

Chapman Client Alert

January 6, 2020

Current Issues Relevant to Our Clients

New California Consumer Privacy Rules Now in Effect. What Should Financial Institutions Be Doing?

The California Consumer Privacy Act of 2018 (CCPA) went into effect on January 1, 2020 and imposes extensive disclosure and record-keeping requirements on businesses that handle personal information. By its terms, the CCPA only applies to the personal information of consumers. However, it defines “personal information” as meaning all information relating to, identifying or in any way linked to a particular person or household, including names, email addresses, IP addresses and postal addresses.¹ And it defines “consumer” as meaning any natural persons residing in California, including customers, potential customers and even employees. Therefore, covered businesses that collect practically any useful information about any natural person residing in California need to put systems in place in order to comply with the law.

Broadly speaking, the CCPA imposes three kinds of requirements on covered businesses, including financial institutions:

1. **Right to Know.** Businesses that collect consumer information must have systems in place to inform consumers at or before the point of collection of the categories and specific pieces of information that they collect² and to deliver copies of the collected information without charge to consumers making a “verifiable consumer request” for that information.³ If the business sells any of this information or otherwise discloses it for a “business purpose”, consumers have the right to request that the business provide them with the information sold or disclosed—again, after the consumer makes a “verifiable consumer request.”⁴
2. **Right to Delete.** The CCPA requires that businesses make a toll-free number and at least one other method available through which consumers can exercise the right to have their personal information deleted.⁵ A business is not required to delete personal information it needs to provide goods or services requested by the consumer or perform a contract between the company and the consumer, or that is needed for security or other specified uses.⁶
3. **Right to Opt Out.** The CCPA gives consumers the right to opt out and prevent the business from selling or disclosing their personal information to third parties, and also prohibits businesses from selling or disclosing the personal information of consumers known to be less than 16 years old without, in the case of consumers between

the ages of 13 and 16, the consumer’s or its parent’s or guardian’s affirmative consent, and in the case of consumers who are less than 13 years old, the guardian’s or parent’s affirmative consent.⁷ California Attorney General Xavier Becerra has publicly stated that his office will prioritize, at least initially, enforcement of these parental consent rights.⁸ Under the CCPA, businesses are also required to provide consumers with a notice of their right to opt out, and regulators are currently in the process of drafting implementing regulations that will extensively describe the form and content of these notices.

The CCPA further prohibits businesses from discriminating against consumers on the basis of their decision to exercise any rights under the CCPA, except to the extent the differential treatment is reasonably related to value provided to the business by the consumer’s data.⁹

Exceptions and Exemptions

The “right to delete” provision of the CCPA are subject to a number of important exceptions. As mentioned above, businesses can preserve personal information needed to provide goods or services requested, or reasonably likely to be requested, by the consumer. Businesses can also retain personal information, among other things, needed to detect security incidents, debug or repair functionality, exercise free speech, and comply with other provisions of law.¹⁰ However, fewer exceptions apply to a consumer’s “right to know” about the information that is collected and the “right to opt out” of sale or disclosure to third parties.

One important exception to the opt out provisions of the CCPA is for the sale and disclosure of credit reporting information. Previously, the text of the CCPA contained a limited exception for the sale or disclosure of personal information used to generate a “credit report.” However, in October 2019, California’s governor signed a number of last-minute bills amending various aspects of the CCPA, one of which expanded the credit reporting exemption. In its current form, the CCPA does not apply to the “collection, maintenance, disclosure, sale, communication, or use of any personal information bearing on a consumer’s credit worthiness”—whether or not that information is used to generate a credit report—but only to the extent that the activity is governed by the Fair Credit Reporting Act.

Another important and potentially sweeping exception to the provisions of the CCPA is for banks and other financial institutions subject to the Gramm-Leach-Bliley Act (GLBA) or the California Financial Information Privacy Act (FIPA). Specifically, by its terms, the CCPA does not apply to “personal information collected, processed, sold or disclosed pursuant to” the GLBA or its implementing regulations, or the FIPA.¹¹ The GLBA itself contains two major consumer protections. First, it imposes the Safeguards Rule, requiring financial institutions to implement comprehensive information security programs to ensure the confidentiality of their customers’ information.¹² Second, it generally requires financial institutions to inform and allow consumers to opt out of disclosures of their personal information to nonaffiliated third parties. The FIPA contains even stronger disclosure regulations and prohibits financial institutions from selling or sharing nonpublic personal information with nonaffiliated third parties without the consumer’s explicit prior consent.¹³

Scope of GLBA Exemption

The million-dollar question is whether all consumer information that a financial institution safeguards counts as “collected, processed, sold or disclosed pursuant to” the GLBA or the FIPA such that all such information is exempt from regulation by the CCPA. If so, then banks will be largely exempt from the “right to know”, “right to delete” and the “right to opt out” provisions of the CCPA. However, the legislative history of the CCPA and the currently proposed administrative guidance shed little light on the intended breadth of the GLBA/FIPA exemption.

It is likely that regulators will take the view that safeguarding is different from “collect[ing], process[ing], [selling] or disclos[ing] pursuant to” the GLBA or the FIPA, and that the exemption was narrowly intended to reconcile the conflicting opt out regimes under the CCPA, the GLBA and the FIPA. In this case, banks will be forced to comply with the “right to know”

and “right to delete” provisions of the CCPA—which have no analog in the GLBA or the FIPA.

In any event, regardless of how regulators interpret the GLBA/FIPA exemption, banks need to be aware that certain categories of information likely fall outside the exemption altogether. The GLBA and FIPA regulate how institutions treat the information of “consumers”, defined in both laws to mean the information of natural persons that obtain a financial product or service from the institution for personal or household purposes.¹⁴ Therefore, if a bank either (i) handles information about a consumer without providing a product or service to that consumer, or (ii) handles information about an individual in connection with a commercial, as opposed to personal or household, transaction (such as information of an individual guarantor or signing officer),¹⁵ then the information is not handled “pursuant to” the GLBA or the FIPA and the bank must comply with all provisions of the CCPA regarding the handling of this information. Unsurprisingly, during the period of public comment on proposed implementing regulations promulgated by the California Attorney General, many banks, credit unions and other financial institutions expressed frustration that the non-overlapping definitions in the CCPA, GLBA and FIPA make the scope of the intended exemption unclear.

Finally, the CCPA governs how a business handles the personal information of its employees, a category of information that clearly is not impacted by the GLBA/FIPA exemption. However, note that most provisions of the CCPA do not become effective as to employee information until January 1, 2021.¹⁶

Next Steps

While the GLBA exception gives financial institutions some welcome sanctuary from dual and possibly conflicting state and federal regulatory regimes, bank compliance departments will still need to wrestle with the wide-ranging scope of the CCPA and the lack of clarity on the exemptions for information collected, processed, sold or disclosed pursuant to GLBA and FIPA while updating their privacy policies and procedures. Financial institutions need to (i) assess what information is being collected about consumers and households across all business units, (ii) establish internal policies about what personal information in their possession is subject to the CCPA but not the GLBA or FIPA, (iii) establish internal policies, procedures and compliant timelines for identifying, verifying and responding to consumer requests regarding information collection and deletion and opt out requests related thereto and (iv) publish updated privacy policies that notify California consumers about their rights under the CCPA and how to exercise them. Updated internal policies will also need to

address a financial institution's information sharing with vendors and other third parties to ensure that such sharing is either exempt from CCPA or that such third parties are also notified and required to comply with such requests (or the financial institution's directives regarding requests that it has received).

The California Attorney General has stated that it will not delay enforcement of the CCPA until implementing regulations are finalized, which is expected to occur in July 2020. However, his office will take into consideration the good faith efforts of businesses that might lack the resources immediately to come into compliance.¹⁷

As of early January 2020, we are seeing many websites that have already posted updated privacy policies with notices specific to the CCPA and we are seeing some websites that

include links to the updates that pop-up the first time the site is accessed after posting of the updated policies.

For More Information

If you would like further information concerning the matters discussed in this Client Alert, please contact any of the following attorneys or the Chapman attorney with whom you regularly work:

Marc P. Franson

Chicago
312.845.2988
franson@chapman.com

Melanie J. Gnazzo

San Francisco
415.278.9020
mgnazzo@chapman.com

- 1 The term "personal information" is defined to mean: "information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household...Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers." Cal. Civ. Code § 1798.140(o).
- 2 Cal. Civ. Code § 1798.100.
- 3 Cal. Civ. Code § 1798.110.
- 4 Cal. Civ. Code § 1798.115. The CCPA defines a "verifiable consumer request" to mean "a request that is made by a consumer, by a consumer on behalf of the consumer's minor child, or by a natural person or a person registered with the Secretary of State, authorized by the consumer to act on the consumer's behalf, and that the business can reasonably verify, pursuant to regulations adopted by the Attorney General pursuant to paragraph (7) of subdivision (a) of Section 1798.185 to be the consumer about whom the business has collected personal information." (Id. § 1798.140 subd. (y).) The Attorney General has proposed implementing regulations that contain general guidelines on how businesses are supposed to verify a consumer's identify, and require, among other things, that when a business receives a request to delete personal information, it adjust the degree of certainty needed to verify the consumer's identity relative to the sensitivity of the information in question. Cal. Code Regs. tit. 11 §999.323-326.
- 5 Cal. Civ. Code § 1798.105.
- 6 Cal. Civ. Code § 1798.105, subd. (d).
- 7 Cal. Civ. Code § 1798.120.
- 8 *California Promises Aggressive Enforcement of New Privacy Law*, S.F. Chronicle (Dec. 16, 2019), available at <https://www.sfchronicle.com/politics/article/California-promises-aggressive-enforcement-of-new-14911017.php?t=f1df9802a8>.
- 9 During the ongoing rule making process, many businesses and interested parties have asked regulators to clarify what it means for differential treatment to be "reasonably related" to value provided to the business and if and how businesses will be expected to quantify this value and document compliance.
- 10 Cal. Civ. Code § 1798.105.

- 11 Cal. Civ. Code § 1798.145, subd. (e).
- 12 16 C.F.R. § 313.3(a).
- 13 Cal. Fin. Code § 4052.5.
- 14 Gramm-Leach-Bliley Act of 1999, Pub. Law 106-102, 113 Stat. 1338, §509(9) (1999); Cal. Fin. Code § 4052, subd. (f).
- 15 The Federal Trade Commission's own guidance states that "[u]nder the Rule [GLBA], a 'consumer' is someone who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that person's legal representative. The term 'consumer' does not apply to commercial clients, like sole proprietorships. Therefore, where your client is not an individual, or is an individual seeking your product or service for a business purpose, the Privacy Rule does not apply to you." *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act: A Guide for Small Business from the Federal Trade Commission* (July 2002), available at <https://www.ftc.gov/system/files/documents/plain-language/bus67-how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act.pdf>.
- 16 Assem. Bill No. 25 (2019-2020)
- 17 *California Promises Aggressive Enforcement of New Privacy Law*, S.F. Chronicle (Dec. 16, 2019), available at <https://www.sfchronicle.com/politics/article/California-promises-aggressive-enforcement-of-new-14911017.php?t=f1df9802a8>.

Chapman and Cutler LLP

Attorneys at Law · Focused on Finance®

This document has been prepared by Chapman and Cutler LLP attorneys for informational purposes only. It is general in nature and based on authorities that are subject to change. It is not intended as legal advice. Accordingly, readers should consult with, and seek the advice of, their own counsel with respect to any individual situation that involves the material contained in this document, the application of such material to their specific circumstances, or any questions relating to their own affairs that may be raised by such material.

To the extent that any part of this summary is interpreted to provide tax advice, (i) no taxpayer may rely upon this summary for the purposes of avoiding penalties, (ii) this summary may be interpreted for tax purposes as being prepared in connection with the promotion of the transactions described, and (iii) taxpayers should consult independent tax advisors.

© 2020 Chapman and Cutler LLP. All rights reserved. Attorney Advertising Material.