CeFPro™ MAGAZINE

Issue 14, January- March, 2020

FINANCE, RISK, TECHNOLOGY AND REGULATION

Real world perspective - Written by the industry, for the industry

CCPA GUIDE: WHAT FINANCIAL INSTITUTIONS NEED TO KNOW ABOUT THE CALIFORNIA CONSUMER PRIVACY ACT

David J. Oberly, *Associate,* Blank Rome LLP / *member,* Cybersecurity & Data Privacy Group

Tanweer Ansari, *SVP Chief Compliance/BSA/CRA Officer,* The First National Bank of Long Island

At the time of writing, business entities across all industries are hard at work gearing up to get in compliance with the California Consumer Privacy Act of 2018 (CCPA) by the law's January 1, 2020 effective date. 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, financial institutions will need to take actionable steps to prepare for compliance with the CCPA by the time the new privacy law goes into effect at the beginning of this year.

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 GLBA 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 FTC has issued guidance that specifies 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." This definition of personal information under the CCPA is much more expansive as compared to the GLBA's definition of the term, as the CCPA's definition is not limited to data collected in connection with financial products or services, and encompasses information such as IP addresses, email addresses, browsing and search history, and information concerning a consumer's interaction with a website.

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 will still be 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 take active steps to get themselves in compliance with the CCPA before the law goes into effect at the beginning of this year. So what must covered financial institutions do in order to achieve compliance 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 exercise 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.

After determining the universe of personal information that is subject to the CCPA, the next step to take to get in compliance with the CCPA is to develop systems and procedures to ensure adherence with the myriad of broad consumer rights that have been afforded to consumers under California's new privacy law. Specifically, financial institutions will have to comply with the following rights:

Right to Know: Consumers must be able to learn—through a general privacy policy and with more details upon request—what personal information an institution has collected about them, where the information originated, the use of the information, and whether and to whom the information is being disclosed or sold.

Right to Access: Consumers can request that financial institutions provide them with a copy of all personal information collected by the institution on the consumer, which the institution must then provide to the consumer free of charge.

Right to Opt-Out: Financial institutions must allow consumers to "opt-out" and stop an institution from selling their personal information to third parties, with the term "sale" defined very broadly to include any sharing of personal information in exchange for something of value.

Right to Deletion: Consumers maintain the right to request that financial institutions delete their personal information and data, subject to several exceptions.

Right to Equal Service & Pricing: Consumers maintain the right to receive equal service and pricing from financial institutions, even if the consumer chooses to exercise his or her privacy rights under the CCPA.

In addition, institutions will also need to provide the mandated privacy disclosures and notices that are required by the CCPA. Here, institutions will need to update their privacy policies with 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 titled "Do Not Sell My Personal Information" to facilitate the opt-out process. Moreover, institutions must also develop 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.

Furthermore, as the financial institution carve-out does not apply to the CCPA's "reasonable" security requirement and private right of action provision, financial institutions will need to ensure that they implement the necessary data security measures 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. Significantly, financial institutions must ensure that they comply 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.

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 on the issue, an effective approach for institutions to take in order to satisfy the CCPA's "reasonable" security requirement is to implement the data security measures previously endorsed by the former 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), which consists of 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 satisfying 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, in addition to making the necessary changes to bring themselves in compliance with California's new privacy law, financial institutions should also examine their cyber insurance coverage to ensure that their 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.

"In addition to making the necessary changes to bring themselves in compliance with California's new privacy law, financial institutions should also examine their cyber insurance coverage to ensure that their policies extend to cover the full range of CCPA-related liabilities."

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 will be 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. Importantly, making the necessary changes to get in compliance with the CCPA will take time and, as such, financial institutions should start evaluating exposure and mapping out compliance steps as soon as possible in the event an institution has not already commenced its CCPA compliance efforts. Ultimately, in order to ensure compliance with the new law, many institutions will face substantial compliance burdens in order to map and inventory all personal information possessed by the institution; establish and update policies, procedures, and practices; put in place "reasonable" security measures; and implement other changes to come into compliance with the CCPA. As such, although the CCPA is not set to go into effect until 2020, now is the time to begin making preparations for compliance with California's new privacy law.

At this time, there are many amendments to the CCPA that are still working their way through the California legislature. In addition, California's attorney general will also publish regulations pertaining to a range of issues covered by the law sometime in the coming months as well. Financial institutions should monitor the status of these amendments and regulations to ascertain whether any additional requirements will ultimately be imposed on covered entities by the final version of the law and its implementing regulations.

The CCPA represents by far the most onerous, stringent data privacy law of its kind on the books today. With that said, while the CCPA has dominated the headlines recently, other states have taken a page out of California's book and have enacted—or have otherwise considered or drafted—new consumer privacy legislation of their own. Moving forward, financial institutions should anticipate the pace of regulation to accelerate in the near future, as it is likely that additional states will follow California's lead in enacting their own similar privacy laws. However, applying a reactive approach to data privacy by attempting to comply with new privacy laws as they are enacted in different states is a costly and inefficient tack to take, and one that should be avoided at all costs. Rather, in light of this growing trend toward greater regulation over how businesses collect, process, and sell consumer data, it is imperative that financial institutions develop comprehensive data privacy programs that integrate the overarching privacy requirements mandated by the CCPA into all facets of their operations so they can be prepared to adapt to the rapidly shifting landscape of American data privacy law. ■