WINSTON & STRAWN LLP

CLIENT ALERT

What Financial Institutions Need to Know About the California Consumer Privacy Act

AUGUST 5, 2019

For the last 20 years, financial institutions have primarily relied on the Gramm-Leach-Bliley Act (GLBA) to wall themselves off from strict adherence to the ever-changing set of state privacy laws. However, with the quickly approaching January 1, 2020 effective date of the hastily drafted California Consumer Privacy Act (CCPA), the exemption that financial institutions have grown accustomed to is set to crumble.

To complicate matters further, leading the charge of change in this field is an ever-growing and increasingly aggressive plaintiffs' bar armed with newly established private rights of action allowing for potentially debilitating class action damages calculations. Indeed, while the CCPA is the most well-known, several similar privacy laws are following in its wake—with over a dozen more percolating in legislative chambers from coast to coast. As such, the time is now for financial institutions to understand how the CCPA and similarly situated laws will impact their compliance obligations and business operations in this new era of privacy regulation.

Unquestionably, the United States has historically lagged behind other countries in its regulation of personal information; generally, the legal regime has been such that organizations may collect, use, and share personal information so long as they appropriately disclose their treatment of that data. That landscape slowly shifted over the past decade, with an increasing focus on providing transparency and respecting individuals' choices, until the CCPA came along in the summer of 2018.

The CCPA imposes extensive requirements on information that was largely unregulated in the past, including identifiers as simple as consumer names, addresses, and IP addresses. In addition, the CCPA's private right of action and statutory damages for data breaches will significantly increase the liability of organizations storing California residents' personal information.

It is important to note that the CCPA contains a limited exception for GLBA-covered entities. The CCPA does "not apply to personal information collected, processed, sold, or disclosed pursuant to (GLBA), and implementing regulations…." However, this is not a general exemption for financial institutions. The CCPA exempts only *information* covered by GLBA; it does not exempt *entities* covered by GLBA. Further, since the scope of the CCPA is much broader than that of GLBA, there will be significant gaps between exempted information and the total cache of personal information collected by financial institutions.

In particular, GLBA regulates non-public personal information that a covered entity collects in connection with providing a financial service or product. In contrast, the CCPA uses a broad definition of personal information that includes any 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…." Because financial institutions collect information from or about individuals outside of their direct product or service offering, that information will still be subject to the CCPA, as it falls outside of the GLBA exemption. One example is information collected from website visitors (e.g., through passive cookie trackers), many of whom may not be customers. Another example is location data collected from individuals—either directly or through geo-location trackers—to, for example, provide special offers based on location or residency.

It is possible that the CCPA's GLBA exemption could be revised or expanded through implementing regulations, which are still in the process of being promulgated by the California regulators. While this remains unclear, the CCPA effective date is approaching and other states are also contemplating similar legislation. As such, financial institutions should begin to take steps to comply with the CCPA and monitor the aforementioned copy cat legislation that has been introduced in more than a dozen states since the CCPA's passage

With this in mind, how will the CCPA affect financial institutions? Most notably, the CCPA grants consumers several rights, some of which are similar to GLBA's Privacy Rule. These include the right to know what personal information is being collected by an organization and whether that information is being disclosed to any third party; the right to opt out of allowing the organization to sell their personal data; and the right to access any personal data stored by the organization. The CCPA also forbids organizations from discriminating against individuals who exercise these rights.

In addition to providing consumers with rights, the CCPA imposes extensive disclosure obligations regarding how organizations process California residents' personal data. This includes a requirement to notify individuals of what information is being collected; the purpose of the collection; and how the information will be shared. This disclosure must take place *before* information is collected. Organizations must also let website users easily opt out of allowing their data to be sold to third parties.

With the effective date of the CCPA rapidly approaching, there are several steps that financial institutions can take now to address compliance obligations.

- *First*, it is critical to understand your organization's data flow and identify the extent to which this data is subject to the CCPA. This can be addressed through a data mapping exercise to document what types of information your organization has; where it came from; how it was collected; when it was collected; where it is stored; how it is used inside of your organization and shared outside of your organization; what rights or consents your organization has; what contracts regulate your organization's ability to use and share the data; and which third parties "touch" the data. This exercise is especially important for financial institutions to help determine what information may not be subject to the GLBA exemption.

- *Second*, it is important to proactively conduct a security assessment before the end of the calendar year and take any measures reasonably necessary to address material vulnerabilities. Such an assessment will help uncover existing risks to data under your organization's purview and identify appropriate remediating measures. In addition, this may be an opportune time to examine any existing employee data privacy and security training and introduce new training to address key issues (e.g., phishing emails). Such an assessment may also provide demonstrable evidence of your organization's diligent and sincere efforts to protect consumer data in the event that your organization faces class action litigation following a data breach.

- *Third*, using the insights gleaned through the data mapping exercise, your organization can take steps to implement or update public-facing privacy notices to incorporate the disclosures required under the CCPA. Relatedly, your organization should begin planning for how to handle the breadth and anticipated volume of consumer requests under the CCPA, and develop effective mechanisms in place to efficiently handle such requests.

- *Finally*, your organization can begin the laborious process of collecting and updating relevant contracts that touch on or govern the transfer of personal information for the purposes of incorporating legally required updates to

comply with the CCPA's disclosure requirements. This includes both consumer contracts (e.g., website click wrap agreements) and contracts with third-party recipients of personal data.

How Winston & Strawn Can Help

Winston takes a cross-practice approach to addressing challenges posed by the CCPA and other pending state laws. Our team of privacy counselors and litigators helps clients understand their obligations under these laws while proactively addressing and taking steps to mitigate potential regulatory and class action exposure.

Winston's team includes a former federal privacy regulator and seasoned class action defense attorneys, several former Assistant U.S. Attorneys, and other counselors and litigators who have deep experience advising clients in complicated privacy matters.

5 Min Read

Related Locations

Charlotte | Chicago | Dallas | Houston | Los Angeles | New York | San Francisco | Silicon Valley | Washington, DC

Related Topics

Technology | Corporate | Finance | Biometrics | Data Privacy

Related Capabilities

Financial Services Transactions & Regulatory | Privacy: Regulated Personal Information (RPI) | Litigation/Trials | Transactions | Financial Services

Related Regions

North America

Related Professionals

Alessandra Swanson

Sean G. Wieber

Eric Shinabarger

Becky Troutman