Supplement to the Los Angeles and San Francisco

Daily Journal

COVER STORY JANUARY 21, 2014

NEW CALIFORNIA LAWS FOR 2014

PERSPECTIVE

AB 1149: Expanding state data breach notification rules

By Jake Romero

California has expanded its data breach notification requirements by adding certain online account information to the definition of "personal information" used to determine whether notification is required under state law. As a result, a number of online service providers may, for the first time, be subject to California's notification requirements.

Previously, California's notification requirements were triggered when the information accessed during a data breach included an individual's name, in combination with the individual's (1) Social Security number, (2) driver's license or California ID number, (3) account, credit or debit card number together with a security or access code, (4) medical information or (5) health information, where either piece of information was not encrypted. Senate Bill 46 and Assembly Bill 1149 amend the definition of "personal information" under California Civil Code Sections 1798.29 and 1798.82 to include, in addition to the information listed above, a "user name or email ad-dress, in combination with a password or security question and answer that would permit access to an online account."

The expanded definition will have a significant impact. As shown in the 2012 Data Breach Report released by California Attorney General Kamala Harris, the number of breach incidents that require notification has already risen dramatically. Online account information is commonly collected by online services, which means that adding that type of information as a trigger for data breach notification may exponentially increase the number of entities that are subject to those requirements.

Entities that collect this type of information should take steps to ensure they are ready in the event of a data breach. First, the business or agency should perform an audit of security measures to assess its risk profile, taking into account, among other things, the categories of information collected, the number and location of individuals whose information is collected and stored, the security measures in place and the number of employees and third parties who have access to such information. Businesses and agencies should be counseled to share user personal information with third parties only when necessary to provide services. For notification purposes, an online service provider can be held equally responsible if the entity who experiences the data breach was a third party who received the information from that provider. Any third party with whom an entity shares personal information should be contractually required to meet reasonable standards for protecting that information.

If the information collected by an entity did not qualify as "personal information" before the expansion, it is likely that the business or agency has not put appropriate policies in place to limit risk and ensure readiness. At a minimum, such entities should maintain a data retention policy to ensure that only necessary information is collected and information that is no longer needed (such as user information linked to closed or inactive accounts) is promptly deleted, as well as a breach response plan detailing steps to be taken following discovery of a breach.

Data breach incidents are, in the words of Adobe Systems Inc. Chief Security Officer Brad Arkin, "one of the unfortunate realities of doing business today." Following the expansion of California's notification requirements, it is even more important that your client's business or agency is ready for the unfortunate reality of a breach before it happens. Ensuring that protections are in place will not stop every incident, but adequate planning can help limit the disruption.

Jake Romero *is an associate in the San Diego office of Mintz Levin Cohn Ferris Glovsky and Popeo PC and can be reached at JRomero@mintz.com.*