Portfolio Media. Inc. | 860 Broadway, 6th Floor | New York, NY 10003 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

New Calif. Data Breach Law May Fall Short

By **Jonathan Randles**

Law360, New York (October 03, 2014, 5:03 PM ET) -- California's new data security law is among the first responses to breaches at Target Corp. and other major retailers, but some attorneys question whether the measure can deliver on its mandate to provide free credit monitoring and if that safeguard will be needed when card issuers jump to chip technology.

Gov. Jerry Brown this week signed into law A.B. 1710, which requires businesses that handle customer data to provide identity theft prevention services in case of an intrusion. The statute also extends California's existing data-security law and obligations to entities that maintain customer information in addition to businesses that either own or license it.

The legislation was introduced by California lawmakers earlier this year in response to the high-profile breaches at Target, Neiman Marcus Group Ltd. and Michaels Stores Inc. The string of cyberattacks has continued throughout 2014, most recently at the Home Depot Inc., which confirmed a massive breach earlier this month.

When it was originally proposed, the law sought to make businesses financially responsible for consumer losses after a breach — a provision that industry groups fought. The final law is more modest, and California attorneys told Law360 that while the statute is a positive step for consumers, the law is poorly written and could be costly for smaller businesses.

BakerHostetler partner Tanya Forsheit said questions remain about exactly what the legislative language requires, so if other states attempt to follow California's lead, they could run the risk of misinterpreting the statute. Forsheit's take on A.B. 1710's potential problems requires a close reading of the statute, which states in part:

“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.”

Forsheit said the phrase “source of the breach,” important for determining which entity is at fault for the breach and responsible for remedial measures, is ambiguous.

Another potential issue is the “if any” language, a phrase Forsheit said was inserted into later versions of

the bill. A lawyer could argue that this means a company is not mandated to automatically give affected customers credit monitoring service in the event of a breach, she said. Under this interpretation of the law, Forsheit said the 12-month requirement would kick in only if a company does provide mitigation service to customers.

“There are a number of articles out there that are saying the bill requires organizations to offer free credit monitoring for 12 months. I will tell you, I do not think the language of the statute is sufficiently clear to impose that requirement. There is considerable ambiguity about that,” Forsheit said.

“I think it would be a mistake for anyone to jump to the conclusion that [A.B. 1710] requires credit monitoring in any circumstance where you have a breach involving Social Security numbers or driver's licenses,” she added.

Other attorneys Law360 spoke with questioned the effectiveness of the credit monitoring service that would be required and the potential financial obligations it would impose on medium and small businesses.

Justine Phillips, special counsel at Sheppard Mullin Richter & Hampton LLP, said the law will extend California's data security requirements to many small and mid-size businesses that don't own or license personal information but do maintain it. In light of the new law, businesses should examine the way in which they handle personal data, Phillips said.

“This legislation is a clear message to all California businesses: Not understanding the technology your business is using and the data your business is maintaining is no longer acceptable or reasonable," Phillips said. “Businesses now have an affirmative obligation to implement reasonable security procedures and practices.”

Sharon Klein — chair of Pepper Hamilton LLP’s privacy, security and data protection practice — said the benefit to consumers of mandatory credit monitoring may be short-lived. Klein said it is unlikely that such mitigation will be necessary once the financial industry switches from payment cards that use magnetic strips to ones using so-called chip-and-PIN technology, which are more difficult to counterfeit.

The U.S. is one of the few remaining developed countries that relies on magnetic strip technology for credit and debit cards, according to the bill. Canada, Mexico, Brazil and other countries in Europe and Asia have already implemented microchip technology, according to the California Legislature.

Moreover, Klein said the benefits of credit monitoring would likely not extend to younger consumers whose driver's licenses or Social Security numbers could be compromised but who do not own credit or debit cards. But while A.B. 1710 should not be seen as a “silver bullet” for protecting consumer data, Klein said, it is a step forward.

“I'm generally in favor of the statute. We have to prevent identity theft,” Klein said. “Anything, from a consumer and parent perspective, to shore that up — even if it's short-term — I'm in favor of. As a California resident, not speaking as a lawyer, I think it's good.”

--Editing by Kat Laskowski and Patricia K. Cole.

All Content © 2003-2014, Portfolio Media, Inc.