Morrison & Foerster Client Alert

October 1, 2013

California Requires Notice for Breaches Involving User Names and Passwords

By Nathan D. Taylor

On September 27, California Governor Brown once again signed into law a bill amending the state's breach law ("S.B. 46"). This latest amendment is particularly significant because it represents the first major effort by a state to require notice to consumers of breaches involving the types of information that consumers use to access online accounts.[1] Historically, the focus of the state breach laws has been on the types of personal information that could be used to commit identity theft or fraud, such as Social Security numbers, driver's license numbers and financial account numbers. California has now tailored its law to recognize the significance and sensitivity of the information that consumers use to access their online accounts. Although it is not clear the extent to which other states may follow California's lead, S.B. 46 represents a significant progression in the evolution of state breach laws.

S.B. 46, THE CALIFORNIA BREACH AMENDMENT

S.B. 46 amends the state breach law's definition of "personal information" to cover certain types of consumer online credentialing and authentication information. Specifically, S.B. 46 provides that, effective January 1, 2014, "[a] user name or email address, in combination with a password or security question and answer that would permit access to an online account" is considered "personal information" for purposes of the state's breach law.

Unlike the other types of "personal information" covered by the California law, the combination of an individual's user name or e-mail address and password or security questions/answers is considered "personal information" even if that information does not also include and is not combined with the individual's name.

In addition, S.B. 46 does not limit the types of online accounts covered by this provision. That is, access information for all online accounts would be covered equally, regardless of the sensitivity of the underlying accounts. For example, a user name and password that would provide online access to an online banking account, e-mail account, social media account or online shopping account would

[1] As a technical matter, California is not the first state to cover at least some of this information. The Puerto Rico breach law applies with respect to an individual's name in combination with a user name and password for a private information system. Also, the North Carolina breach law applies with respect to an individual's name in combination with e-mail address, but only if the e-mail address would permit access to the individual's financial account or resources.

UNITED STATES

California

Tiffany Cheung	(415) 268-6848
Rebekah Kaufman	(415) 268-6148
Christine E. Lyon	(650) 813-5770
David F. McDowell	(213) 892-5383
James R. McGuire	(415) 268-7013
Daniel F. Muto	(858) 720-7959
Purvi G. Patel	(213) 892-5296
Andrew Serwin	(858) 720-5134
William L. Stern	(415) 268-7637
Nancy R. Thomas	(213) 892-5561
David M. Walsh	(213) 892-5262

New York

Cindy Abramson	(212) 336-4178
Melissa Crespo	(212) 336-4354
John F. Delaney	(212) 468-8040
Sherman W. Kahn	(212) 468-8023
Mark P. Ladner	(212) 468-8035
Peter McLaughlin	(212) 336-4290
Michael B. Miller	(212) 468-8009
Suhna N. Pierce	(212) 336-4150
Marian Waldmann Agarwal	(212) 336-4230
Miriam H. Wugmeister	(212) 506-7213

Washington, D.C.

Nicholas A. Datlowe	(202) 887-1590
L. Richard Fischer	(202) 887-1566
D. Reed Freeman, Jr.	(202) 887-6948
Julie O'Neill	(202) 887-8764
Obrea O. Poindexter	(202) 887-8741
Cynthia J. Rich	(202) 778-1652
Andrew M. Smith	(202) 887-1558
Nathan David Taylor	(202) 778-1644

EUROPE

Brussels

Joanna Łopatowska	32 2 340 7365
Karin Retzer	32 2 340 7364
Alja Poler De Zwart	32 2 340 7360

London

Ann Bevitt	44 20 7920 4041
Anthony Nagle	44 20 7920 4029
Caroline Stakim	44 20 7920 4055
David Varney	44 20 7920 4058

ASIA

Beijing

Gabriel Bloch	86 10 5909 3367
Jingxiao Fang	86 10 5909 3382
Paul D. McKenzie	86 10 5909 3366

Hong Kong

Gordon A. Milner	852 2585 0808

Tokyo

Daniel P. Levison	81 3 3214 6717
Gabriel E. Meister	81 3 3214 6748
Jay Ponazecki	81 3 3214 6562
Toshihiro So	81 3 3214 6568
Yukihiro Terazawa	81 3 3214 6585

each be considered "personal information" for purposes of the California law. The California legislature's approach appears to assume that user names and passwords for any type of account should be considered sensitive because many consumers use the same user name and password combination for multiple online accounts, even if that may not be appropriate.

S.B. 46, however, does provide companies with some flexibility regarding how they can provide notice to consumers of a breach involving this type of online account access information. Specifically, S.B. 46 provides that if a company experiences a breach involving online account access information and no other type of "personal information," the company may provide a notice of the breach "in electronic or other form that directs the [consumer] 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 [company] and all other online accounts for which the [consumer] uses the same" access information. However, if the compromised information provides access to an e-mail account provided by the company, the company may not provide notice to that e-mail address. Instead, the company can provide notice, for example, by mail or by providing a clear and conspicuous notice that is delivered to a consumer online when the consumer connects to her online account "from an Internet Protocol address or online location from which the [company] knows the [consumer] customarily accesses the account."

PRACTICAL IMPLICATIONS FOR BUSINESSES

In light of S.B. 46, it is important for companies to consider the potential impacts of the amendment on their business.

- Security incidents involving online account access information have begun to occur with greater frequency. Over the past several years, a number of highly public incidents have occurred involving user names and passwords regarding which businesses have provided notice to their customers. These notices, however, have been "voluntary" and not required by law. S.B. 46 changes the legal analysis, at least with respect to information relating to residents of California.

- Potentially most important among the factors that companies should consider is how they maintain, store and secure online account user names, passwords and security questions/answers. Even if a company maintains a consumer-facing website with online "accounts" that are not particularly sensitive, that company may be required to provide notice, at least to California residents, regarding breaches involving the information used by consumers to access those accounts. As a result, any company that maintains such a website should consider whether its existing security is appropriate or whether it should heighten the security for this type of information in order to avoid a potential legal obligation to notify.

While California is the most recent state to tweak the types of personal information covered under the state's breach law, it undoubtedly will not be the last. Businesses should be cognizant of the ever-changing state landscape, and, in the event of the breach, determine any applicable requirements, including whether the incident involves the types of personal information covered under the various state laws.

About Morrison & Foerster:

We are Morrison & Foerster — a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer's A-List* for 10 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Morrison & Foerster has a world-class privacy and data security practice that is cross-disciplinary and spans our global offices. With more than 60 lawyers actively counseling, litigating, and representing clients before regulators around the world on privacy and security of information issues, we have been recognized by *Chambers* and *Legal 500* as having one of the best domestic and global practices in this area.

For more information about our people and services and the resources we offer such as our treatise setting out the U.S. and international legal landscape related to workplace privacy and data security, "*Global Employee Privacy and Data Security Law,*" or our free online Privacy Library, please visit: http://www.mofo.com/privacy--data-security-services/ and "like" us on Facebook at http://www.facebook.com/MoFoPrivacy.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.