



December 6, 2019

**VIA ELECTRONIC SUBMISSION**

Privacy Regulations Coordinator  
California Office of the Attorney General  
300 South Spring Street, First Floor  
Los Angeles, CA 90013  
Email: [PrivacyRegulations@doj.ca.gov](mailto:PrivacyRegulations@doj.ca.gov)

**Re: Notice of Proposed Rulemaking Regarding the California Consumer Privacy Act**

Dear Mr. Becerra:

The Consumer Bankers Association<sup>1</sup> (“CBA” or “the Association”) appreciates the opportunity to offer our views on the California Attorney General’s (“the Attorney General” or “the AG”) Notice of Proposed Rulemaking (the “Proposed Rule” or the “Draft Regulations”) concerning California’s regulatory approach to the California Consumer Privacy Act (the “Act” or “the CCPA”).

CBA appreciates the Attorney General’s efforts to provide guidance to businesses on how to comply with the CCPA and to clarify the Act’s requirements through proposed regulations. Most importantly, CBA’s member banks share the Attorney General’s goal of protecting the privacy of consumers. However, we have significant concerns about the proposed regulations as drafted by the Attorney General. Below, we have identified our most pressing issues and offered the Attorney General solutions to consider in the next phase of the rule writing process.

**I. The Attorney General’s Right to Opt-Out of Sale Guidance is Insufficient to Address Practical Business Concerns.**

CBA urges the Attorney General to provide more certainty about the right to opt-out of sales of personal information. From a review of the draft regulations, it seems a bank, or any covered entity, may present the choice to opt-out of certain sales, so long as a global option to opt-out of the sale of all personal information is more prominently presented than other choices. Note, this option assumes a global option is feasible. From a practical perspective, it is likely a business may possess varying data elements about a single consumer through different relationships with the consumer, which may not be linked.

Moreover, the proposed regulations require a bank, or covered entity, which collects personal information from consumers online to “treat user-enabled privacy controls, such as browser plugin or privacy setting or another mechanism, which communicates or signal the consumer’s choice to opt-out of

---

<sup>1</sup> The Consumer Bankers Association is the only national trade association focused exclusively on retail banking. Established in 1919, the Association is now a leading voice in the banking industry and Washington, representing members who employ nearly two million Americans, extend roughly \$3 trillion in consumer loans, and provide \$270 billion in small business loans.

the sale as a valid request” to opt-out of sale of personal information “for that browser or device, or, if known, for that consumer.” This raises a number of operational complexities and issues since neither the statute nor the proposed regulations condition this opt-out method being a well-established or widely used standard to communicate requests to opt out of sale of personal information.

## **II. Provide Covered Entities with a Safe Harbor When Verifying Consumer Requests.**

The CCPA establishes a series of rights which are contingent upon the receipt and authentication of a “verifiable consumer request.” In order to comply with a consumer’s request to exercise his or her rights under the CCPA, the “business shall promptly take steps to determine whether the request is a verifiable consumer request.”

CBA appreciates the Attorney General for providing helpful guidance related to verification requests. Generally, the proposed regulations direct banks to use a more rigorous verification process when dealing with more sensitive information. The proposed regulations also take it a step further by directing banks not to release sensitive information without being highly certain about the identity of the individual requesting the information. The proposed regulations also provide prescriptive steps of what to do in cases where an identity cannot be verified.

As the Attorney General is aware, banks collect personal information as part of routine transactions to facilitate consumer requests. Even with the proposed rules, furnishing personal information to customers purporting to exercise their rights under the CCPA, in response to a verifiable consumer request, may result in unintended risk and harm to the consumer, including misuse of personal information to perpetuate fraud and identity theft. As a potential solution, the Attorney General should establish a safe harbor from liability to assure banks, and other covered entities, that rejecting a suspicious right of access request in good faith will not later result in a violation.

Moreover, CBA implores the Attorney General to look to the implementation issues encountered by the General Data Protection Regulation (GDPR) in its next stage of rule writing. According to a study published by Blackhat USA 2019 (“the Study”)<sup>2</sup>, the Study demonstrates how legal ambiguity surrounding the “right of access” process may be used by social engineers to facilitate fraud. The Study’s experimental findings also demonstrate many organizations fail to adequately verify the originating identity of right of access requests. As a result, social engineers can abuse right of access requests as a scalable attack mechanism for acquiring deeply sensitive information about individuals.

The Attorney General’s proposed regulations do not seem to consider the prevalence and petulance of social engineers. Without a safe harbor from liability, banks may be hesitant to reject the legitimacy of consumer requests for fear of potential enforcement actions. Thus, the Attorney General’s oversight would allow more potential gateways for social engineers to exploit legal and policy loopholes.

As the CCPA is set to apply to various industries, CBA also encourages the Attorney General to better consider a business’ size and complexity, the nature and scope of its business activities, and the sensitivity of any personal information at issue. In alternative, the Attorney General may consider

---

<sup>2</sup> <https://i.blackhat.com/USA-19/Thursday/us-19-Pavur-GDPArrrrr-Using-Privacy-Laws-To-Steal-Identities-wp.pdf>

utilizing principles such as those found in existing authentication guidance issued by the Federal Financial Institutions Examination Council.

### **III. The CCPA as Proposed is Potentially Harmful for Consumers' Information.**

Building on the previous discussion, CBA encourages the Attorney General to finalize a rule which does not put consumers at any additional risk of fraud or identity theft. The proposed regulations impose new disclosure obligations beyond those enumerated in the statute.

In particular, the proposed disclosures require banks, and other covered entities, to specify a potentially concerning level of detail about certain privacy practices. For example, the draft would require a business to address the following new disclosures:

- Describe the process the bank will use to verify the consumer request, including any information the consumer must provide;
- Explain how a consumer can designate an authorized agent to make a request under the CCPA on the consumer's behalf; and
- For each category of personal information collected, provide the categories of sources from which the information was collected, the business or commercial purposes(s) for which the information was collected, and the categories of third parties with whom the business shares personal information.

As previously mentioned, banks are constantly having to safeguard and mitigate against potential and real fraud. The CCPA as proposed seems to be another apparent path for fraudsters to attempt to infiltrate the banking system and harm real consumers.

### **IV. The CCPA Should Protect the Intellectual Property Rights of Covered Entities.**

As the proposed rules are currently written, CBA believes the CCPA may infringe on the intellectual property rights of our member banks. Pursuant to § 1798.185(a)(3), the CCPA grants the Attorney General the authority to establish "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."

Furthermore, we urge the Attorney General to include a rule to establish an exception from the CCPA for intellectual property or for data which, if disclosed, would have an adverse effect on the rights or freedoms of others. The CCPA should not apply to information which is protected intellectual property of a bank, or any other covered entity, including information subject to copyright, patent, service mark and/or trade secret protections. A bank also should be required to disclose any information which is subject to intellectual property protections, including any formula, pattern, compilation, program, device, method, technique or process developed to process or analyze personal information, or any information derived from such process or analysis.

The Attorney General should consider duplicating the EU's GDPR approach to intellectual property. The GDPR places reasonable limitations on its enumerated consumer privacy rights. It provides both an intellectual property exclusion and the avoidance of infringement on the rights of others. CBA believes its

member banks, and other covered entities, deserve the same protections if a bank is presented with a scenario where its attempt to comply with a consumer's request may put it in the position of violating the rights of others or placing it in jeopardy with its competitors.

**V. The Definition of "Sell" is too Broad and Unnecessarily Burdensome.**

The CCPA includes definition for "sell" as follows:

"(t)(1) "Sell," "selling," "sale," or "sold," means selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration. (2) For purposes of this title, a business does not sell personal information when: (A) A consumer uses or directs the business to intentionally disclose personal information or uses the business to intentionally interact with a third party, provided the third party does not also sell the personal information, unless that disclosure would be consistent with the provisions of this title. An intentional interaction occurs when the consumer intends to interact with the third party, via one or more deliberate interactions. Hovering over, muting, pausing, or closing a given piece of content does not constitute a consumer's intent to interact with a third party. (B) The business uses or shares an identifier for a consumer who has opted out of the sale of the consumer's personal information for the purposes of alerting third parties that the consumer has opted out of the sale of the consumer's personal information.

(C) The business uses or shares with a service provider personal information of a consumer that is necessary to perform a business purpose if both of the following conditions are met: (i) The business has provided notice that information being used or shared in its terms and conditions consistent with § 1798.135. (ii) The service provider does not further collect, sell, or use the personal information of the consumer except as necessary to perform the business purpose. (D) The business transfers to a third party the personal information of a consumer as an asset that is part of a merger, acquisition, bankruptcy, or other transaction in which the third party assumes control of all or part of the business, provided that information is used or shared consistently with § 1798.110 and 1798.115. If a third party materially alters how it uses or shares the personal information of a consumer in a manner that is materially inconsistent with the promises made at the time of collection, it shall provide prior notice of the new or changed practice to the consumer. The notice shall be sufficiently prominent and robust to ensure that existing consumers can easily exercise their choices consistently with § 1798.120. This subparagraph does not authorize a business to make material, retroactive privacy policy changes or make other changes in their privacy policy in a manner that would violate the Unfair and Deceptive Practices Act (Chapter 5 (commencing with § 17200) of Part 2 of Division 7 of the Business and Professions Code)."

CBA urges the Attorney General to provide more clarification about the covered activities in its definition of "sell." The definition as written is too general and too open-ended. There are a myriad of activities which would possibly fall within the CCPA's current definition of sale, which see beyond the scope of the law's actual public policy concerns. For example, cookies embedded on a bank's website could currently be construed to be covered under the current definition of "sell." As an additional practical complexity posed by the CCPA, it is also unclear how a bank's interactions with the Google

search engine or via an ad placed on Facebook would be treated under the current definition. There is also a lack of clarity about what constitutes valuable consideration under the CCPA.

Note, banks, and other covered financial institutions, are also unsure about the scope of the CCPA's Gramm-Leach-Bliley exception. The Attorney General should draft rules to provided banks, and other covered entities, with the clarity needed to comply with this comprehensive privacy law.

## **VI. Transfers of Personal Information to Service Providers is Not a Sale.**

Banks, and other financial institutions, transfer personal information to service providers to maximize the consumer experience by providing products and services. These transfers are not sales as contemplated in the CCPA, and the final regulations should clarify this distinction for service providers. Section 999.314 proposes a covered entity which otherwise meets the definition of a service provider is a service provider even if it collects personal information directly from consumers at the request of a business.

Note, the proposed rules also state a service provider which also meets the definition of a business must comply with the CCPA for any personal information it collects or sells outside of its role as a service provider. CBA supports this proposed clarification regarding service providers, and we urge the Attorney General to consider further clarifications. A final rule with additional clarity is essential to ensure banks, and other financial institutions, can transfer personal information to a service provider to benefit the bank's customers without the transfer being deemed a sale of personal information pursuant to the CCPA.

## **VII. Provide More Clarity Concerning the "Right to Cure."**

Section 1798.155(b) states, in part, a "[bank] shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance." To begin, the Attorney General's regulations did not propose any rules to codify this provision of the CCPA. CBA urges the Attorney General to establish specific criteria for what is necessary in order for a bank, or other covered entity, to successfully "cure" a violation.

The Attorney General should provide more detailed guidance. For example, there may be a circumstance where a cure cannot unwind the effects of a violation, guidance is needed as to other means in which the bank, other covered entity, could cure, or mitigate against, the violation through implementation of enhanced business practices.

## **VIII. The "Lookback" Period Should Begin January 1, 2020.**

As the proposed rules are currently written, the CCPA appears to apply retroactively by requiring businesses to provide information subject to a consumer's request covering the time period prior to the Act's effective date and prior to the publication of implementing regulations. CBA believes rulemaking should clarify the 12-month lookback period provided for in § 1798.130 applies from the effective date of

the CCPA, which is January 1, 2020. This change would preclude its application to activities occurring prior to the effective date.

**IX. Establish an Effective Date for Final Rules to Allow Covered Entities Adequate Time to Comply.**

The Attorney General should exercise its discretionary authority to set an effective date of 18 months after the final rules are issued. CBA believes this extension is essential so banks, and other covered entities, can properly comply. Banks will need sufficient time to review and implement direction from the Attorney General's final regulations, which may require changes to implementation plans which were based in good faith on the statutory language, prior to regulations being adopted.

For example, the final regulations will require banks, and other covered entities, to change their verification processes due to the CCPA's prescriptive requirements, e.g. "double" authentication for deletion, declaration signed under penalty of perjury, etc. These potential changes and clarifications will require development work, testing and validation, and employee training. Truncating these necessary steps into a potentially short time frame, e.g. 1 month, may create the undue operation risk of either not properly verifying a valid request or disclosing information to the incorrect person. These types of risks are anti-consumer and preventable.

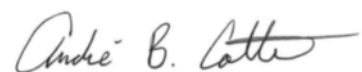
Currently, the CCPA's deadline for the Attorney General's rulemaking is July 1, 2020, six months after the law's January 1 effective date. Pursuant to the CCPA, the Attorney General could technically begin enforcement of the CCPA on July 1, 2020, which is the same day the final rules could be published. This would be an unreasonable request for covered entities. CBA supports the goal of consumer privacy protection, however, the CCPA is complex and in part, unclear. Banks, and other covered entities, will need sufficient time to come into full compliance to ensure they implement the full privacy protections as intended by the legislature to ultimately benefit consumers.

**X. Establish an Enforcement Date of No Earlier than July 1, 2020.**

CBA urges the Attorney General to preclude any enforcement action based on conduct or omission occurring on or after the enforcement date. The CCPA provides in §1798.185(c), the "Attorney General shall not bring an enforcement action under this title until six months after the publication of the final rule issued pursuant to this section or July 1, 2020, whichever is sooner." For example, if the enforcement date is July 1, 2020, because it is earlier than the six-month anniversary of final regulations, the AG should clarify any enforcement will be based only on conduct or omissions occurring July 1, 2020 or later and not conduct or omissions occurring on or after the CCPA effective date, January 1, 2020.

CBA appreciates the opportunity to comment on the Notice of Proposed Rulemaking, and we plan to continue to engage the California Office of the Attorney General as the rulemaking process continues and to ensure our member banks have the necessary guidance to comply with the tenants of the final rule. Please feel free to contact André Cotten for further discussion regarding our comments at [Acotten@consumerbankers.com](mailto:Acotten@consumerbankers.com) or 202-552-6360.

Sincerely,

A handwritten signature in black ink, reading "Andre B. Cotte". The signature is written in a cursive style with a long horizontal flourish extending to the right.

---

Assistant Vice President, Regulatory Counsel  
Consumer Bankers Association