The CCPA Is Here: What Financial Institutions Need To Know About the California Consumer Privacy Act

By David J. Oberly and Tanweer Ansari

As of January 1, 2020, the California Consumer Privacy Act of 2018 (CCPA) is now the law of the land, having gone into effect at the beginning of this year. One of the more complex issues concerning the CCPA pertains to the extent to which financial institutions governed by the Gramm-Leach-Bliley Act (GLBA) must adhere to the mandates of the CCPA. While California's new privacy law does afford a carve-out for financial institutions, it does not provide a comprehensive, across-the-board "get out of jail free" card for the financial services industry. Consequently, at this juncture it is imperative that all covered financial institutions ensure that they are in compliance with the CCPA to minimize the potential liability risk that now exists for noncompliance with the law. Fortunately, through the implementation of several best practices, financial institutions can continue to effectively leverage data in the course of their business operations, while at the same time steering clear of the potential pitfalls that could result in substantial liability exposure resulting from a failure to adhere to the CCPA's broad mandates.

The CCPA's GLBA Carve-Out

The CCPA was amended in September 2018, and now provides the following carve-out for financial institutions: "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 . . . . This subdivision does not apply to Section 1798.150." Pursuant to this language, the financial institution carve-out applies to personal information that is collected "pursuant to" the GBLA or the California Financial Information Privacy Act ("CFIPA"). Thus, financial entities will be subject to the requirements of the CCPA where they engage in activities that fall outside the scope of the GLBA.

Specifically, the GLBA applies to financial institutions' collection and use of "nonpublic personal information," which is defined as personally identifiable financial information provided by a consumer to a financial institution that results from a consumer transaction or that is otherwise obtained by the financial institution. While this definition seems expansive at first glance, the Federal Trade Commission (FTC) has issued guidance specifying that the term applies only to information that is collected about an individual in connection with providing a financial product or service. Conversely, the CCPA provides for a much broader definition of "personal information" that extends to include all 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 device."

As such, while financial institutions are generally exempted from complying with the CCPA in connection with personal information collected through core consumer financial activities, the carve-out does not provide a blanket exemption, and there will be certain scenarios where banks will be required to comply with California's new privacy law. Specifically, if a financial institution collects personal information outside the context of providing a financial service or product, the institution will be subject to the mandates of the CCPA.

In addition, the financial institution carve-out also expressly provides that the exemption does not apply to CCPA § 1798.150. That provision sets forth a private right of action for consumers to pursue individual or class litigation, with significant allowable statutory damages, where the consumer's personal information has been impacted by a data breach and the institution is found to have violated its duty to implement "reasonable" data security measures. As such, GLBA-regulated entities are now subject to being on the receiving end of consumer-initiated CCPA lawsuits in the event the institution suffers a data breach.

Compliance Strategies for Financial Institutions

Importantly, as the CCPA does not provide a comprehensive exemption for the financial services industry, financial institutions must ensure that they have satisfied their current compliance obligations placed on them under California's new, sweeping privacy law. So what must covered financial institutions do in order to ensure they are compliant with the CCPA?

In terms of actionable compliance steps themselves, the first order of business to get in compliance with the CCPA is to conduct a data mapping and inventory exer-

David J. Oberly is an associate at Blank Rome LLP and is a member of the firm's cybersecurity and data privacy group. David focuses his practice on counseling and representing sophisticated clients in a wide assortment of complex cybersecurity and data privacy matters. Tanweer Ansari is Senior Vice President and Chief Compliance Officer of First National Bank of Long Island, and a past Chair of the NYSBA Banking Law Committee. He serves on various boards and is involved in relevant legal and compliance circles.

cise to determine what personal information is not exempted by the GLBA carve-out and, in turn, is "in scope" for purposes of the CCPA. In addition, from a broader perspective, data mapping is also a prudent course of action for financial institutions to take in order to prepare for the additional regulatory changes that are sure to come in the immediate future.

To accomplish this task, institutions must map and inventory every piece of personal information that is collected, used, and sold by the institution, as well as all of the institution's data processing practices. In doing so, institutions will need to analyze all aspects of their organization, and all points where the institution collects, utilizes, or transmits information for any purpose and in any format. From there, institutions should determine—dataset by dataset—whether the entity's personal information is covered by the GLBA or the CFIPA, which would remove it from the scope of the CCPA. When performing this task, financial institutions should keep in mind that application of the CCPA will depend on the context in which personal information is collected, used, and shared and, as such, some of the same data elements—including names, IP addresses, and email addresses—may be excluded from the scope of the CCPA in some scenarios, but not in others.

Second, financial institutions must maintain systems and procedures to ensure adherence to the myriad of broad consumer rights that have been afforded to consumers under California's new privacy law, including the following: (1) right to know; (2) right to access; (3) right to opt-out; (4) right to deletion; and (5) right to equal service and pricing. In particular, institutions must maintain the operational capabilities to provide information to consumers upon request in the event a consumer seeks information regarding the data that is collected and sold by the institution, including the specific pieces of information that the institution has collected concerning the requesting consumer.

Third, institutions must also provide the mandated privacy disclosures and notices that are required by the CCPA. Here, institutions must include in their privacy policies the information that is required to be affirmatively disclosed to consumers pertaining to the institution's data practices and consumers' rights under the CCPA, including a toll-free number and a website for consumers to submit requests, as well as a link on the institution's web page entitled "Do Not Sell My Personal Information" to facilitate the opt-out process.

Fourth, as the financial institution carve-out does not apply to the CCPA's "reasonable" security requirement and private right of action provision, financial institutions also must have in place the necessary data security measures and controls that are required to comply with the CCPA. While the CCPA does not impose any express, direct data security requirements on financial institutions, the CCPA does require that institutions put in place "reasonable security procedures and practices" to protect personal information from being improperly accessed, disclosed, or acquired.

Financial institutions must ensure that they are in strict compliance with this obligation, as consumers are entitled to pursue litigation under the CCPA's private right of action provision if their data is impacted by a data breach event and the institution is found to have violated its duty to implement reasonable security measures. Consumers can pursue individual or class lawsuits if their data is compromised by a data breach, and can recover between $100 and $750 in statutory damages per incident. Although this damages figure may seem small, institutions must keep in mind that a class of just 10,000 consumers under the CCPA would subject an institution to $7.5 million in potential exposure.

"Consumers can pursue individual or class lawsuits if their data is compromised by a data breach, and can recover between $100 and $750 in statutory damages per incident. Although this damages figure may seem small, institutions must keep in mind that a class of just 10,000 consumers under the CCPA would subject an institution to $7.5 million in potential exposure. "

To further complicate matters, although financial institutions are subject to liability under the CCPA for data breaches arising out of violations of the duty to implement reasonable security measures, the CCPA does not provide any description of this duty nor offer any insight as to what satisfies the threshold for maintaining "reasonable" security measures.

In the absence of any formal CCPA guidance, financial institutions can consider implementing the data security measures previously endorsed by the California attorney general in its 2016 Data Breach Report. In the Report, the California AG endorsed the Center for Internet Security's Critical Security Controls ("CIS Controls"), a set of 20 different data security safeguards that were viewed by the then-AG as constituting reasonable security measures. As such, these CIS Controls can be used as a guide for complying with the reasonable security requirement of California's new privacy law.

In addition, financial institutions should also consider supplementing the CIS Controls by incorporating other well-accepted information security frameworks into their security programs—such as the International Standard Organization's (ISO) 27001 Series and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework—which can aid in further demonstrating an institution's satisfaction of the "reasonable" security requirement so as to avoid class action litigation under the CCPA's private right of action provision.

Finally, financial institutions should also ensure that their cyber coverage policies extend to cover the full range of CCPA-related liabilities. While privacy liability is ordinarily a staple in most cyber insurance policies, this coverage is oftentimes triggered only in the event of a data breach. Importantly, however, under the CCPA a wide range of privacy violations can still take place outside of the data breach context. As such, many financial institutions may find that their current cyber coverage does not adequately shield them against the CCPA's broad statutory liabilities. To avoid any gaps in coverage, financial institutions must ensure that their policies provide coverage for acts or omissions stemming from the collection, use, disclosure, and storage of "personal information," as that term is used in the CCPA. In addition, cyber policies should also afford coverage for legal fees associated with regulatory investigations, regulatory fines, data breach response costs, and liabilities stemming from class action litigation.

Conclusion

While the CCPA affords some level of relief to financial institutions from the onerous obligations placed on covered businesses under California's new privacy law, the CCPA does not provide financial institutions with a complete exemption from the law. Rather, entities governed by the GLBA are subject to the mandates of the CCPA if they collect, use, sell, or share the personal information of California consumers outside of the context of providing a consumer financial service or product.

As such, because the CCPA went into effect at the start of the year, financial institutions that fall under the scope of the CCPA should be in full compliance with the law at this time. For those institutions that have yet to finalize their CCPA compliance efforts, now is the time to take action to bring themselves in line with the CCPA's requirements, especially with the California attorney general having begun its enforcement efforts on July 1, 2020. At the same time, financial institutions should also remain on the lookout for the finalized version of the CCPA Regulations, which may impose additional compliance burdens that would require covered institutions to further tweak their privacy compliance programs to align themselves with any new wrinkles in the CCPA that may come about when the final Regulations are issued.

Reprinted with permission from: *NY Business Law Journal*, Summer 2020, Vol. 24, No. 1, published by the New York State Bar Association, One Elk Street, Albany, NY 12207.