November 20, 2019

California Consumer Privacy Act: Compliance Best Practices for Investment Managers

In 2018, the State of California enacted a wide-sweeping privacy law for California resident consumers titled the California Consumer Privacy Act of 2018 (CCPA), which goes into effect January 1, 2020. In contrast to other state privacy laws that established privacy standards, the CCPA creates specific affirmative rights and bases for legal action for individuals.

Although SEC-registered investment advisers are subject to the Gramm-Leach-Bliley Act (GLBA) and Regulation S-P promulgated thereunder,[1] all advisers, whether registered or not, may also be subject to the requirements of the CCPA, as described below. The CCPA provides California residents with the right to seek a private right of action against investment managers for data breaches if reasonable security policies and procedures are not in place and followed by the manager. Additionally, the California attorney general can bring civil enforcement actions and assess penalties against investment managers of up to $7,500 per violation, depending on the severity of the violation. Thus, failure to comply with the CCPA will have significant repercussions to investment managers.

This client alert describes the general parameters of the CCPA, including its applicability to investment managers located within and outside the State of California, along with reviewing best practices for compliance. In addition, this alert will examine the possible exemptions available to investment managers subject to the GLBA.

Last, whether the CCPA applies or not, in view of the number of other states considering privacy bills, along with proposed federal legislation, investment managers would be well advised to be proactive in designing their processes and systems and when engaging vendors to create their systems in order to conform to the types of requirements contained in the CCPA. As seen in Europe with the General Data Protection Regulation (GDPR), it is only a matter of time until the United States adopts wide-ranging data privacy and security rights for individuals.

The CCPA

The CCPA requires certain for-profit businesses that collect "personal information"[2] from California consumers[3] (Covered Entities) to respect certain rights of privacy of such consumers; namely, that Covered Entities will have to (i) provide consumers access to their personal information collected within the past 12 months;[4] (ii) delete their personal information if so requested and (iii) cease the sale of their personal information if such consumers opt out of such sale. Similar to the GLBA, under the CCPA, Covered Entities must provide notices to consumers about the types of personal information collected by them and the purpose of collection.

Who does the CCPA apply to?

The CCPA applies to any Covered Entity doing "business" in the State of California[5] and meets one of the following criteria: (i) has annual gross revenue of over $25 million;[6] (ii) buys, shares, sells or receives personal information of 50,000 or more California resident[7] consumers (which includes households or electronic devices, such as phones, tablets, computers, etc.) per year (whether directly or through third parties); or (iii) derives at least 50 percent of its annual revenue from selling California consumers' personal information. Therefore, as long as the investment manager, including a non-U.S. investment manager and non-California domiciled investment manager, collects, buys, shares, sells or receives personal information of California consumers, households or electronic devices, the CCPA will likely apply.

In addition, the CCPA will also apply to any entity that is owned or controlled by, or that owns or controls, a Covered Entity *and* shares common branding with such Covered Entity. "Control" or "controlled" under the CCPA means ownership of, or the power to vote, more than 50 percent of the outstanding shares of any class of voting security of a business; control in any manner over the election of a majority of the directors or of individuals exercising similar functions; or the power to exercise a controlling influence over the management of a company. "Common branding" means a shared name, service mark or trademark.

Differences between the GLBA, GDPR and CCPA

The CCPA exempts personal information that is collected, processed, sold or disclosed pursuant to the GLBA and its regulations, but it is not a blanket exemption for investment managers. The exemption relates to core financial services data (e.g., receiving and reviewing a loan application from a consumer, opening a credit card with a financial institution, and opening a checking or savings account for personal purposes), but investment managers are using alternative data that California regulators may not have considered in the GLBA exemption, in particular, web scraping data, social media, advertisement spend data, shipping data, satellite and drone data, pharmaceutical prescription data, data from financial aggregators, and credit card data, to name a few. In addition, if there is a data breach, the GLBA exemption does not apply and the investment manager would remain liable for damages under the CCPA.

The CCPA applies to "personal information" that is any data that identifies, relates to, describes or could be reasonably linked, directly or indirectly, to a particular consumer. The GLBA is more narrowly drawn than the CCPA; the GLBA protects a consumer's non-public personal information, which is "personally identifiable financial information" such as information provided by a consumer to a financial institution. The CCPA may also pick up personal information about prospective investors, which falls outside the GLBA exemption under the CCPA and within the CCPA requirements.

While there are many similarities between the GDPR and the CCPA, such as the individual's right to have protected information deleted and to limit the use of their information, compliance with the GDPR does not exempt a business from complying with the CCPA, nor does it guarantee full compliance with the requirements of the CCPA. For example, the deadlines for responding to consumer requests are different and the CCPA requires a Covered Entity have a toll-free number for California consumers to use to contact said Covered Entity.

What steps should investment managers undertake to determine whether they possess "personal information" of California consumers?

Investment managers should undertake a data-mapping effort to evaluate the data they collect; although not required by the Securities and Exchange Commission (SEC), it is consistent with the best practices procedure noted by the SEC's Office of Compliance Inspections and Examinations for cybersecurity compliance. In addition, managers should take the following steps: (i) identify and train key personnel within the firm responsible for collecting, using and maintaining the personal information; (ii) identify the relevant California resident (client or contact of the investment manager); (iii) determine the personal information flowing into the investment manager–"data scraping" with respect to California consumers; (iv) categorize the personal information collected from such consumers in the preceding 12 months into the 12 categories defined in the CCPA; (v) identify personal information flowing out of the investment manager and the purpose of such disclosures—whether any information is being sold and what the repercussions are of these sales with compliance under the CCPA; and (vi) ensure that data retention policies and online privacy notices are updated and consistent with the requirements of the CCPA. Although the CCPA does not mandate the use of encryption, managers should consider ensuring that all personal information is encrypted and appropriately redacted, because as of January 1, 2020, all California residents will be entitled to bring a private right of action for security breach of the individual's non-encrypted and non-redacted personal information and recover damages of $100 to $750 per consumer per incident or actual damages, whichever is greater.

Additional amendments on the horizon under the CCPA

Two amendments were recently signed into law by the governor of California that hopefully address those situations where the GLBA exception falls short. These amendments allow additional time—until January 1, 2021—for managers who are

Covered Entities to be in compliance with the CCPA with respect to personal information collected from job applicants, employees, owners, directors, officers, contractors and certain business-to-business contacts. The California attorney general is also required to adopt regulations on or before July 1, 2020, to clarify certain aspects of the CCPA.

Although not presently required, investment managers should start thinking about implementing a nationwide "data management" standard to guide its internal operations. This is not the same as implementing a universal data privacy policy that gives the same rights to all consumers, regardless of a consumer's place of residence. Using the most consumer-friendly consumer privacy law as a guide for establishing internal data management standards will put businesses in a good position for the anticipated arrival of similar "rights"-granting legislation. Other states are likely to take a page from California's book; in fact, New York, Massachusetts and Maryland may not be far behind California in enacting new consumer privacy legislations modeled on the CCPA and the GDPR.

For additional information on the CCPA, the GDPR or state privacy laws, investment managers may contact their Day Pitney investment management lawyer or any of the members of the Day Pitney Privacy and Security team:

Richard (Rick) Harris

Michael Dunne

Susan Huntington

Alex P. Garens

Kritika Bharadwaj

---

[1] Investment advisers who are registered with the states in which their principal offices are located are regulated by the Federal Trade Commission, not the GLBA.

[2] "Personal information" means any information that identifies, relates to, describes, is capable of being associated with or could reasonably be linked, directly or indirectly, with a particular individual consumer, device or household. This definition may also pick up names, email addresses, account information, Social Security numbers, browser history and a wide array of other types of personal information, including information provided to an administrator for Know Your Customer purposes, capital account statements and information in a subscription agreement.

[3] A "consumer" is defined as any natural person who is a California resident. A consumer may or may not be a prospective or actual customer of the investment manager.

[4] The CCPA includes a provision requiring investment managers provide consumers with their personal information collected up to 12 months prior to the date of the request.

[5] There has been no guidance thus far from the California attorney general on what constitutes "doing business"; in the absence of such guidance, we recommend taking a broad interpretation of "doing business," which would include, among other activities, soliciting investors in California and entering into contracts with California service providers, regardless of where the investment manager resides.

[6] There is no specific definition of what constitutes "revenue." It is unclear if revenue in this context relates only to revenue derived from within the State of California or whether the manager would need to aggregate revenue derived from affiliates (e.g., management fees earned by the manager and carried interest allocated to a general partner affiliate).

[7] "California resident" means individual customers, households and electronic devices that are either in California for other than a temporary or transitory purpose or domiciled in California but are outside the state for a temporary or transitory purpose.

Authors



Eliza Sporn Fromberg
Partner

New York, NY | (212) 297-5847

efromberg@daypitney.com



Kritika Bharadwaj
Partner

New York, NY | (212) 297-2477

kbharadwaj@daypitney.com



Peter J. Bilfield
Partner

Stamford, CT | (203) 977-7569

New York, NY | (212) 297-5853

pbilfield@daypitney.com



R. Scott Beach
Partner

Greenwich, CT | (203) 862-7824

Stamford, CT | (203) 977-7336

rsbeach@daypitney.com



Richard D. Harris
Of Counsel

Hartford, CT | (860) 275-0294

New Haven, CT | (203) 752-5094

rdharris@daypitney.com