices, without providing useful information about how personal information is collected and used.

Moreover, the metrics publication requirement may have the unintended consequence of creating an unfair perception of avoidance by businesses. The Revised Proposed Regulations contemplate legitimate grounds for denial of consumer requests, for example, if a business cannot verify the identity of the requestor. Financial institutions, in particular, must balance the CCPA’s consumer request requirements with existing financial laws. Requiring publication of metrics, without context, may lead consumers to think businesses are avoiding compliance with consumer access rights and deter the sharing of personal information, even when denials are based on

---

3 ld. at § 1798.145(e).
legitimate and lawful grounds. This is especially true for financial institutions collecting personal information regulated under GLBA and Cal FIPA, which may unfairly be viewed as avoiding compliance with the CCPA.

The Attorney General, instead, should require covered businesses to provide such metrics only to the Attorney General, and only upon request. Since the CCPA is enforced by the Attorney General and not by the consumers for whom a privacy policy is drafted, it would be more appropriate for businesses to be required to provide these metrics to the Attorney General upon request. Such an approach would also respect the principle embodied in subsection 11346.3(a) of the California Administrative Procedure Act, which states that an agency must consider the impact on California businesses and avoid imposing "unnecessary or unreasonable regulations or reporting, recordkeeping, or compliance requirements."

C. Subsection 999.313(c)(10) should be revised to permit businesses not to provide each category of third parties to whom they disclosed a particular category of personal information when doing so would create a substantial, articulable risk of fraud or hinder the ability of a business to comply with legal obligations.

Subsection 999.313(c)(10)’s requirement that covered businesses provide individual consumers with categories of third parties to whom they disclosed particular personal information may subject businesses to additional security risks and run afoul of existing laws. This is especially relevant for banks and other financial institutions that have reporting obligations under federal financial laws. For example, the Bank Secrecy Act requires banks and other financial institutions to submit Suspicious Activity Reports (SARs) in certain circumstances. The Act contains confidentiality requirements for SARs, including prohibitions on revealing the existence of a SAR. If an individual requesting information is the subject of a SAR, banks risk being trapped in a “catch-22,” required on one hand to comply with the CCPA’s regulations and potentially reveal the existence of a SAR; and on the other hand, obligated to comply with a federal law prohibiting the provision of that exact information.

BPI recommends that the Revised Proposed Regulations be further revised to permit businesses not to provide each category of third parties to whom they disclosed that particular category of personal information when doing so would create a substantial, articulable risk of fraud or hinder the business’s ability to comply with legal obligations. Such an exemption would be consistent with federal laws. For example, § 1033(b)(2) of the Dodd Frank Act exempts financial institutions from providing consumers with information collected for “the purpose of preventing fraud or money laundering, or detecting, or making any report regarding other unlawful or potentially unlawful conduct." Furthermore, such a statement would support the provisions set forth in Section 1798.145(a)(1-3) of the CCPA that the law shall not restrict a business’s ability to comply with relevant federal, state, or local laws and cooperate with law enforcement. In the absence of a general exemption in § 999.313(c)(10), BPI requests a specific exemption for banks and other financial institutions subject to federal financial laws.

D. Language added in § 999.314(e) about service providers responding to consumer data requests on behalf of businesses may (incorrectly) be read to permit service providers to respond without notice to or consent of the involved business, thereby possibly opening businesses up to unauthorized exposure of data, encouraging fraud, or facilitating violations of federal financial laws.

The CCPA contemplates that businesses that collect personal information from consumers act as the controller of that information. Enabling service providers to make decisions unilaterally as to how to respond to consumer data requests jeopardizes businesses’ ability to sufficiently control that information and comply with the

---

4 See, e.g., 31 U.S.C. §§ 5318(g)(2), 5321, and 5322.
5 12 U.S. Code § 5533(b)(2).
6 See, e.g., id. at § 1798.140(c)(defining “business” as an organization meeting certain criteria “that collects consumers’ personal information or on the behalf of which that information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information.”) (emphasis added).
CCPA’s requirements. This is an issue that, under the CCPA’s terms, should be handled in contract negotiations between the covered entity and its service providers rather than being mandated by regulation.

Financial institutions may face additional compliance problems due to subsection 999.314(e)’s apparent blessing of service providers unilaterally responding to consumer data requests. As outlined previously, financial institutions are required to have protocols to protect consumer financial data under federal and state financial laws. Specifically, financial institutions must have vendor management protocols that outline a vendor’s ability to use, disclose and process consumer financial data. 7 Enabling vendors to directly respond to consumer data requests, without input from financial institutions, may run afoul of such financial laws. Likewise, service providers may lack the tools and capabilities to properly verify consumer data requests, which may lead to exposure of data or fraudulent activity.

For these reasons, subsection 999.314(e) should be omitted from the final regulations. At a minimum, if it is retained, it should be revised to make clear that covered businesses may prohibit service providers by contract from responding to consumer data requests on their behalf.

E. The Attorney General should add back in subsection 999.313(c)(3) the requirement that a “business 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.”

The Revised Proposed Regulations would ease the burden on businesses in responding to consumer requests when a business does not maintain personal information in a searchable or reasonable format and certain other conditions are met. At the same time, however, the Revised Proposed Regulations omit a critical protection for both businesses and consumers by eliminating the ability of a business not to provide specific pieces of information when doing so would pose a risk to the security of personal information, consumer accounts, or businesses’ systems or networks. No alternative protections appear in the Revised Proposed Regulations so the reason for removing this provision is unclear. For the protection of consumers, a business should be afforded the flexibility to only provide categories of information when it determines that disclosure of personal information in a given circumstance would pose a substantial, articulable security risk. Adding this exception back into the Revised Proposed Regulations would maintain a critical security measure to protect consumers and businesses. Moreover, adding flexibility for businesses to protect their records and systems would not harm consumers because they still would be able to understand the data maintained and exercise their rights in accordance with relevant laws.

F. Language added in § 999.317(e) prohibiting sharing information obtained for record keeping purposes with third parties should be revised to clarify that businesses should be able to share such information as required by applicable law and for security and anti-fraud purposes.

Subsection 999.317(e)’s prohibition on sharing information maintained for record keeping purposes with third parties may subject businesses to additional security risks and run afoul of existing laws. For example, personal information businesses obtain for recordkeeping purposes may also be useful for security and anti-fraud purposes. Allowing a security and anti-fraud exception to this requirement could serve a narrow and legitimate business need and pose no discernable risk of consumer harm from secondary uses of the information.

As noted above, financial institutions are required to maintain and submit certain records to applicable federal and state regulators as part of its compliance program. The language in § 999.317(e), as written, may put financial institutions in a position to have to decide whether to comply with federal and state financial laws or the CCPA. BPI asks that § 999.317(e) be revised to enable businesses to share information maintained for record

---

keeping purposes where required by applicable law and where shared for security and anti-fraud purposes. Such a statement would also support statutory language in Section 1798.145(a)(1-3) of the CCPA that states that the law shall not restrict a business's ability to comply with relevant federal, state, or local laws and cooperate with law enforcement.

*****

The Bank Policy Institute appreciates the opportunity to submit comments on the Attorney General's Revised Proposed CCPA Regulations. If you have any questions, please contact the undersigned by phone at 202-589-1935 or by email at Angelena.Bradfield@bpi.com.

Respectfully submitted,

Angelena Bradfield
Senior Vice President, AML/BSA, Sanctions & Privacy
Bank Policy Institute