

THE
NATIONAL LAW REVIEW

California Amends Its Data Breach Notification Law...Again

Thursday, November 10, 2016

Under [this most recent change](#) to **California's** breach notification laws (California Civil Code sections 1798.29 and 1798.82), which takes effect January 1, 2017, businesses and agencies subject to the laws can no longer assume that notification is not required when the personal information involved in the breach is encrypted.

Under current California law, notification of a breach is required when a California resident's personal information was, or is reasonably believed to have been, acquired by an unauthorized person, and that personal information was unencrypted. Thus, before the change made by **AB 2828**, if an unauthorized person acquires encrypted personal information of California residents, notification is not required.

Beginning in 2017, notification will be required for breaches of encrypted personal information of California residents under the following conditions:

- encrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person,
- the encryption key (confidential key or process designed to render the data readable) or security credential was, or is reasonably believed to have been, acquired by an unauthorized person, **and**
- there is a reasonable belief that the encryption key or security credential could render that personal information readable or useable.

You should also remember there was a change to these laws that became effective in 2016 which addressed encryption. On October 6, 2015, California Governor Jerry Brown signed three laws which substantially altered and expanded the state's security breach notification requirements. Among those changes, [Assembly Bill 964](#) added a definition for encryption:

rendered unusable, unreadable or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information technology.

This language seems to allow for flexibility in the types of encryption that can be applied, as well as for future changes in encryption technology. But, with the more recent change, a breach involving personal information protected under a standard meeting the definition above still may trigger the statute's notification requirements if the encryption key or security credentials also are involved and there is a reasonable belief that as a result the personal information will be readable or useable.

Jackson Lewis P.C. © 2019

Source URL: <https://www.natlawreview.com/article/california-amends-its-data-breach-notification-law-again>



Article By [Jackson Lewis P.C.](#)
[Joseph J. Lazzarotti](#)
[Workplace Privacy Blog](#)

[Communications, Media & Internet](#)
[California](#)