CLIENT NEWS BRIEF

Data Breach Notification Law Gets Updates With Important Implications

January 2020
Number 2

Data breaches are all but inevitable and occur in all types of organizations. Public entities are no exception, with cyber criminals increasingly targeting the wide-range of sensitive information they maintain (e.g., student data, resident data, confidential government infrastructure data, etc.). Against the backdrop of and in response to this looming threat of cyber-attacks, Governor Newsom recently signed into law Assembly Bill (AB) 1130, which makes small but significant changes to the state's existing data breach notification laws.

Current Law

Under Civil Code section 1798.29, any agency (including a local government or school district) that owns or licenses computerized data that includes personal information has an obligation to provide notice to any California resident whose unencrypted personal information is or is reasonably believed to have been acquired without authorization. Notification to affected individuals must be made in the format and include the information specified in the law. Importantly, notification obligations are triggered when the acquired information includes personal information as defined under the law, unless the information was encrypted and the security credentials or encryption key that would permit access to the information was not also acquired. As defined under the law, personal information includes an individual's first name or first initial, and last name, in combination with certain other types of information including social security number, driver's license number, and medical information. For a more detailed discussion, including the specific information required to be included in a breach notice, see Lozano Smith's 2017 TIPJar Article.

New Law

Effective January 1, 2020, AB 1130 amends the definition of personal information under Civil Code section 1798.29 with the purpose of addressing perceived gaps in the categories of sensitive information protected under the law. Under these amendments, personal information will now include an individual's first name or first initial, and last name, in combination with either of the following (in addition to the data elements previously included in the definition):

- Driver's license number, California identification card, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual.
- Unique biographic data generated from measurements or technical analysis of human body characteristics, such as fingerprint, retina, or iris image, used to authenticate a specific individual (not including a physical or digital photograph, unless used or stored for facial recognition purposes).

These changes have the potential to significantly impact public entities in terms of data breach notification obligations. Because biometric data is less


Devon B. Lincoln
Partner
Monterey Office
dlincoln@lozanosmith.com


James N. McCann
Associate
Fresno Office
jmccann@lozanosmith.com

Lozano Smith
ATTORNEYS AT LAW

commonly found in public entity databases, the largest impact from the new law will likely be the expansion of the types of government identification numbers that, if disclosed, may create a reportable event. By including within this definition "other unique identification numbers issued on a government document," the law now potentially encompasses many additional types of information used by public entities to identify individuals within their databases and which they would not normally associate with or guard as personal information, one of example of which would be student identification numbers.

Takeaways

The best response to the threat of a cyber-attack is being prepared for it. Public entities should act now to review their data security and breach incident policies and procedures to ensure those documents define a reportable incident in compliance with the changes made by AB 1130. Personnel responsible for the organization's data security should be placed on notice of these changes and instructed to make updates to all relevant policies, procedures, and data security training, as appropriate. Finally, those organizations without such policies or procedures should strongly consider adopting them to ensure they are prepared to comply with the California's breach notification requirements, when, not if, an information security incident occurs.

If you have any questions about AB 1130 or data security breach notification obligations of public entities in general, please contact the authors of this Client News Brief or an attorney at one of our eight offices located statewide. You can also subscribe to our podcast, follow us on Facebook, Twitter and LinkedIn or download our mobile app.