BANK POLICY INSTITUTE

March 8, 2019

Via Electronic Mail

California Department of Justice
Attn: Privacy Regulations Coordinator
300 South Spring Street
Los Angeles, CA 90013

Re: Preliminary Rulemaking Request for Comment concerning the California Consumer Privacy Act

Ladies and Gentlemen:

The Bank Policy Institute[1] appreciates the opportunity to respond to the California Attorney General's request for preliminary rulemaking comments on implementing the California Consumer Privacy Act ("CCPA").[2] BPI member banks are dedicated to protecting customer data and have adopted robust privacy and information security programs with administrative, technical, and physical safeguards to assist in such efforts. These programs are designed pursuant to and consistent with the requirements of state, federal and international laws – notably the Gramm-Leach-Bliley Act ("GLBA") and its implementing regulations.[3] Therefore, BPI member banks already adhere to notice and disclosure requirements, protect the security and confidentiality of customer information, protect against any anticipated threats or hazards to the security or integrity of customer information, and protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to customers.[4] These programs are tailored to the size, complexity, activity, and overall risk profile of a bank as contemplated under federal law.[5]

---

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 2 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.*

3 15 U.S.C. §§ 6800 *et seq.* and implementing regulations.

4 As noted by President Clinton, the GLBA requires banks to "clearly disclose their privacy policies to customers up front…consumers will have an absolute right to know if their financial institution intends to share or sell their personal financial data, either within the corporate family or with an unaffiliated third-party [and]…will have the right to "opt out" of such information sharing with unaffiliated third parties…[and] allows privacy protection to be included in regular bank examinations…[and] grants regulators full authority to issue privacy rules and to use the full range of their enforcement powers in case of violations." *See* William J. Clinton, Statement on Signing the Gramm-Leach-Bliley Act, November 1999. *Available at* web.archive.org/web/20160322081604/http://www.presidency.ucsb.edu/ws/?pid=56922; *accessed* March 1, 2019.

5 Interagency Guidelines, 12 C.F.R. pt. 30, app. B, § II.A.

As an initial matter, data transparency is inherent in a bank's business model. Banks provide customers with account information through statements or other written notices, online services, mobile banking applications, and other tools that allow customers direct access to categories of information the bank collects on them. In addition, financial institutions provide disclosures to their customers and the general public that detail the categories and types of data they collect, the ways in which it is used, and how to further inquire about collected information.[6]

Banks use a wide range of physical and technical safeguards regarding the collection, storage, use, access, and delivery of information, including physical access restrictions, firewalls, intrusion detection and threat monitoring tools, and encryption technologies. These safeguards are carefully tailored to reflect the scope of individual bank activities and the sensitivity of the personal information collected and stored. Furthermore, bank GLBA-compliant privacy programs are tested and continually updated and subject to evaluation and review by compliance, IT and internal audit professionals as well as executive management and boards of directors. Finally, both in scale and scope and in terms of the already existing regulatory framework, such programs are also subject to exams conducted by federal and state regulators.

Given the extensive privacy and data security programs banks already employ, which differ from those utilized by other sectors of the economy, it is important that any rulemaking undertaken by the California Attorney General recognize and align with these long-standing and effective frameworks in the financial institution space.[7] This is particularly important when determining the law's implementation date and further clarifying the definition of covered information.

I. Any rule should focus on protecting information that a customer provides to a business in their personal capacity, consistent with the CCPA's legislative intent, and account for the robust privacy frameworks financial institutions already have in place.

Both the preamble to the CCPA and its legislative history make clear that the purpose of the law is to protect information relating to a consumer's relationship with a business for personal, family or household purposes. As noted in the preamble, "[m]any businesses collect personal information from California consumers. They may know where a consumer lives and how many children a consumer has, how fast a consumer drives, a consumer's personality, sleep habits, biometric and health information, financial information, precise geolocation information, and social networks…California consumers should be able to exercise control over their personal information, and they want to be certain that there are safeguards against misuse of their personal information." This focus is reinforced by the law's definition of personal information which is tied to the ability to reasonably link data to "a particular consumer or household,"[8] as well as the law's focus on the rights a customer has to understand how a business collects and uses its information.

Such expectations should be made clear through the rulemaking process in order to clarify that data collected outside of the interaction a customer has with a business in their personal capacity, notably through commercial and other relationships, is not covered by the law given its broad definitions of consumer and personal information. Ensuring clarity on this point is particularly important in the context of the definition of personal information as presently it could be, albeit inappropriately, read to grant members of a consumer's household rights intended for only an individual consumer – including information access, disclosure and deletion rights. Such a result

---

6 Under the GLBA, financial institutions must provide notice of its privacy policies and practices, and in certain circumstances, allow the consumer to opt out of the disclosure of its nonpublic personal information to affiliates and nonaffiliated third parties. 15 U.S.C. § 6802(b). We note that covered financial institutions are also required to obtain consent prior to sharing information with nonaffiliated parties under the California Financial Information Privacy Act.

7 Indeed, the CCPA acknowledges the strength of this federal framework in Section 1798.145(e).

8 Section 1798.140(o)(1).

would clearly be inconsistent with the legislative intent of the CCPA and therefore should be further clarified in any rulemaking.

In addition, as presently drafted, the CCPA could be read to capture data collected outside of the relationship a business has with a consumer, like employee, contractor, or job applicant data. Employee information is already covered by state and federal laws that govern its protection and confidentiality. For example, it is subject to the Health Insurance Portability and Accountability Act ("HIPAA"), which protects health-related data, and California's breach notification laws[9] which protects such data from unauthorized disclosure and affords substantial protections to that data. Furthermore, as described above, such relationships appear to be outside the scope of the legislative intent of the law. The CCPA contemplates this and similar circumstances by providing the Attorney General with the authority to "[e]stablish[] any exceptions necessary to comply with state or federal law including, but not limited to, those relating to trade secrets and intellectual property rights within one year of passage of this title and as needed thereafter."[10] Therefore, given the protections already afforded this information and the Attorney General's clear statutory authority to exempt such information from being covered by the CCPA, we strongly recommend that any rulemaking defer to the privacy frameworks that banks already have in place for safeguarding employee information.

II. CCPA compliance requirements and enforcement activity should commence 12 months after regulatory standards are finalized.

As acknowledged by Attorney General Becerra in his August 22, 2018 letter to members of the California legislature, the promulgation of regulations requires a "sufficient and realistic amount of time" for rulemaking to be conducted.[11] The same is true for companies subject to such regulations, as they will have to review their existing processes against the requirements of the law and any implementing regulations, develop plans to adapt their programs – both technologically and administratively – to address new or different expectations, and test those new processes prior to implementing the revised program. This analysis is further complicated by a consumer's right to request from a business "categories and specific pieces of personal information the business has collected," and once the request has been verified, the obligation of the business to disclose the personal information collected in the preceding 12 months.[12] As the CCPA's effective date is January 1, 2020, and the deadline for rulemaking is July 1, 2020, there is ambiguity as to when businesses need to be in compliance with the law, much less its 12-month look-back period. Given the operational components banks will be required to put in place to address the Attorney General's regulations, a transitional implementation period of a minimum of 12 months ("implementation date") should be provided to firms to establish and test compliance procedures that reflect the regulations promulgated under the statute. Furthermore, any "look back" requirements and enforcement activity should commence upon the implementation date of the CCPA's regulations. This approach is not unprecedented, the federal government has set similar precedents on data subject to "look back" and enforcement provisions.[13]

* * * * *

---

9 Cal. Civ. Code §§ 1798.82 and 1798.84.

10 Section 1798.185(a)(3).

11 Letter from Attorney General Xavier Becerra re "California Consumer Privacy Act," August 22, 2018. *Available at* digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=2801&context=historical; *accessed* March 1, 2019.

12 Section 1798.100(a) and 1798.130(a)(2).

13 For example, in 2016, the Financial Crimes Enforcement Network chose not to require identification of beneficial owners on a "look back" basis, prior to the May 11, 2018 implementation date of its Customer Due Diligence rule as it felt it would be "unduly burdensome" due to the "significant changes to processes and systems that [covered institutions were] required to implement" under the rule. *See* 81 Fed. Reg. at 29, 404.

The Bank Policy Institute appreciates the opportunity to submit preliminary rulemaking comments concerning the CCPA. 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

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