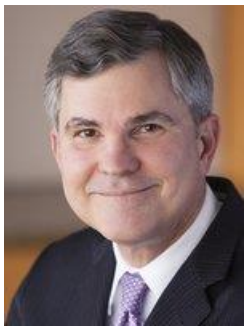
Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Calif. Privacy Law Considerations For Private Funds

By **Reece Hirsch and Brian London**



Reece Hirsch

Brian London

(April 2, 2020, 5:50 PM EDT) -- This article discusses when private investment funds and their managers are subject to the California Consumer Privacy Act and similar state laws, when they are exempt, and what they need to do to comply. It also includes a compliance checklist for managers of private funds that collect personal information.

What is the California Consumer Privacy Act?

The CCPA was signed into law on Jan. 28, 2018, by then-Gov. Jerry Brown, ushering in what appears to be a new era in U.S. privacy regulation. The principal features of the CCPA, which became effective on Jan. 1, 2020, include the creation of the following new consumer privacy rights for residents of California:

- The right to know specific pieces and categories of personal information to be collected about the consumer;
- The right to receive a privacy policy;
- The right to have personal information deleted;
- The right to opt out of the sale of personal information to third parties; and
- The right to equal service and price.

The enforcement date for the CCPA is now six months after the Attorney General's Office issues regulations, so organizations subject to the CCPA must adopt policies and procedures designed to put them in compliance with the law no later than July 1.

Who enforces the CCPA?

The CCPA can be enforced by the California attorney general. Private plaintiffs may also bring an action under the CCPA with respect to a security breach involving personal information, with statutory damages available.

But there is a wrinkle: Businessman Alastair Mactaggart, the primary backer of the California ballot initiative that was the impetus for the CCPA, has formally filed the California Privacy Rights and Enforcement Act, a new initiative that will appear on the California ballot in November if it obtains sufficient signatures.

The proposed ballot measure includes provisions that would add significant new privacy obligations to the CCPA, eliminate the California attorney general's responsibility for enforcing the CCPA, and grant that authority to a new California Privacy Protection Agency.

Are there any exemptions from CCPA obligations for managers of private investment funds?

Yes. The CCPA would not apply to the following information collected by private fund managers.

Personal Information Subject to the GLBA

The consumer privacy rights obligations of the CCPA do not apply to personal information collected, processed, sold, or disclosed pursuant to the Gramm-Leach-Bliley Act, with which many private fund managers are already complying.

Note, however, that the scope of the CCPA is broader than the scope of the GLBA, which is limited to nonpublic personal information of consumers and does not always cover prospective investors.

For instance, if a private fund manager were to collect marketing-lead information about high-net-worth individuals that might become potential customers of the manager's financial services, then that personal information is likely to be subject to the CCPA's consumer privacy rights because an individual on a list of leads has not yet become a consumer or customer of the manager, as those terms are defined under the GLBA. Accordingly, the GLBA exemption cannot be relied on as a blanket exemption to the CCPA in all instances.

Employee, Officer, Director, Applicant and Contractor Information

The CCPA exempts certain personal information collected from job applicants, employees, owners, directors, officers and contractors of a business from most requirements of the CCPA for one year, until Jan. 1, 2021.

The information covered by the exemption includes personal information (1) collected about a person as a job applicant, employee, owner, director, officer, medical staff member, or contractor of that business; (2) collected and used solely for the purpose of maintaining emergency contact information; and (3) collected and used solely to administer benefits to an individual, all of which would typically be categorized as human resources data.

Note, however, that fund managers that would otherwise be subject to the CCPA would still be required to provide these individuals with a CCPA-compliant privacy notice.

B2B Transaction Data

To the extent that a private fund manager collects personal information of individual representatives of institutional investors or other business customers, such personal information should qualify for the CCPA's business-to-business exemption, which applies to personal information (1) reflecting a written or

verbal communication or transaction between a business and a consumer; and (2) where the consumer is an individual acting as an employee, owner, director, officer, or contractor of a business.

In many cases, such information will qualify for both the B2B and GLBA exemptions.

When would a private fund manager be subject to the CCPA?

The CCPA will generally apply to private fund managers that collect personal information of California consumers that is not subject to an exemption such as those listed above, do business in California, determine the purposes and means of processing that personal information and (1) have annual gross revenues in excess of $25 million; (2) buy, receive, sell or share personal information of 50,000 or more consumers, households or devices; or (3) derive 50% or more of their annual revenue from selling consumer information.

The CCPA defines "consumers" broadly as natural persons who are California residents. This could include, for instance, current fund investors, prospective investors, advisory clients, employees and applicants who are California residents.

The scope of personal information under the CCPA is broad. For instance, when a business collects information about visitors to a website through the use of cookies or a "Contact Us" page, that information may be considered personal information under the CCPA's broad definition of that term.

The CCPA does not define what it means to do business in California, and therefore, absent further guidance, this term is likely to be construed broadly. For instance, a private fund manager may be considered to be doing business in California just by operating a website in which California residents are permitted to provide their personal information, even if the manager is not organized under California law and has no physical presence in California.

What should be on a private fund manager's compliance checklist?

For a private fund manager that is not eligible for an exemption and is subject to CCPA obligations, the compliance checklist below includes actionable steps that the manager can take to ensure compliance and many other useful tips. These action steps should be completed before the compliance date of July 1, 2020.

Identify California Ties and Relevant Data Elements

Consider whether any current fund investors, prospective advisors, employees, or other business contacts are California residents, whether any of the manager's processes may be collecting personal information from California residents, and for what purposes that information is used.

As discussed above, the scope of "personal information" under the CCPA is broad. As of Jan. 1, it includes any information that "identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," such as (but not limited to) the following information routinely collected in the course of know your client and investor onboarding processes:

- Name, address, personal identifier, IP address, email address, account name, Social Security number, driver's license number and passport number;

- Personal information under California's records destruction law (Cal. Civ. Code § 1798.80(e)), which additionally includes signature, physical characteristics or description, telephone number, insurance policy number, education, employment, employment history, or financial account information;

- Professional or employment-related information; and

- Education information that is not publicly available personally identifiable information, as defined in the Family Educational Rights and Privacy Act.

Update Privacy Policies and Procedures

Update privacy policies and procedures to provide disclosures required under the CCPA regarding a consumer's rights to know, to opt out and to be forgotten.

Businesses covered by the CCPA must disclose, at or before the point of collection, in their website privacy policy or otherwise, the following:

- The categories of personal information to be collected about the consumer and the purposes for which the information will be used; and

- The categories of consumers' personal information that were actually collected in the preceding 12 months and sold or disclosed for business purposes in the preceding 12 months.

Businesses must provide notice to consumers that their personal information may be sold and inform consumers that they have the right to opt out of such sale. In order to comply with the right to opt out, a business must describe the right and include a link to the "Do Not Sell My Personal Information" page in its privacy policy.

Businesses must also inform consumers of their right to be forgotten. The CCPA does not state how consumers should be informed of this right, but one of the best paths to compliance would be to add such a provision to the privacy policy.

Review Service Provider Agreements

Ensure that the applicable agreements limit the service provider's use of personal information as strictly as the CCPA requires and revise as necessary.

The CCPA allows businesses to share personal information with third parties or service providers for business purposes, so long as there is a written contract prohibiting the third party or service provider from selling the personal information or "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."

Note: On Feb. 7, the California Office of the Attorney General proposed amendments to the draft regulations implementing the CCPA that, if adopted, would modify certain service provider obligations.

The CCPA defines "business purpose" as "the use of personal information for the business's or service provider's operational purposes, or other notified purposes, provided that the use of personal

information shall be reasonably necessary and proportionate to achieve the operational purpose for which it was collected."

The CCPA enumerates categories of activities that constitute business purposes, including auditing; detecting security incidents; performing services, such as maintaining or servicing accounts, providing customer service, processing payments, fulfilling orders and transactions, and providing analytic services; and undertaking internal research for technological development and demonstration.

Conduct Employee Training and Implement Processes to Respond to Consumer Requests

Ensure that personnel responsible for handling consumer inquiries regarding the CCPA's new privacy rights are informed of the applicable requirements and know how to direct consumers to exercise those rights.

Businesses must make available two or more designated methods for the consumer to request this information, including, at a minimum, a toll-free telephone number and website address (if the business maintains a website).

However, as of Jan. 1, a business that operates exclusively online and has a direct relationship with a consumer is only required to provide an email address for submitting requests.

Consumers have the right to make such requests twice in any 12-month period.

In response to such requests, the CCPA requires businesses to disclose:

- The categories of personal information the business collected about the consumer;
- The categories of sources from which personal information is collected;
- The business or commercial purpose for collecting or selling personal information;
- The categories of third parties with whom the business shares personal information;
- The specific pieces of personal information the business has collected about the consumer; and
- The categories of the consumer's personal information that were sold or disclosed for business purposes in the 12 months preceding the consumer's verifiable request.

Create a Robust Incident Response Plan

While implementing a robust incident response plan has been a best practice for some time, the CCPA's new statutory damages and civil penalties further underscore the need for a thoughtful and comprehensive approach to breach response because the CCPA will almost certainly lead to a spike in data breach–related litigation in California.

W. Reece Hirsch is a partner and co-head of the privacy and cybersecurity practice at Morgan Lewis & Bockius LLP.

Brian T. London is an associate at the firm.

This article is excerpted from Lexis Practice Advisor®, a comprehensive practical guidance resource that includes practice notes, checklists, and model annotated forms drafted by experienced attorneys to help lawyers effectively and efficiently complete their daily tasks. For the full version of this article, click here. For more information on Lexis Practice Advisor or to sign up for a free trial, please click here. Lexis is a registered trademark of RELX Group, used under license.

Law360 is owned by LexisNexis Legal & Professional, a RELX Group company.