PUBLICATION

The Effect of California's New Privacy Laws on Your Company

Authors: Alisa L. Chestler
October 09, 2014

California Governor Jerry Brown signed into law on September 30, three amendments to California's privacy laws of which every business must be aware. The amendments to the Civil Code (i) significantly broaden the scope of businesses that are required to have data security procedures in place; (ii) establish minimum requirements for identify theft prevention and mitigation services if such services are offered in response to a data breach; and (iii) forbid the sale, offer to sell or advertisement for sale of an individual's social security number, except under limited circumstances. These amendments go into effect on January 1, 2015.

Businesses do not need to have a physical presence in California for this law to be in effect. Any company that maintains any personal information on a California resident must adhere to the new laws.

Expanded Scope of Security Requirements

Before the adoption of these amendments, businesses that owned or licensed "personal information about a California resident" were required to "implement and maintain reasonable security procedures and practices . . . to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." The new law expands this requirement to businesses that "own, license, or ***maintain***" personal information about California residents. The law defines "maintain" to include "personal information that a business maintains but does not own or license," and the terms "own" and "license" are defined as "personal information that a business retains as part of the business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." For purposes of this data security requirement, "personal information" is defined as an individual's first name or first initial and last name in combination with any one or more of the following elements, when either the name or the elements are not encrypted or redacted: (a) social security number; (b) driver's license number or California identification card number; (c) account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; and (d) medical information. Because the California law now includes businesses that "maintain" personal information about California residents, it significantly expands the number of businesses that must comply with its requirements. In particular, third-party service providers, such as cloud storage, software-as-a-service and platform-as-a-service appear to be subject to these data security requirements.

This is the same law requiring that any business that discloses personal information about California residents to nonaffiliated third parties pursuant to a contract, must then require by contract that those same third parties implement and maintain reasonable security procedures and practices. These kinds of contractual obligations are certainly more common and are becoming a major point in the negotiation of contracts.

Minimum Requirements for Identity Theft Prevention and Mitigation Services

The newly-adopted amendments also establish minimum requirements for identity theft prevention and mitigation services when such services are offered as part of a notification made in response to a data breach. The requirements only apply if the person or business providing the notification was the source of the breach. If identity theft prevention and mitigation services are offered, the offer must be made to "any person whose information was or may have been breached if the breach exposed or may have exposed personal information," the services must be provided "at no cost to the affected person for not less than 12 months," and

the offer must contain all of the information necessary to take advantage of the offer. It is important to note that this amendment does not require a person or business to offer or provide identity theft prevention and mitigation services. Rather, it establishes minimum requirements for such services ***if*** such services are offered. While others have reported that offering identity theft prevention and mitigation services is required under the new law, the language was amended before the law was finalized, and the addition of certain language appears to have softened the requirement.

Sale and Advertisement for Sale of Social Security Numbers Prohibited

The third important privacy law that was recently amended affects the actions a person or business can take with respect to an individual's social security number. Currently, a person or business is prohibited from taking certain actions that may compromise an individual's social security number, such as publicly posting or publicly displaying a social security number, requiring an individual to transmit a social security number over the Internet in clear text, or printing a social security number on materials mailed to an individual (unless required by law). The amendment prevents a person or business from selling, advertising for sale or offering to sell an individual's social security number except for certain exceptions. These exceptions include "the release of an individual's social security number if the release of the social security number is incidental to a larger transaction and is necessary to identify the individual in order to accomplish a legitimate business purpose," and "the release of an individual's social security number for a purpose specifically authorized or specifically allowed by federal or state law." The "minimum necessary" concept is not a new concept in the area of privacy and security of personal information, but this broad application and requirement should cause all enterprises to re-evaluate their practices.

As a result of these new amendments, businesses that "maintain" personal information should carefully assess their data security procedures and practices to ensure they comply with California law. Businesses should also reexamine their service provider contracts to ensure that any necessary amendments are pursued.

If your business needs help with its data security procedures and practices, or if you have questions about this Alert or any other federal or state privacy laws, please contact your Baker Donelson attorney.