The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 32017

October 21, 2019

Important Updates Relating to the California Consumer Privacy Act

[32017]

October 21, 2019 TO: ICI Members
Chief Compliance Officer Committee
Chief Risk Officer Committee
Internal Audit Committee
Operations Committee
Privacy Issues Working Group
SEC Rules Committee
Transfer Agent Advisory Committee SUBJECTS: Privacy
State Issues RE: Important Updates Relating to the California Consumer Privacy Act

As we previously advised you, in July 2018, California Governor Jerry Brown signed into law The California Consumer Privacy Act of 2018 (CCPA), which takes effect January 1, 2020. Earlier this month, there were two significant developments relating to the CCPA that members should be aware of: (1) California Governor Newsom signed into law amendments to the CCPA that provide an exemption for employee information; and (2) California Attorney General Becerra published for comment proposed rules to implement the CCPA. Each of these developments is briefly described below.

More extensive information about the CCPA and its impact on members of the Institute and other financial institutions is available on the Institute's California Consumer Privacy Law Resource Center, which members can access through the Institute's password-protected website through this link: https://www.ici.org/ca_privacy**.**

Revisions to the CCPA

While the CCPA applies to all businesses with California consumers, Section 1798.145(e) of it provides an exemption from the CCPA for any business that collects information pursuant to Title V of the Gramm-Leach-Bliley Act (GLBA). While this exemption carves most of a financial institution's business out of the CCPA, information a financial institution collects on its California employees or trustees does not fall within the GLBA exemption because such information is not collected pursuant to the GLBA. This employee information would include both the information the institution collects on its own California employees or trustees *and* the information it may obtain on individuals (consumers) associated with other businesses that the institution acquires in the course of conducting due diligence or other business

transactions and communications. As a result, as the CCPA was originally enacted in 2018, even if a mutual fund as a financial institution did not have to implement the CCPA with respect to the information it collects, processes, or discloses on its shareholders, it would have to implement it with respect to the information it collects, processes, or discloses on employees or trustees.

The Institute is pleased to report that, during the 2019 session of California's General Assembly, working together with the California Chamber of Commerce and others, we were successful in having the CCPA revised to include a new exemption for employee information. In particular, with respect to a business's own employees, a new subsection (g) was added to Section 1798.145 to provide as follows:

(g) (1) This title[1] shall not apply to any of the following:

> (A) Personal information that is collected by a business about a natural person in the course of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the natural person's personal information is collected and used by the business solely within the context of the natural person's role or former role as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or a contractor of that business.
>
> (B) Personal information that is collected by a business that is emergency contact information of the natural person acting as a job applicant to, an employee of, owner of, director of, officer of, medical staff member of, or contractor of that business to the extent that the personal information is collected and used solely within the context of having an emergency contact on file.

This amendment clarifies, however, that the exemption does not extend to two provisions of the CCPA – *i.e.,* Sections 1798.100(b)[2] and 1798.150.[3] This was to ensure that employees have (1) a right to be informed of the categories of information their employer collects about them and (2) recourse in the event of a breach of such information. Importantly, these newly added provisions, which were signed into law on October 12, 2019, will expire by operation of law on January 1, 2021. It is hoped that, in lieu of addressing employees' privacy concerns in the CCPA, they will instead be addressed in a more comprehensive way during the 2020 legislative session the California General Assembly, thereby rendering moot the need for retaining these provisions in the CCPA.

With respect to consumer (employee) information an institution collects from another business in the course of conducting due diligence of engaging in transactions or communications with such other business, a new subsection (m) was added to Section 1798.145 of the CCPA to provide an exemption for this information:

> The obligations imposed on businesses by Sections 1798.100, 1798.105, 1798.110, 1798.115, 1798.130, and 1798.135[4] shall not apply to personal information reflecting a written or verbal communication or a transaction between the business and the consumer, where the consumer is a natural person who is acting as an employee, owner, director, officer, or contractor of a company, partnership, sole proprietorship, non-profit, or government agency and whose communications or transaction with the business occur solely within the

context of the business conducting due diligence regarding, or providing or receiving a product or service to or from such company, partnership, sole proprietorship, non-profit, or government agency.

This provision is intended by its sponsor to exempt employee information captured in a business-to-business transaction.

As a result of these revisions to the CCPA, it appears that, until January 1, 2021, the only provisions in the CCPA that financial institutions subject to both the GLBA and the CCPA need to implement are:

- The provision in Section 1798.100(b) that imposes upon an employer a duty to inform its employees, prior to or at the time of collecting personal information from such employees, of the categories of personal information that will be collected from them and how the employer plans to use such information;[5] and
- With respect to employee information obtained in connection with a business-to-business transaction, the provision in Section 1798.120 that provides a consumer to right to opt-out of the sale if the consumer's personal information.

The Attorney General's Rulemaking

The CCPA requires California's Attorney General to adopt rules necessary to implement it. After conducting a series of hearings throughout California to inform this rulemaking initiative, on October 11, 2019, the Attorney General published proposed rules for comment. The text of these proposed rules along with the Statement of Reason for them and the Economic and Fiscal Impact Statement associated with them can be found at: https://www.oag.ca.gov/privacy/ccpa. Comments are due on the proposed rules by December 6, 2019.

The Institute is currently reviewing the proposed rules to determine whether we need to comment on behalf of our member in light of the exemptions in the CCPA discussed above that they can now rely on.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] As used in this new provision, "title" refers to the entirety of the CCPA with the exceptions of Sections 1798.100(b) and 1798.150, which are discussed in this memo.

[2] Section 1798.100(b) provides as follows:

(b) A business that collects a consumer's personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.

[3] Section 1798.50 authorizes any consumer whose nonencrypted or nonredacted personal

information is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business' violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information to institute a civil action for damages and other relief the court deems proper.

[4] The provisions referenced are as follows:

> Section 1798.100, Consumer's Right to Request Information;
>
> Section 1798.105, Consumer's Right to Request Deletion of Information;
>
> Section 1798.110, Consumer's Right to Request Categories of Information Collected;
>
> Section 1798.115, Consumer's Right with Respect to Information Sold or Disclosed;
>
> Section 1798.130, Notices Required Under Sections 1798.100, 1798.105, 1798.11, 1798.115, and 1798.125; and
>
> Section 1798.135, Opt-Out Link.

The provisions that remain applicable to this information notwithstanding this carve out are:

> Section 1798.120, Consumer's Right to Opt-Out of the sale of the consumer's information; and
>
> Section 1798.150, Liability/Enforcement, which provides a consumer the right to institute a civil suit in the event of a reach of nonencrypted information.

[5] Pursuant to Section 1798.130 and 1798.140 of the CCPA, it appears that the "categories" referred to in this provision include the following: identifiers (e.g., real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers); commercial information (e.g., records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies); biometric information; Internet or other electronic network activity information (e.g., browsing history, search history, and information regarding the employee's interaction with an Internet Web site, application, or advertisement); geolocation information; audio, electronic, visual, thermal, olfactory, or similar information; professional or employment-related information' and education information,

should not be considered a substitute for, legal advice.