MEMORANDUM

JULY 9, 2020

Schneider Smeltz Spieth Bell LLP

CALIFORNIA CONSUMER PRIVACY ACT

The California Consumer Privacy Act ("CCPA") went into effect on January 1, 2020 and granted broad privacy rights to California residents and imposed obligations on covered businesses regarding the use of personal information. Penalties for non-compliance vary with administrative fines imposed by the California Attorney General ($2,500 per violation or $7,500 per intentional violation) and the CCPA allows for a private cause of action.

Briefly, the CCPA grants California residents broad rights as to how their personal information is used by businesses. These rights include the right to know what information businesses maintain about them, the right to have businesses delete that information and the right to opt out from the sale of personal information by a business.

The CCPA imposes obligations on "Covered Businesses". A "Covered Business" is any for profit business doing business in California that collects a consumer's information and determines the means and purposes of processing that information (whether alone or with others) and meets one or more of the following criteria: (a) has annual revenue in excess of $25 million (it is unclear whether this threshold is calculated from global revenue, revenue combined between parent level and subsidiaries, revenue derived only from business within California or some other metric), (b) the business annually buys, receives, shares for commercial purposes or sells the personal information of more than 50,000 consumers or households, or (c) the business derives more than 50% of its annual revenue from the sale of personal information. Entities that control or are under common control with a Covered Business and that share common branding are also subject to the CCPA.

Given the nature of e-commerce and the expansive definitions in the CCPA, the CCPA will impact businesses based outside of California. That likelihood is magnified by the broad definition of personal information in the CCPA. Personal information is "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." This broad definition specifically includes eleven categories of information ranging from obvious personal identifiers (names, addresses, social security numbers etc….) to non-obvious categories such as information generated from employment and business to business interactions.

While the CCPA provides big picture guidance on what is legally permitted and prohibited, much was left to implementing regulations. To that end, The California Attorney General issued multiple versions of proposed regulations. The proposed final regulations were issued in June of 2020 and are subject to final review and approval by the California Office of Administrative Law (the "Regulations"). The Regulations provide needed framework as to what businesses need to do. Broadly, these obligations fall within 2 categories: notice to consumers and responses from businesses to consumer requests.

There are 4 types of notices due from covered businesses, (1) a privacy policy, (2) notices due at the point of data collection, (3) notices of financial incentives and (4) opt out notices. These notices are self-explanatory from their titles and generally all need to be written in plain language, made visible and be in a format accessible to persons with disabilities. Not all businesses need to provide all 4 notice types.

Schneider Smeltz Spieth Bell LLP

The Regulations address each notice and its required contents in detail. For privacy policies, covered businesses need to notify consumers on what information a business collects, uses, discloses and sells. The privacy policy needs to include how consumers can submit requests to exercise their rights, how businesses will respond to requests and additional disclosures concerning a businesses' information practices including categories of personal information collected, business purposes for collecting or selling personal information and whether a business sells personal information.

Notices at collection are notices that are made available to consumers at or before the information is collected. The timing, display and to some extent content will vary by business depending on each businesses' purpose for collecting information.

An opt-out notice is a notice to a consumer when a business sells personal information of consumers. The Regulations detail how the notice is to be posted, how to approach offline vs. online interactions and content of the notice.

A notice of financial incentive explains to a consumer the terms of a financial incentive or price difference the business offers due to the collection, retention or sale of personal information. Just like the other three categories of notices, the Regulations detail what the notice of financial incentive needs to include.

The Regulations also address how businesses need to approach consumer requests related to their personal information. The Regulations cover the methods in which consumers can request action by businesses, the timeline in which businesses need to respond and how businesses are to respond.

A business needs to confirm a request within 10 business days and generally must respond to a request within 45 calendar days (subject to an extension in certain circumstances). The methods in which consumers can request action depend on each business and look to several factors such as how the business operates and the business's primary interaction with consumers.

Before responding, businesses need to verify the identity of the person making a request. In no event should a business disclose a consumer's social security number, driver's license number or similar identification number or security questions and answers in response to a request to know.

Beyond the forbidden disclosure of extremely sensitive information, different types of information require different degrees of verification. Some information requests may require at least 2 verifiable data points to confirm the identity of the requestor while other requests may require at least 3 verifiable data points and a declaration from the requestor (signed under penalty of perjury) that the requestor is the consumer whose personal data is the subject of the request.

The distinction between these two approaches (referred to as a reasonable degree of certainty and a reasonably high degree of certainty, respectively) centers on the sensitivity of the personal information and the risk of harm to the consumer posed by unauthorized deletion.

While the Regulations remain subject to final review and approval, businesses should review the CCPA and the Regulations and take steps to come into compliance as soon as possible. While the future finalization (and potential for change, either via subsequent legislation or regulation) puts businesses in an awkward position taking action now helps mitigate the risk of fines and enforcement actions in the future.

The foregoing is a summary of extensive legislation and not intended as legal advice.

Should you have questions about this update and any implications to your unique circumstances, please contact Michael Schauer at mschauer@sssb-law.com