BRYAN CAVE
A Broader Perspective
Bulletin

Data Privacy & Security Team

To: Our Clients and Friends October 7, 2014

California Amendments to Data Breach Law Create Panic…Over Nothing.

California's Governor signed into law Assembly Bill No. 1710 on September 30th, enacting the latest round of changes to California's data breach notification law, Cal. Civ. Code § 1798.82. A flurry of internet activity quickly erupted over whether the amendment requires companies who are victims of a data breach to provide identity theft prevention and loss mitigation services to affected California residents. Despite the differences in interpretation, the language of the statute should make clear that California **has not** become the first state to take such drastic measures.

The existing law has long required notification to affected California residents and, where more than 500 residents are impacted, to the California Attorney General, in the event of a security breach involving the unauthorized acquisition of certain types of personal information (*e.g.*, social security number, driver's license number, financial account information, medical information). A January 2014 amendment also requires notification if the breach involved the username or email address and password that would permit access to an online account.

As of September 30th, the law now requires that:

"If the person or business providing the notification was the source of the breach, 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 to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h)." (emphasis added). Cal. Civ. Code § 1798.82(d)(2).

Relying on basic principles of statutory construction, the phrase "if any" modifies "an offer to provide appropriate identity theft prevention and mitigation services." Accordingly, the most reasonable interpretation of the statute is that **if** a breached entity **chooses to provide** identity theft prevention and mitigation services, **then** it must meet certain requirements under California law. These requirements include:

(1) providing the services for at least 12 months;

(2) for free; and

(3) notifying the California recipients of such services how they can take advantage of the free offer.

As a practical matter, companies that offer such mitigation services typically already do so under these conditions, and the effect of this latest amendment likely will be minimal.

Adding further support to this interpretation is a prior version of the bill which would have provided for the mandatory offering of identity theft prevention and mitigation services if the breach involved specific personal information. This provision was quickly changed to include the "if any" language and to remove the mandatory offering requirement, proving that California is not quite ready to be the first state to legally mandate credit monitoring or identity theft protection services after a data breach.

For more information, please contact Jena Valdetero in Chicago at +1 312 602 5056, David Zetoony in Boulder at +1 303 444 5955, or any member of Bryan Cave's Data Privacy & Security Team. In the event of a data breach, you can reach our team 24 hours a day, 7 days a week, by calling our hotline at +1 844 8BREACH.