MCINTYRE & LEMON PLLC

DECEMBER 2018

Visit our blog for regular updates on consumer protection news for the banking and insurance industries:

blog.mcintyrelf.com

STATE SPOTLIGHT

CALIFORNIA'S CONSUMER PRIVACY ACT — IMPACT ON BANKS, INSURANCE COMPANIES AND AGENCIES, AND OTHER FINANCIAL INSTITUTIONS

Born from the European Union's General Data Protection Regulation (GDPR) and the recent uptick in data breaches (*e.g.*, Cambridge Analytica, Equifax, and Target), the California Consumer Privacy Act (CCPA) will provide Californians with the most stringent consumer privacy protections in the country. The compliance burdens of the CCPA will affect not only California companies; companies that operate beyond the borders of the Golden State may also have to comply. Only time will tell if other states opt to provide their residents with the same level of protection, but one thing is clear: data privacy protections are here to stay, and California wants to lead the way.

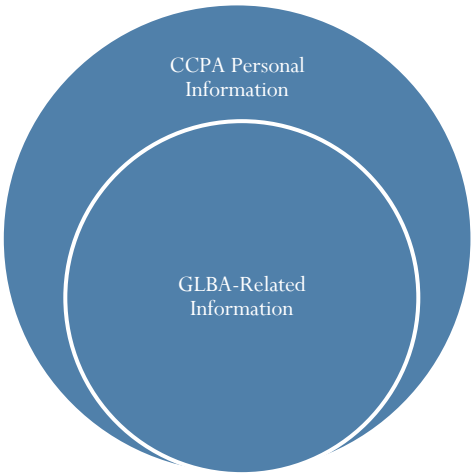
What Type of Information is Covered by the CCPA?
The CCPA's primary goal is to provide consumers with increased transparency, access, and control over their *personal information*, which the CCPA broadly defines as "information that identifies, relates to, [or] describes, . . . directly or indirectly, . . . a particular consumer or household." In other words, *personal information* is any information a business could use to identify a California consumer or household — for example, a consumer's name and address, education records, biometric information, location data, IP addresses, and internet browsing and search history.

Which Businesses Must Comply with the CCPA?
The CCPA applies to any business that collects the *personal information* of California residents and: (a) has annual gross revenues that exceed $25 million; (b) derives 50 percent or more of its annual revenues from selling *personal information*; *or* (c) annually buys, receives, or shares for commercial purposes the *personal information* of 50,000 or more consumers, households, or devices. Because of the Act's expansive definition of *personal information*, the threshold triggers are easier to cross than may be apparent. For example, a small business that neither sells *personal information* nor meets the annual revenue threshold may, nevertheless, be subject to the CCPA if it simply collects 50,000 or more IP addresses annually from California consumers who visit its website.

Does the CCPA Apply to Personal Information Collected or Sold by Banks, Insurance Companies and Agencies, and Other Financial Institutions?
Maybe. The CCPA does "not apply to personal information collected, processed, sold, or disclosed pursuant to the federal Gramm-Leach-Bliley Act [GLBA], and implementing regulations . . . [,]" except that it does permit a private right of action for data breaches. The scope of this GLBA exemption will need to be clarified via regulation, but what is certain is that the scope of information subject to the CCPA is much broader than the information regulated by the GLBA.

Specifically, the GLBA only regulates the handling of personally identifiable financial information that a financial institution collects in connection with an

individual obtaining or seeking to obtain a financial product or service (i.e., GLBA-related information).



Accordingly, financial institutions that are collecting and sharing consumer information outside the scope of the GLBA, may need to assess the CCPA's compliance requirements.

What Non-GLBA Related Information Would Constitute CCPA-Personal Information?

Financial institutions regularly collect *personal information* from website visitors. If the financial institution is collecting *personal information* from someone who is neither a pre-existing customer nor is applying for a financial product or service, the information collected is likely subject to the CCPA. Examples include:

- The website visitor's search history or cookies
- Information regarding the visitor's interaction with the website
- The visitor's IP address
- Geolocation data

What Rights Does the CCPA Provide Consumers?

A financial institution that collects non-GLBA related information that is subject to the CCPA will need to comply with a number of CCPA provisions. The CCPA provides consumers with four primary rights: (1) The right to know what *personal information* is being collected and whether the *personal information* is to be sold or disclosed and to whom; (2) the right to say "no" to the sale of *personal information* (a/k/a *opt-in* and *opt-out* rights); (3) the right to access *personal information*; and (4) the right to equal service and price, even if privacy rights are exercised. How the CCPA implements each of these rights is discussed in turn below.

1. The Right to Know

When a company *collects personal information*, it must make "reasonably accessible," through a privacy policy or otherwise, the categories of *personal information* it collects, the purposes for which it collects the information, and the categories of information it has disclosed or sold in the preceding 12 months.

2. The Right to Opt-out and Opt-in

Companies that *sell personal information* must give consumers the opportunity to opt out. Accordingly, the CCPA requires that all companies have a "Do Not Sell My Personal Information" link on their website that enables consumers to opt out of having their *personal information* sold. The CCPA's *opt-out* provisions apply to all consumers age 16 and over.

The CCPA also has a number of *opt-in* provisions for minors. For example, the CCPA prohibits a business from selling the *personal information* of consumers if the business has "actual knowledge" that the consumer is under the age of 16 unless the consumer (or their parent/legal guardian for children under 13) has affirmatively authorized the sale.

Although the CCPA does not define *actual knowledge*, it does state that businesses that "willfully disregard" a consumer's age will be deemed to have actual knowledge of the consumer's age. To comply with the CCPA's *opt-in* provisions, companies will likely need to either directly request the consumer's age or implement an age verification system.

3. The Right to Access Personal Information

The CCPA allows consumers to exercise their *right to access* their *personal information* for free up to two times a year. Within 45 days of a *verifiable consumer request*, a company must deliver to the consumer all the *personal information* it holds on the consumer, including *personal information* obtained from third parties.

Because businesses may store *personal information* in different locations, databases, and servers, the process of identifying, capturing, and delivering all of the consumer's *personal information* may be logistically challenging. Further, companies will need to create internal compliance procedures for dealing with the CCPA's consumer request deadlines and provide customer service employees with additional training to handle consumer requests.

4. The Right to Equal Service and Price

Businesses must not *discriminate* against consumers who exercise their rights under the CCPA. Consequently, when a consumer exercises their rights, a business may not deny goods or services, impose a penalty, charge a different price, or provide a different level of service. In complying with this provision of the CCPA, companies should carefully review existing pricing policies and practices to verify that they do not intentionally or unintentionally discriminate against consumers who opt out of — or do not opt in to — the sale of their *personal information*.

When Does the CCPA Become Operative?

The CCPA becomes operative on January 1, 2020, but California's attorney general is not required to issue interpretive regulations until July 1, 2020, and the attorney general is prohibited from bringing an enforcement action until six months after publication of the final regulations or July 1, 2020, whichever is sooner.

Although this should provide companies with sufficient time to revamp their privacy compliance regime, companies that have been proactive in preparing for the General Data Protection Regulation have seen the benefits of getting a head start. Consequently, companies should not wait to start thinking about compliance strategies and planning how to address operational difficulties that may arise to fully comply with the law.

How will the CCPA be Enforced?

The majority of the CCPA's provisions will be enforced by the California attorney general. The CCPA provides for civil penalties of up to $7,500 for intentional violations of the CCPA.

For private actions, the CCPA grants consumers, either individually or as a class, statutory or actual damages if their *personal information* is subject to "unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information . . . ." Thirty days before filing a complaint against an organization, consumers must notify the organization of any alleged violations.

How We Can Help?

McIntyre & Lemon, PLLC is continuing to monitor the operational and compliance implications of the CCPA for financial institutions. McIntyre & Lemon, PLLC can help your organization determine whether you need to comply with the CCPA, and if necessary, assist in developing revised privacy policies and procedures that comply with the CCPA.

Contact: Chrys Lemon at cdl@mcintyrelf.com or Michael Aphibal at maphibal@mcintyrelf.com, both at 202-659-3900.

Follow McIntyre & Lemon's blog to stay up-to-date on the latest consumer protection news affecting the consumer finance, banking, and insurance industries:

blog.mcintyrelf.com