Montgomery & Hansen LLP

Client Alert September 30, 2014

California Amends Data Breach Notification Law

On September 30, 2014, Governor Jerry Brown signed into law several amendments of California's data breach notification law and California's prohibition on certain uses of social security numbers. These amendments take effect on January 1, 2015.

Implementation of Security Procedures and Practices to Protect Personal Information

The recent breaches of security at national chain retailers such as Target and Home Depot have prompted calls for laws that better protect digitized personal information. Current California law requires organizations that own or license personal information about Californians to implement and maintain "reasonable security procedures and practices" to protect that personal information from unauthorized access, destruction, use, modification and disclosure. In the event of a known or suspected breach, the law also requires those organizations to notify California residents whose information may have been compromised of the breach. California's Civil Code provides that California residents who have suffered harm attributable to a breach of these requirements may sue the companies that failed to comply and may recover damages.

One of the new amendments extends the first requirement (that of implementing and maintaining reasonable security procedures and practices) to organizations that maintain personal information, even if they don't own it or license it from others. Thus, businesses that host or otherwise retain data for others, such as cloud and co-location service providers, and retail businesses that collect information from their customers but do not own or license it, must now implement and maintain reasonable security procedures and practices if that data contains any personal information.

For purposes of California's data breach law, "personal information" means a person's first name or initial and last name in combination with any one or more of the following data elements: (i) social security number, (ii) driver's license number, (iii) California identification card number, (iv) an account, credit or debit card number in combination with any required security code, access code or password or (v) any individually identifiable information regarding the person's medical history, medical treatment or diagnosis by a health care professional. However, personal information that is encrypted does not trigger the law's compliance requirements.

The new amendment does not specify the scope of what it means to "maintain" personal information. Consequently, "maintain" can be interpreted quite broadly; and businesses that collect personal information about California residents would be prudent to comply with the law's requirements, at least until future cases provide clarification.

The law also does not specify what security procedures and practices will be considered sufficient, other than to say that those measures must

For more information changes to California's Data Breach Law, please contact Daniel Appelman at dappelman@mh-llp.com or at 650-331-7014.

be "appropriate to the nature of the [personal] information." Thus, the law leaves it up to each business to implement what it deems to be reasonable security measures under the circumstances. Whether those measures are sufficient or insufficient will be determined in retrospect by a court when the business is sued for failure to comply with the law.

Offers of Identity Theft Prevention and Mitigation Services

Another recent amendment requires businesses experiencing a breach of their security systems to offer all affected persons not less than twelve months of free identity theft prevention and mitigation services along with all information necessary to take advantage of the offer. This applies only to those who own or license the personal information that has been compromised, not to those who merely maintain that information. This amendment does not specify what identity theft and mitigation services to offer or any minimum benefits that must be included with those services.

Amendment of Prohibitions on Certain Uses of Social Security Numbers

California law currently prohibits businesses from (i) publicly posting or displaying social security numbers, (ii) printing social security numbers on cards required to access products or services, (iii) requiring individuals to transmit their social security numbers over the Internet in an unsecured or unencrypted fashion, (iv) requiring the use of social security numbers to access Internet web sites without also requiring a password or unique personal identification number or other authentication device to access that web site, and (v) printing social security numbers on any materials that are mailed, unless state or federal law requires it.

The new California amendments also make it illegal to sell, offer to sell, or advertise for sale any individual's social security number. However, the release of a social security number for a purpose allowed by federal or state law, or as part of a larger transaction where the release is necessary in order to accomplish a legitimate business purpose, does not violate the new law.

Tips and Recommendations.

(1) Most businesses, regardless of where located, that maintain computerized databases that include personal information will have to comply with California's breach notification law because those databases are likely to include personal information about California residents.

(2) If possible, Companies that own, license or maintain computerized data that include personal information should encrypt either the names of the individuals contained in their databases or the data elements or both. The requirements in California's breach notification law to provide reasonable security for personal information and to notify those affected by a breach in that security do not apply if the personal information is encrypted.

(3) Offering theft prevention and mitigation services following a breach is now mandatory for companies that actually own or license personal information, and the offer must comply with the new requirements mentioned above. Companies that maintain personal information (but do not own or license it) who experience a breach should consider this type of offer as a form of best practices to mitigate harm, even though this part of the law does not apply to them.

(4) Keep in mind that each state enacts its own laws in the data privacy area and those laws vary significantly from one another. At least three other states, Florida, Kentucky and Iowa, recently amended their personal information breach notification laws, and California has enacted several previous amendments since its law first became effective in 2003. This is an area of the law that changes frequently, and California is often in the forefront of those changes. Companies must keep up to date on protection and breach notification requirements that affect how they conduct their business in all states.

The changes described in this client update are contained in **Assembly Bill 1710.** They amended Sections 1798.81.5, 1798.82 and 1798.85 of California's Civil Code.

Client Alert September 30, 2014

Montgomery & Hansen, LLP provides notices from time to time to keep its clients updated on important changes in the law that may affect their business. If you have any questions about how these new amendments or California's breach notification law in general applies to you, please contact your **M&H attorney**.