National Financial Institutions—Developing A Project Plan To Comply With The California Consumer Privacy Act

by Joseph Lynyak and Erin Bryan

Since its adoption last year, U.S. financial institutions have been confronted with the challenge of planning their compliance with the California Consumer Privacy Act (the "CCPA")[1]. The CCPA becomes effective in two stages—January 1, 2020 and July 1, 2020 (or possibly sooner depending upon the date the California Attorney General adopts implementing regulations).[2]

Regrettably, considerable confusion exists within the financial industry about the scope of the CCPA and the obligations it imposes on financial institutions.

In an effort to provide our financial intermediary clients and friends with a workable summary of a financial institution's obligations—and in particular for financial institutions that do not have a physical presence in California—this Alert is intended to assist in identifying coverage considerations, and provide a practical approach to the development of a project plan that will demonstrate reasonable compliance with the CCPA's admittedly ambiguous set of requirements and obligations.

What obligations does the CCPA impose on a covered business?

The CCPA requires that a covered business respond to newly enacted privacy rights for a California resident, which includes the rights to:

- Know what categories of "personal information" or "PI" is being collected;
- Know whether personal information is sold or disclosed and to whom;
- Say "no" to the sale or disclosure of personal information, and to require a covered business to delete PI; and
- Receive equal service and price, whether or not privacy rights under the CCPA are exercised.

The CCPA creates a complicated set of procedural and substantive requirements on the part of a covered company. For example, a covered business must be capable of responding to a "verified consumer request" for personal information, provide a summary

Related People

- Joseph Lynyak
- Erin Bryan

Related Capabilities

- California Consumer Privacy Act (CCPA)
- Banking & Financial Institutions

of categories of PI that are collected about a California resident, state whether PI is sold or transferred to third parties, and delete information at the direction of the California resident (similar to the right to be forgotten under the EU's General Data Protection Regulation).[3]

Is a financial institution a covered business under the CCPA?

Two distinct questions should be asked to determine whether a financial institution could be subject to the requirements of the CCPA: (1) does the financial institution qualify as a "business" covered by the CCPA; and (2) to what extent may a covered financial institution take advantage of one or more of the exemptions, including the exemption for its treatment of PI pursuant to Title V of the federal Gramm-Leach-Bliley Act ("GLBA") or the California Financial Information Privacy Act ("CFIPA") (which we refer to collectively as the "GLBA Exemption")[4].

The CCPA broadly defines the term "business" to include various entities, including a corporation, partnership, limited liability company or similar entity, "that is organized or operated for the profit or financial benefit of its shareholders or other owners." However, a covered business also must "[do] business in the State of California" and meet one or more of the following thresholds: (A) have an annual revenue (currently interpreted to be global revenue) of $25,000,000; (B) engage in commercial activities involving the collection, sale, or disclosure of "the personal information of 50,000 or more consumers, households, or devices;" or (C) "[d]erive 50 percent or more of its annual revenues from selling consumers' personal information." Even though the conditions and thresholds appear to target larger or data-rich companies, the definition of a "business" will subject most national financial institutions to the facially broad coverage of the CCPA.[5]

Second, the GLBA Exemption may afford a financial institution partial relief from certain requirements of the CCPA. Commercial banks, savings banks, mortgage companies, loan servicers, data aggregators, and others generally qualify as a type of "financial institution" that is engaged in collecting, processing, selling, or disclosing PI "pursuant to" the GLBA (and the CFPB's implementing Regulation P[6]) or the CFIPA. The scope of the partial GLBA Exemption is important for purposes of developing an effective compliance plan, and will be discussed in greater detail below.

To what extent might the GLBA Exemption reduce a financial institution's compliance obligations under the CCPA?

Unfortunately for the financial industry, the GLBA Exemption leaves financial institutions exposed to a number of compliance risks under the CCPA. After the CCPA was enacted, the GLBA Exemption was hurriedly added at the very end of the 2018 California legislative session. The GLBA Exemption states:

This title shall not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act (Public Law 106-102), and implementing regulations, or the California Financial Information Privacy Act (Division 1.4 (commencing with Section 4050) of the Financial Code). This subdivision shall not apply to Section

1798.150.[7]

By its terms, the CCPA's GLBA Exemption only exempted PI—meaning the data itself—from coverage under the CCPA, but not the financial institution holding the data. Further, notwithstanding the exemption, liability for data breaches of a limited range of a California resident's data remains subject to the CCPA's private right to recover statutory damages.[8]

How do the CCPA, the GLBA and the CFIPA fit together?

This interplay among and between the CCPA, the CFIPA and the GLBA has created an interpretative quagmire for covered financial institutions attempting to determine the scope of their compliance responsibilities. On one hand, some industry stakeholders have argued that the GLBA Exemption excludes PI from virtually all requirements under the CCPA, while others have advocated that the exemption is very limited in scope, and specifically does not exclude financial institutions from obligations established by the CCPA that are not similar to those in the GLBA and the CFIPA.

The compliance risk for financial institutions

As a starting point in the analysis, we look at the interplay between the CFIPA and the GLBA. When initially adopted by the California Legislature in 2003 (and effective in 2004), it was clear that the CFIPA was an attempt to create substantially equal privacy rights under California law as were created by the GLBA. However, the CFIPA was more extensive than the GLBA in that, rather than providing a California consumer with the right to "opt-out" from covered data being sold or transferred to a non-affiliated party (which was the approach adopted by the GLBA), the CFIPA required that covered financial institutions obtain an affirmative opt-in consent from a California consumer prior to sharing or transferring data to third parties. Importantly, because Section 524 of the GLBA contains a "reverse preemption" provision that provides that state law privacy rights trump privacy rights as contained in the GLBA, for years covered financial institutions have provided the more extensive California-based privacy rights contained in the CFIPA rather than the more limited privacy rights as contained in the GLBA.[9]

It is important to understand that both the GLBA and the CFIPA are primarily disclosure statutes, and impose no substantive obligations on a covered financial institution beyond the opt-out and opt-in rights exercised by a California consumer, discussed above. Neither statute limits the amount or content of information that may be collected by a covered financial institution, including responding to consumer requests for information following the delivery of required disclosures.[10]

Given the limited nature of the GLBA Exemption—and its interplay with the CFIPA—the disclosure scheme as contemplated by those statutes (including Regulation P) arguably may control initial disclosures required to be delivered (as specified by the CFIPA and the GLBA), but may not exempt a financial institution from responding to a "verified consumer request" for PI whether or not the data was originally disclosed in accordance with the GLBA (as modified by the opt-in requirements of the CFIPA).

Planning for compliance

A careful reading of the CCPA's GLBA Exemption indicates that, subsequent to the delivery of initial account disclosures, the GLBA Exemption may be of limited value in real-world communications between a covered financial institution and California residents exercising their privacy rights pursuant to Sections 1798.100 through 1798.125 of the CCPA. Importantly, both the GLBA and the CFIPA contain data definitions that are narrower than the expansive definitions of PI contained in the CCPA. Also, the GLBA and the CFIPA are generally limited to consumers opening accounts with a covered financial institution, whereas the exercise of a consumer's privacy rights under the CCPA is not limited by the establishment of an account relationship. Further, the CCPA's definition of a "consumer" extends to a California resident, whereas the GLBA's and the CFIPA's disclosure requirements are limited to the traditional concept of data obtained as part of a "consumer purpose" relationship (*i.e.*, for personal, household or family purposes).

Unless the California Attorney General elects to clarify the coverage question created by the GLBA Exemption discussed above, covered financial companies may have no choice but to comply with all requirements of a covered business under the CCPA (with the possible exception of continuing to employ GLBA- and CFIPA-compliant disclosures). Failing to adopt a narrow view of the scope of the CCPA's GLBA Exemption may jeopardize the structuring of an effective compliance program by the deadlines established by the CCPA in 2020.

What must be included in a project plan to comply with the CCPA?

In order to comply with the extremely short time frames required by the CCPA, we suggest that several components should be considered, as follows:

Essential plan elements

There are two essential elements that should be included in any CCPA project plan. The first is data mapping to identify systems of records that contain PI covered by the CCPA. Anecdotal reports from national financial institutions—particularly those who did not engage in data mapping in order to comply with the GDPR—indicate significant operational difficulties being experienced to both identify data systems and develop methodologies to capture and to retrieve covered data to respond to a verified consumer request. Stated another way, data mapping should begin as soon as possible.

The second element is perhaps the most important risk mitigation step that a covered financial institution can take to avoid liability. The CCPA allows for the recovery of statutory damages for specified data breaches by private parties (including class action liability for breaches involving multiple California residents). Statutory damages range from $100 per incident to $750 per individual breach.[11] According to the statutory liability provision of the CCPA, the only defense to statutory damages is a showing that a covered company had in place reasonable data security measures for the PI it held in its systems.[12] Liability for statutory damages for specified data breaches commences as of

January 1, 2020, regardless of whether the California Attorney General issues implementing regulations after that date.[13]

Accordingly, as an essential element of a project plan, a covered financial institution should be prepared to demonstrate that its data security measures are reasonable, based upon industry standards, and have been regularly confirmed by internal and external audits.

General project plan elements

In addition to the two essential components of a financial institution's project plan, discussed above, the following implementation tasks may likely be required to be included in a CCPA project plan, and include:

- Identifying data constituting PI
- Determining the applicability of full or partial exemptions from data use and retention
- Determining the scope of the GLBA Exemption for data, discussed above
- Determining the methodologies for receiving and responding to a verifiable consumer request
- Designing and building internal call centers/response teams
- Amending disclosures of privacy policies
- Modifying website(s)
- Adopting methodologies to implement "opt-out" and "opt-in" elections and deletion of PI
- Reviewing and modifying agreements with third parties and vendors
- Drafting internal policies and procedures
- Establishing training programs

A recommended implementation approach—evolving compliance

We note that several commentators and vendors have advocated engaging in an implementation program that is extraordinarily complex and (in our view) not capable of being completed within the CCPA's time limitations. Importantly, the patent ambiguities in regard to a covered financial institution's compliance obligations require that a financial institution establish its own compliance goals and response measures while interpretative guidance is being developed and eventually becomes available.

As a practical matter, lending and account relationships may form the basis for most data requests made by a California resident to a covered financial institution, which may constitute an initial starting point for responding to CCPA inquiries. Similarly, a financial institution may have to determine the degree of information included in a response, and may have to implement an evolving degree of data inquiries as the Attorney General refines the question of reasonable compliance.[14]

In sum, until the matter is clarified, financial institutions should be wary of overreliance on a broad reading of the partial GLBA Exemption. To do so may result in the development of an implementation plan that is deficient in regard to reasonable scope and content.

Please note that the analysis set forth in this Alert is not intended to be a comprehensive discussion of the obligations that are contained in the CCPA; California-licensed lawyers at Dorsey have been closely following CCPA legislative and regulatory developments, and are available to discuss the same.

[1] Cal. Civ. Code § 1798.100 et. seq.
[2] Cal. Civ. Code § 1798.185.
[3] Cal. Civ. Code § 1798.105 to 1798.125.
[4] 15 U.S.C. § 6801 et seq.; Cal. Fin. Code § 4050 et seq.
[5] Cal. Civ. Code § 1798.140(c). It should be noted that California takes an expansive view of what constitutes "doing business" for purposes of the CCPA and other statutes intended to protect its citizens. Specifically, dealing with a California resident using the internet and commercial webpages will likely constitute doing business for purposes of the CCPA.
[6] 12 C.F.R. § 1016.1 et seq.
[7] Cal. Civ. Code § 1798.145(e).
[8] Id.
[9] 15 U.S.C. § 6807.
[10] See generally, 289 Cal. Fin. Code §§ 4050, et seq.; 6 CFR § 313.1 et seq. (15 U.S.C. § 6801 et seq.).
[11] Cal. Civ. Code § 1798.150(a)(1)(A). Although the categories of PI that are covered by the CCPA's statutory damages provisions is narrower than the entire definition of PI, it includes personal identifiers that are commonly part of a data breach.
[12] Cal. Civ. Code § 1798. 150(a)(1)(C)(2).
[13] Cal. Civ. Code § 1798.198(a).
[14] One of the significant compliance challenges presented is the degree of specificity of PI that must be provided to a California resident when responding to a verifiable consumer request. See, Cal. Civ. Code § 1798.110(c)(5).