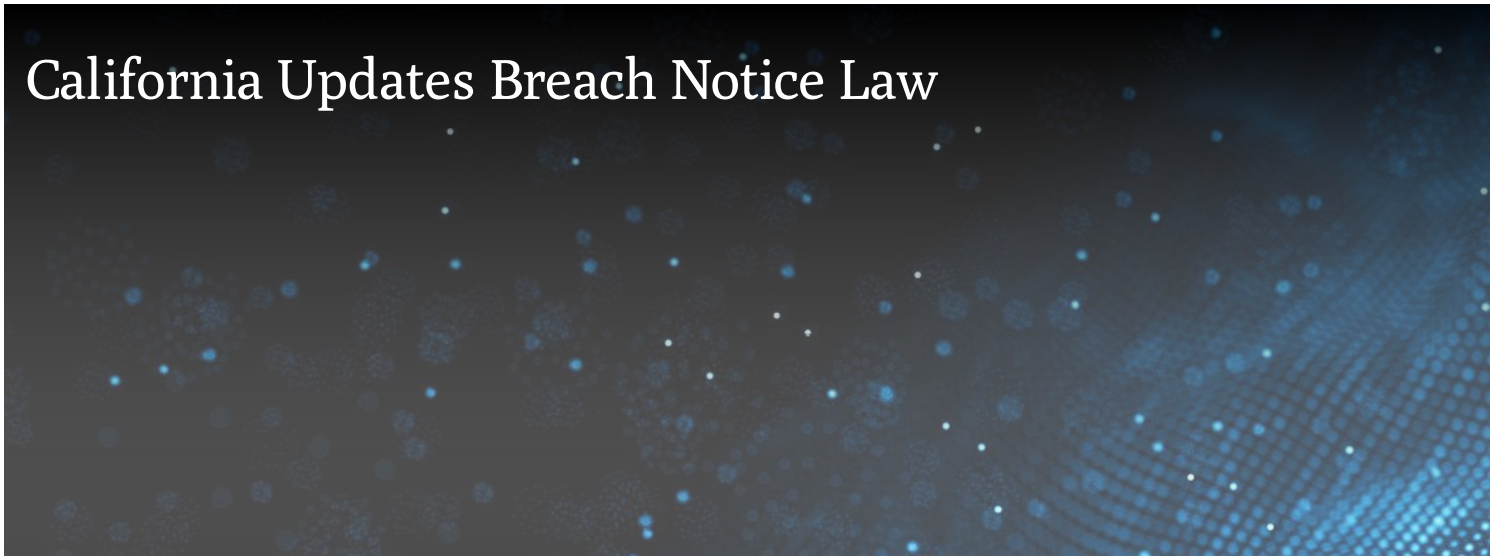
WINSTON & STRAWN LLP

BLOG

California Updates Breach Notice Law



OCTOBER 7, 2014

California Governor Jerry Brown has signed into law an amendment to California's data breach notification law. The revised law impacts those who are the "source of a breach" (a phrase that is undefined in the law), which breach exposed or may have exposed the social security number, driver's license number or government identification number of a Californian. In particular, the amended law now states that "an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months, along with all information necessary to take advantage of the offer." Given the inclusion of the phrase "if any" in this sentence, confusion has arisen regarding whether this amendment *requires* offering identity theft prevention and mitigation services, or if it simply places certain requirements on the identity theft prevention and mitigation services for those entities that *choose* to offer such services. A plain language reading of the statute suggests that the latter interpretation is more accurate, such that only those entities that *elect* to offer identity theft prevention and mitigation services need to comply with the requirements set forth in the law. That said, the legislative history associated with the law suggests that the legislature intended to make the offering of these services mandatory. For example, the California Senate Judiciary Committee analysis of June 23, 2014, provided, "This bill would…*require* the person or business providing notification that was the source of the breach to provide to affected consumers with [sic] identity theft prevention and mitigation services for a minimum of 12 months." In addition, the author's press release announcing the Governor's signing of the bill indicates that the bill "[r]equires the source of the breach to offer identity theft prevention mitigation services…."

The amendment also impacts portions of the law which govern how companies must protect personal information. Entities that maintain information on behalf of third parties are now required to provide security for personal information (rather than just those who own the information being required to provide protection). As amended, companies will also not be able to sell -or offer to sell- social security numbers. These new provisions will go into effect January 1, 2015.

TIP: Most companies that offer credit monitoring and similar ID theft mitigation services following a breach are unlikely to find the requirements of this amendment to be onerous. Indeed, most identity theft services begin at a minimum of 12 months, and are offered by impacted companies for free. Given the ambiguity in the amendment, it seems prudent given the ambiguity for those who suffer a breach where Californians are impacted to offer ID theft mitigation services that meet the standards outlined in the amendment. While it may

be defensible to elect not to provide such services given the plain-language of the amendment, making such a decision would not be without potential risk of drawing regulatory scrutiny.
2 Min Read

Related Locations

Chicago

Related Topics

Data Breach

Related Capabilities

Privacy & Data Security

Related Regions

North America