ALSTON & BIRD LLP

WWW.ALSTON.COM

Privacy & Security ADVISORY ■

SEPTEMBER 30, 2014

California Governor Signs New Data Breach Law

By Dominique R. Shelton, Kim Peretti and Sheila Shah

Retailers and consumer-facing businesses should take note of three small but important changes to California's privacy laws. On September 30, 2014, Governor Brown signed Assembly Bill 1710, which made the following changes to existing privacy and data security laws:

- California businesses that "maintain" personal information on state residents are now required to adopt reasonable security procedures to protect personal information (a requirement that previously only applied to businesses that own or license such data);
- California's breach notification law now requires that notifying entities offer identity theft protection and mitigation services to affected individuals in certain cases; and
- the state's Social Security number (SSN) protection law now prohibits the sale or advertisement for sale of such numbers, with limited exception.

These amendments will take effect on January 1, 2015.

The Amended California Privacy Laws

New Security Obligations for Companies that Maintain Personal Information

A.B. 1710 amended Civil Code Section 1789.81.5, a data security law designed to encourage businesses to protect the personal information of California residents. Previously, the law required businesses that ***own*** or ***license*** "personal information about a California resident" to "implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure." The bill amended the existing law by requiring businesses that merely "***maintain***" personal information, in addition to businesses that own and license personal information, to adopt reasonable security procedures to protect personal information. The term "maintain" is defined only within the context of what it means to "own or license" data, as the amended statute defines "maintain" as including "personal information that a business maintains but does not own or license. " A business "owns" or "licenses" personal information that it "retains as part of the

business' internal customer account or for the purpose of using that information in transactions with the person to whom the information relates." The bill did not change California Civil Code Section 1789.81.5's definition of "personal information"; personal information is still defined as including the individual's first name or first initial and last name in combination with one or more of the following data elements, when either the name or the data elements are not encrypted: Social Security Number; driver's license number or California Identification Card number; account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; medical information; or health insurance information. As reported in Alston & Bird's prior client alert California Expands Data Breach Notification Law to Include Breaches of User Names and Email Addresses for Online Accounts, effective January 1, 2014, California amended its data breach disclosure law Civil Code Section 1798.82(h) to expand the definition of "personal information" for which breach notification is required. The newly added Civil Code Section 1798.82(h) adds to the definition of personal information for data breach disclosure: "A user name or email address, in combination with a password or security question and answer that would permit access to an online account." The new amendment proposed by A.B. 1710 does not expand the definition of personal information to include emails and account information for security obligations.

New Requirement to Offer Breach Mitigation Services

A.B. 1710 also amended California's breach notification law, California Civil Code Section 1798.82 (previously amended last year as discussed above), by requiring breached entities provide identity theft prevention services to affected individuals. While many breached entities (including Target and Neiman Marcus) already offer credit monitoring or similar services in the wake of a breach, this action is not required by any of the breach notification laws effective in 47 states and the District of Columbia. California is the first state to enact such a requirement. The amended California statute requires any notifying entity that is "the source of [a] breach" to offer affected individuals "appropriate identity theft prevention and mitigation services . . . at no cost to the affected person" for at least one year. Importantly, this requirement only triggers when an individual's name and either his or her social security number, driver's license number or California ID number was acquired by an unauthorized person as a result of a breach. While California residents must also be notified of a breach that compromised their financial account numbers and security codes, medical information or health insurance information, in such cases the notifying entity would not be required to provide identity theft services.

New Prohibitions on the Sale of Social Security Numbers

Finally, the bill further limits actions that persons or businesses may take with respect to SSNs. Previously, California Civil Code Section 1798.85 prohibited persons or entities from acting in ways that potentially compromised a person's Social Security number, e.g. publicly posting or displaying an SSN, prohibiting the transmission of an SSN over the internet in plain text, etc. The amended statute takes these protections further: California Civil Code Section 1798.85 now prohibits a person or entity from selling, advertising for sale, or offering to sell an SSN. The amended statute provides that "sell" does not include the release of an SSN if the release of the SSN is incidental to a larger transaction and is necessary to identify the individual in

order to accomplish a legitimate business purpose, nor does it include the release of an SSN for a purpose specifically authorized or specifically allowed by federal or state law. However, the amended statute is explicit that "[r]elease of an individual's [SSN] for marketing purposes is not permitted."

Legislative Landscape

A.B. 1710 was a direct response to data breaches involving consumer data at major retailers such as Target and Neiman Marcus over the 2013 holidays. However, the first iteration of A.B. 1710 was far more robust than the version that passed. In addition to the changes described above, previous iterations of the bill imposed payment data retention and storage limitations, stronger encryption standards in order to warrant an exemption from existing data breach notification law and direct notification to consumers when a business that maintains personal information is the source of a data breach. However, these provisions drew strong opposition from retailers and other consumer-facing businesses, who argued that these changes imposed onerous and unneeded data management mandates and created new financial liabilities for non-governmental entities that take payment cards or other payment devices. Opponents argued the changes would be ineffective and in some ways counterproductive to improving data security in California – it would increase fraud, waste resources that would be better spent on security and would result in over-notification that would ultimately confuse California consumers. As a result, the senate substantially narrowed the bill, deleting the encryption requirement and limiting or deleting other provisions.

Conclusion and Outlook: Companies That Maintain or Store Personal Information Should Understand Precedent on Reasonable Security Standards

Retailers and consumer-facing business that "maintain" personal information should become familiar with the new law and should assess their current data security procedures to ensure future compliance with the amended statute's "reasonable security" requirements. These groups should be aware that compliance in this area may require extra vigilance. Courts, regulators and legislators have yet to offer a comprehensive definition or standards regarding what constitute the "reasonable security" obligations imposed on businesses that maintain consumer personal information. Indeed, regulators like the Federal Trade Commission (FTC) continue to state that data security expectations are to be derived by companies from publicly available resources such as FTC reports, business education, congressional testimony, articles, blogs and settlements in enforcement actions. A thorough review of FTC guidance and enforcement orders is a good first step on getting a handle on what regulators and courts may consider to be "reasonable security." Alston & Bird's Cyber Security Updated Legal Risk Package has done precisely that insofar as it surveys all of the FTC's data security and privacy enforcement actions on an ongoing basis.

Please feel free to contact the undersigned or your Alston & Bird contact if you would like to discuss reasonable security obligations in light of California's new law.

Dominique R. Shelton | 213.576.1170 | dominique.shelton@alston.com

Kim Peretti | 202.239.3720 | kimberly.peretti@alston.com

Sheila Shah | 213.576.2510 | sheila.shah@alston.com

If you would like to receive future *Privacy & Security Advisories* electronically, please forward your contact information to **privacy.post@alston.com**. Be sure to put "**subscribe**" in the subject line.

If you have any questions or would like additional information, please contact your Alston & Bird attorney or one of the following:

Members of Alston & Bird's Privacy & Security Group

Atlanta

Angela T. Burnette
angie.burnette@alston.com
404.881.7665

Kristine McAlister Brown
kristy.brown@alston.com
404.881.7584

Lisa H. Cassilly
lisa.cassilly@alston.com
404.881.7945

Maki DePalo
maki.depalo@alston.com
404.881.4280

Clare H. Draper, IV
clare.draper@alston.com
404.881.7191

Peter K. Floyd
peter.floyd@alston.com
404.881.4510

James A. Harvey
jim.harvey@alston.com
404.881.7328

John R. Hickman
john.hickman@alston.com
404.881.7885

William H. Jordan
bill.jordan@alston.com
404.881.7850
202.239.3494

David C. Keating
david.keating@alston.com
404.881.7355

W. Scott Kitchens
scott.kitchens@alston.com
404.881.4955

Dawnmarie R. Matlock
dawnmarie.matlock@alston.com
404.881.4253

Kacy McCaffrey Brake
kacy.brake@alston.com
404.881.4824

Bruce Sarkisian
bruce.sarkisian@alston.com
404.881.4935

Katherine M. Wallace
katherine.wallace@alston.com
404.881.4706

Michael R. Young
michael.young@alston.com
404.881.4288

Los Angeles

Jonathan Gordon
jonathan.gordon@alston.com
213.576.1165

Katherine E. Hertel
kate.hertel@alston.com
213.576.2600

Sheila A. Shah
sheila.shah@alston.com
213.576.2510

Dominique R. Shelton
dominique.shelton@alston.com
213.576.1170

Washington, D.C.

Louis S. Dennig, IV
lou.dennig@alston.com
202.239.3215

Kimberly K. Peretti
kimberly.peretti@alston.com
202.239.3720

Eric A. Shimp
eric.shimp@alston.com
202.239.3409

Paula M. Stannard
paula.stannard@alston.com
202.239.3626

Jeffrey R. Sural
jeff.sural@alston.com
202.239.3811

ALSTON&BIRD LLP

WWW.ALSTON.COM