Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Calif. Consumer Privacy Act: 6 Considerations For Banks

By **Nathan Taylor and Purvi Patel** (May 30, 2018, 12:03 PM EDT)

Nathan Taylor

Purvi Patel

Financial institutions in the United States are no strangers to privacy regulations, particularly given the obligations imposed by the federal Gramm-Leach-Bliley Act and the California Financial Information Privacy Act (SB1). More recently, financial institutions have been focused on whether and/or the extent to which the EU's General Data Protection Regulation may apply to their U.S. operations. Many financial institutions, however, have yet to consider an equally important U.S. privacy development — the California Consumer Privacy Act, a ballot initiative likely to appear on the November ballot.[1]

If approved by voters, the act would impose notice obligations on covered businesses to disclose the categories of personal information they collect, sell and share about California consumers, and give those consumers a right to say "no" to the "sale" of their information.[2] We discussed the act and its potential requirements and related risks, including litigation arising from alleged violations of the act, in greater detail in a previous Law360 article.

Here, we highlight certain considerations that are unique to financial institutions and evaluate the potential impact of the act on financial institutions, particularly given their existing privacy obligations under the GLBA and SB1. Below are six key considerations for financial institutions to keep in mind as they navigate the interplay between the act, the GLBA and SB1.

1. No GLBA or SB1 Exception

Although the California Consumer Privacy Act includes a Fair Credit Reporting Act exception for consumer report information, the act does not include an exception for financial institutions or for compliance with the GLBA or SB1.[3] That is, the act fails to recognize that financial institutions doing business in California are already subject to both a comprehensive federal financial privacy regime (the GLBA) and the most significant state financial privacy regime (SB1). Nor does the act otherwise acknowledge the existing notice obligations and disclosure limitations to which financial institutions are already subject. As a result, financial institutions doing business in California that meet one or more of the act's applicability criteria (e.g., annual gross revenue beyond $50 million) would be subject to the act's requirements.[4]

2. Difference in Scope Between the Act and the GLBA and SB1

While there are many distinctions between the GLBA, SB1 and the California Consumer Privacy Act, the most basic (but nonetheless critical) distinction is the types of individuals they respectively protect. The GLBA and SB1 both apply to information about individuals who obtain financial products and services for personal, family or household purposes.[5]

The act, however, would apply more broadly to information about individuals who are California residents.[6] It is similar to California's data security and breach notification laws in this regard,[7]applying to information about Californians generally, regardless of their relationship to a business. As a result, a covered financial institution would be subject to the act's various privacy obligations with respect to not only its customers who are California residents, but also any other California resident regarding whom the financial institution collects PI, including, for example, an employee or vendor who is a California resident.

3. The Relevance to Existing GLBA Notice Requirements

There are two types of "notice" requirements under the act. First, a covered business would be required to include various act-related disclosures in, among other things, "any California-specific description of consumers' privacy rights."[8] For instance, a business would be required to update — at least annually — the list of the categories of PI it has collected, sold to a third party, or disclosed for business purposes.[9] If a financial institution includes a disclosure in its GLBA privacy notice that is specifically for California residents (e.g., a "for California residents" statement in the "other important information" section of its GLBA notice),[10] the financial institution would have to consider whether that disclosure would be considered a "California-specific description of consumers' privacy rights" and, if so, whether the financial institution is required to address the act's disclosure requirements in its GLBA privacy notice (in addition to any notice that it may prepare specifically to address the act).

The act, however, goes beyond traditional concepts of macro-level, privacy-related disclosures that focus on listing generally applicable examples or categories of information or activities. For example, upon a consumer's request, a covered business would be required to identify by category the PI that the business has sold to a third party and has disclosed for business purposes in the preceding 12 months, as well as "provide accurate names and contact information" for the recipients of that information.[11]

The consumer "right to know," particularly as it pertains to PI disclosed for a business purpose, is far reaching, and implicates the everyday transactions that a financial institution undertakes for its customers. A transaction, by definition, involves multiple parties, and banks must disclose customer PI in order to provide the very financial products and services requested by a customer. To illustrate, when a bank's customer uses her credit card online to pay for a purchase, the bank will receive the authorization request through the relevant payment card network. Regardless of whether the bank authorizes or declines the request, the bank must communicate its authorization decision to the relevant payment card network so that information can then be communicated back to the merchant. As a result, the act's "right to know" provisions could require a financial institution to engage in a burdensome administrative and record-keeping process to track every recipient (and its contact information) to whom it has disclosed data relating to a California resident pertaining to routine business purposes.

4. Difference in Scope of Opt-Out Rights

The GLBA and SB1 provide a consumer with some control over the extent to which a financial institution can disclose information about the consumer to a nonaffiliated third party. Specifically, the GLBA gives consumers the right to opt out of a financial institution's disclosure to nonaffiliated third parties, while SB1 only permits a financial institution to share information with nonaffiliated third parties if a customer opts in to such sharing.[12]

But, a consumer's rights under the GLBA and SB1 are not "absolute." More specifically, both the GLBA and SB1 include sensible exceptions to their respective opt-out and opt-in requirements to facilitate the types of non-controversial disclosures that a financial institution must make to run its business and provide the very financial products and services requested by consumers.[13] In particular, both the GLBA and SB1 include exceptions that permit a financial institution to disclose information for activities like fraud prevention, maintaining and servicing accounts, and processing transactions.[14] To the extent a GLBA or SB1 exception applies, a financial institution may disclose information about a consumer, regardless of whether the customer has exercised a GLBA opt-out or has not opted in under SB1.

In contrast, the California Consumer Privacy Act's broad scope and limited exceptions would functionally create a far more "absolute" consumer right to opt out of the "sale" of information than exists under either the GLBA or SB1, separately or together. The act does not include any practical exceptions with respect to its opt-out right for the "sale" of information similar to those found in the GLBA and SB1. This is critical because of the act's extremely broad definition of the term "sale," which includes "sharing ... a consumer's [PI] with a third party, whether for valuable consideration or for no consideration, for the third party's commercial purposes."[15]

This aspect of the definition of "sale" is focused on disclosures that are for the recipient's "commercial purposes," presumably as distinct from the business purposes of the entity disclosing the information. A financial institution would have to evaluate the extent to which it shares information with third parties for the third party's commercial purposes, notwithstanding the fact that the financial institution may receive no compensation (and may not even consider the disclosure to be a "sale," as that term is commonly understood). For example, if a consumer applies for a mortgage with Bank A, and Bank A contacts Bank B (with which the consumer has a checking account) to confirm that the consumer has sufficient funds to cover her down payment in the mortgage transaction, would Bank B's disclosure to Bank A be considered a disclosure for Bank A's "commercial purposes," a disclosure for Bank B's "business purposes," or both?

The combination of the act's expansive definition of "sale" and lack of the types of exceptions found in the GLBA and SB1 would create an important inconsistency among the three privacy regimes. The challenge here will be reconciling disclosures that are otherwise permitted under the GLBA and SB1 and those that a consumer will be able to opt out of under the act.

5. Affiliate Sharing Implications and Potential Preemption Challenges

On its face, the California Consumer Privacy Act does not appear to differentiate between sharing consumer PI with an affiliate — whether through a sale or a disclosure for a business purpose — and sharing with a non-affiliate.[16] If the act's broad definitions of "sale" and "third party"[17] limit the ability of a financial institution to disclose information to an affiliate, the act may conflict with the FCRA and be vulnerable to preemption challenges.

There is precedent in this regard. After the passage of SB1, the American Bankers Association, The Financial Services Roundtable, and Consumer Bankers Association sued the California attorney general and others asserting that the FCRA's affiliate-sharing preemption provision preempted the affiliate-sharing provision of SB1.[18] The trade associations prevailed on that claim to the extent that SB1 sought to limit the sharing of information permitted under the FCRA. A similar challenge could be raised against the act to the extent it attempts to limit the sharing of information with an affiliate that the FCRA permits.

6. Indirect Implications for Fraud Prevention and Other Purposes

The California Consumer Privacy Act's right to "say no" to the sale of consumer PI could present operational challenges for a financial institution,[19] regardless of whether the financial institution is subject to the act. Financial institutions often rely on non-FCRA, third-party data products to evaluate applications, process transactions, and otherwise engage in "core" financial service activities. A financial institution may purchase non-FCRA data in various contexts, such as:

- A bank may obtain a fraud report in evaluating an application for credit;

- A bank may obtain information relating to whether a computer device attempting to log in to online banking has previously been associated with fraud; or

- A bank may obtain an Office of Foreign Assets Control report in the context of evaluating an application to open a deposit account or a wire transfer request on an existing account to ensure that the underlying transaction would not be prohibited by anti-money laundering and anti-terrorist financing provisions under federal law.

If the financial institution seeks the above information for a California resident who has opted out of the sale of her information by the data provider from which the financial institution requests the information, the financial institution would not be able to obtain the information (assuming, of course, that the information is not a consumer report subject to the FCRA).

Even more troubling, because the act does not have a fraud prevention exception to its opt-out right, fraudsters and other criminals residing in California would be able to functionally "clean" non-FCRA fraud databases by exercising their opt-out rights, thereby impairing the value of critical information on which financial institutions rely to prevent fraud and money laundering and to comply with the law.

Conclusion

Financial institutions should pay close attention to the act and this year's ballot initiative process. If the initiative is successful, financial institutions will need to consider the extent to which existing GLBA and SB1 procedures will need to be modified to address the act. Moreover, financial institutions will need to put in place new privacy processes to provide California consumers with accurate disclosures regarding the sale and disclosure of PI.

Nathan D. Taylor and Purvi G. Patel are partners at Morrison & Foerster LLP.

[1] On May 3, 2018, proponents of the California Consumer Privacy Act announced they had collected the number of signatures needed to qualify the Act for the November ballot. https://ballotpedia.org/California_Consumer_Personal_Information_Disclosure_and_Sale_Initiative_(2018). Before the Act can be included on the ballot, however, county election officials must verify the signatures, and the Secretary of State must certify the measure qualifies for the ballot.

[2] See §§ 1798.100–1798.102. Unless otherwise specified, all citations are to Section 4 of the initiative measure, and track proposed changes to the California Civil Code.

[3] See § 1798.107(d). The Act also expressly exempts "protected health information" governed by the Health Insurance Portability and Accountability Act. § 1798.107(c).

[4] See § 1798.106(b).

[5] See 12 C.F.R. § 1016.3(e)(1) (defining a "consumer," in pertinent part, as "an individual who obtains or has obtained a financial product or service ... that is to be used primarily for personal, family, or household purposes"); Cal. Fin. Code § 4052(f) (SB1) (defining a "consumer," in pertinent part, as "an individual resident of this state ... who obtains or has obtained from a financial institution a financial product or service to be used primarily for personal, family, or household purposes").

[6] § 1798.106(g) (defining "consumer" as a "natural person who is a California resident").

[7] See Cal. Civ. Code §§ 1798.81.5(a)(1) (noting the intent of the California legislature to require that "personal information about California residents is protected"), 1798.82(a) (requiring notice to "a resident of California" for certain security incidents involving personal information relating to the individual).

[8] § 1798.104(a)(5).

[9] Id.

[10] See 12 C.F.R. pt. 1016, App.

[11] § 1798.104(a)(4).

[12] See 12 C.F.R. § 1016.10 (GLBA); Cal. Fin. Code § 4052.5 (SB1).

[13] See 12 C.F.R. §§ 1016.13–1016.15 (GLBA); Cal. Fin. Code § 4056 (SB1).

[14] See, e.g., 12 C.F.R. §§ 1016.14(a), 1016.15(a)(2)(ii).

[15] § 1798.106(q).

[16] §§ 1798.101(a), 1798.104(a)(4), 1798.106(l), (s).

[17] § 1798.106(q), (s).

[18] Am. Bankers Ass'n v. Lockyer, 541 F.3d 1214 (9th Cir. 2008).

[19] § 1798.102.