ALSTON & BIRD LLP

WWW.ALSTON.COM

Privacy & Security/Legislative & Public Policy ADVISORY ■

SEPTEMBER 20, 2013

California Expands Data Breach Notification Law to Include Breaches of User Names and Email Addresses for Online Accounts

S.B. 46 Adds Notification Requirements for Breaches of an Individual's User Name or Email Address in Combination with a Password or Security Question and Answer that Permit Access to an Online Account

By Dominique R. Shelton and Paul G. Martino

California Governor Brown is preparing to sign into law a new data security breach notification bill (S.B. 46) that expands the coverage of California's existing breach law to include breaches of individuals' online user names and email addresses, when acquired in combination with passwords or a security question and answer that would permit access to their online accounts. The bill passed the California legislature unanimously, by a final vote of 38-0 in the Senate on September 4, 2013, following final passage of an amended bill by the Assembly (77-0) on September 3, 2013. Governor Brown is expected to sign the bill before the expiration of the signing period on October 13, 2013.

Provisions of the Existing and Amended California Breach Notification Law

The new law amends the existing California data breach notification law, California Civil Code Section 1798.82, which has been in effect in California since July 1, 2003. That law already requires businesses and governmental agencies to notify consumers when a security breach occurs involving "an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted: (1) Social security number. (2) Driver's license number or California Identification Card number. (3) 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. (4) Medical information. (5) Health insurance information." Cal. Civ. Code Section 1798.82(h).

S.B. 46 amends Section 1798.82(h) to expand the definition of "personal information" for which breach notification is required. The new law adds to the definition: "A **user name or email address**, in combination with a **password or security question and answer** that would **permit access to an online account.**" [Emphasis added] Once the amendment is made to the statue, this new prong of the definition will appear as Cal. Civ. Code Section 1798.82(h)(2) and the existing definition will be redesignated as Section 1798.82(h)(1).

Notification for breaches of personal information involving user names and email accounts may or shall, depending on the circumstance, occur differently than with breaches involving other types of personal data. Specifically, the new legislation adds Section 1798.82(d)(4), which indicates how businesses "may comply" with the notification requirements of the statute in cases where no other personal information and no "login credentials of an email account" are breached. Where email login information is breached, new Section 1798.82(d)(5) specifically prohibits "providing the security breach notification to that email address."

The new rules for notification of breaches of an individual's user name or email address with accompanying password or security question and answer that permits access to an online account (defined, for purposes of this discussion, as "Online Account Data") may be summarized as follows:

- **Notification for Breaches of Online Account Data that *Does Not Involve Login Credentials* for an Email Account:** In the case of breaches involving Online Account Data and "no other personal information," businesses **may comply** with the notification obligations of the statute "**by providing the security breach notification in electronic or other form that directs the person whose personal information has been breached promptly to change his or her password and security question or answer**, as applicable, or to take other steps appropriate to protect the online account with the person or business and all other online accounts for which the person whose personal information has been breached uses the same user name or email address and password or security question or answer." [Emphasis added]
- **Notification for Breaches of Online Account Data *Involving Login Credentials* for an Email Account:** In the case of breaches involving Online Account Data that contains "login credentials of an email account furnished by the person or business," the entity that furnished the login credentials, if breached, "**shall not comply with this section by providing the security breach notification to that email address, but may, instead, comply with this section by providing notice by another method** described in [the statute for breaches of other personal information] **or by clear and conspicuous notice delivered to the resident online when the resident is connected to the online account from an Internet Protocol address or online location from which the person or business knows the resident customarily accesses the account**." [Emphasis added]

Because email notification would not be appropriate to individuals whose email account login information has been breached, the statute requires other types of notification to be used, directing businesses to use either the existing notification methods covered in Section 1798.82(j) or by providing clear and conspicuous notice delivered to an IP address or online location that the business knows the consumer often uses to access the breached account.

Other than for email login credential breaches, where notice cannot occur via email from the furnisher of the account, notice of online account or email account breaches may occur under the amended statute using all other pre-existing methods of breach notification, as the amended Section 1798.82(j) will specify: "(1) Written notice. (2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code. (3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed

two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following: (A) Email notice when the person or business has an email address for the subject persons. (B) Conspicuous posting of the notice on the Internet Web site page of the person or business, if the person or business maintains one. (C) Notification to major statewide media."

Conclusion and Outlook

The amended California breach notification statute will become effective on January 1, 2014. Businesses collecting and storing data of consumers who are California residents where the data contains user names or email addresses, along with passwords and security answers for accessing online and email accounts, should become familiar with the new law. These businesses should assess their current data security procedures and breach incident response plans in order to ensure future compliance with the amended statute in the event of a security breach incident.

Additionally, the expansion of the California breach notification law to cover user names and email addresses may have a significant influence nationwide, aiding the movement to pass similar amendments to the existing breach laws in 45 other states, as well as proposed federal breach notification legislation in Congress. The U.S. House of Representatives Committee on Energy and Commerce, for example, is considering adding provisions to upcoming breach notification bills that would require notification of breaches of consumers' online account information, including email addresses, with accompanying passwords that would permit access to their online accounts. California's passage of S.B. 46 may provide both the impetus and model for renewed action in Congress to enact a similar federal law.

Paul G. Martino | 202.239.3720 | paul.martino@alston.com
Dominique R. Shelton | 213.576.1170 | dominique.shelton@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
kacy.mccaffrey@alston.com
404.881.4824

Todd S. McClelland
todd.mcclelland@alston.com
404.881.4789

Zachary Neal
zach.neal@alston.com
404.881.4968

Bruce Sarkisian
bruce.sarksian@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

Claire L. Readhead
claire.readhead@alston.com
213.576.1181

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

Nicholas Stamos
nick.stamos@alston.com
213.576.2515

Washington, D.C.

Edward Britan
edward.britan@alston.com
202.239.3364

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

Paul G. Martino
paul.martino@alston.com
202.239.3439

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