MORRISON | FOERSTER

Morrison & Foerster Client Alert.

September 1, 2011

California Expands Security Breach Notification Requirements

By Anna T. Ferrari, Nathan D. Taylor and Christine E. Lyon

A new amendment to California's security breach notification law will raise the stakes for businesses required to give notice of a data security breach affecting California residents. California Senate Bill 24 ("SB 24"), signed by Governor Brown on August 31, 2011, imposes detailed new requirements for the content of security breach notices. Significantly, SB 24 also requires notice to the California Attorney General for larger-scale security breaches.

California's security breach notification law was the first of its kind to be approved by a state legislature.[1] It requires a person or entity conducting business in California to notify California residents whose unencrypted "personal information" was (or is reasonably believed to have been) acquired by an unauthorized person through a security breach.[2] Notice may be provided in written form, electronic form, or through "substitute notice."[3] SB 24 expands both the requirements regarding content of these notices and the scope of necessary recipients.

SB 24's provisions will become effective on January 1, 2012.

[1] Cal. Civ. Code § 1798.82. A similar breach notification law applies to California state agencies. *See* Cal. Civ. Code § 1798.29.

[2] Cal. Civ. Code § 1798.82(a). Any person or entity that maintains computerized data that includes "personal information" that the person or entity does not own must notify the owner or licensee of that information about any such incident. Cal. Civ. Code § 1798.82(b). "Personal information" is defined as 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 or 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; or (5) health insurance information. Cal. Civ. Code § 1798.82(e).

[3] Cal. Civ. Code § 1798.82(j). "Electronic notice" is defined in accordance with the terms of 15 U.S.C. § 7001, which governs electronic records and signatures. Cal. Civ. Code § 1798.82(j)(2). Substitute notice involves notice by email, conspicuous posting on the person or entity's web site, and notification to major statewide media, and it is only available when the cost of providing notice would exceed $250,000 or involve an affected class of more than 500,000 persons. Cal. Civ. Code § 1798.82(j)(3).

Beijing
Jingxiao Fang 86 10 5909 3382
Paul D. McKenzie 86 10 5909 3366

Brussels
Joanna Łopatowska 32 2 340 7365
Karin Retzer 32 2 340 7364

Hong Kong
Gordon A. Milner 852 2585 0808

London
Ann Bevitt 44 20 7920 4041
Deirdre Moynihan 44 20 7920 4164
Anthony Nagle 44 20 7920 4029

Los Angeles
Michael C. Cohen (213) 892-5404
David F. McDowell (213) 892-5383
Purvi G. Patel (213) 892-5296
Russell G. Weiss (213) 892-5640

New York
Madhavi T. Batliboi (212) 336-5181
John F. Delaney (212) 468-8040
Sherman W. Kahn (212) 468-8023
Mark P. Ladner (212) 468-8035
Michael B. Miller (212) 468-8009
Suhna N. Pierce (212) 336-4150
Marian A. Waldmann (212) 336-4230
Miriam H. Wugmeister (212) 506-7213

Northern Virginia
Daniel P. Westman (703) 760-7795

Palo Alto
Anna Ferrari (650) 813-5681
Christine E. Lyon (650) 813-5770
Bryan Wilson (650) 813-5603

San Francisco
Roland E. Brandel (415) 268-7093
Jim McCabe (415) 268-7011
James R. McGuire (415) 268-7013
William L. Stern (415) 268-7637

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

Washington, D.C.
Nicholas A. Datlowe (202) 887-1590
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
Kimberly Strawbridge Robinson (202) 887-1508
Robert A. Salerno (202) 887-6930
Andrew M. Smith (202) 887-1558
Nathan David Taylor (202) 778-1644

Informational Requirements for Notices: SB 24 requires that security breach notices "be written in plain language" and contain, at a minimum, the following information:[4]

- The name and contact information of the person or business reporting the breach;
- A list of the categories of "personal information" that were, or are reasonably believed to have been, affected by the breach;
- The actual or estimated date (or range of dates) of the breach, along with the date on which notice was given;
- An indication of whether the notice was delayed as a result of a law enforcement investigation;
- A general description of the nature of the breach (if such information can be determined at the time notice is given); and
- If the breach exposed a Social Security number, driver's license number, or California identification card number, the toll-free telephone numbers and addresses of the major credit reporting agencies.

The person or entity reporting the breach may elect to provide the following additional categories of information:[5]

- Information about what the person or business has done to protect individuals whose information has been breached; and
- Advice on what steps the individual recipient of the notice may take to protect himself or herself.

Notification of California Attorney General: Under SB 24, any person or entity required to notify more than 500 California residents of a single security breach also must notify the state Attorney General.[6]

Additionally, SB 24 makes minor changes to the statute's substitute notice provisions. A person or business invoking substitute notice will be required to notify the state Office of Privacy Protection.[7]

HITECH Act Exemption: SB 24 provides that an entity covered by the federal Health Insurance Portability and Accountability Act of 1996 ("HIPAA") that has complied with the breach notification provisions of the federal Health Information Technology for Economic and Clinical Health ("HITECH") Act will be deemed to have complied with the new content requirements for security breach notices under California's security breach notification law as well.[8]

Currently, 45 other states, as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, also have enacted security breach notification laws. Although these state security breach notification laws are understood to be modeled upon the California law, many states have developed more detailed notification requirements. With the passage of SB 24, California joins at least 17 states and U.S. territories in (1) regulating the specific content of

[4] Cal. Civ. Code § 1798.82(d)(1), (2).

[5] Cal. Civ. Code § 1798.82(d)(3); Cal. Civ. Code § 1798.29(d)(3).

[6] Cal. Civ. Code § 1798.82(f); Cal. Civ. Code § 1798.29(e).

[7] Cal. Civ. Code § 1798.82(j)(3)(C). SB 24 makes a similar amendment to Civil Code section 1789.29. State agencies invoking substitute notice will be required to notify the state Office of Information Security. Cal. Civ. Code § 1798.29(i)(3)(C).

[8] Cal. Civ. Code § 1798.82(e).

security breach notices to include certain types of information for consumers,[9] and (2) requiring an entity that suffers a security breach to notify a state regulator, such as the Attorney General, in addition to the affected individuals.[10] Before the passage of SB 24, the bill's sponsor, Senator Joe Simitian, had introduced equivalent legislation in 2008, 2009, and 2010. Each time, the legislature approved the measure, but former Governor Arnold Schwarzenegger vetoed it.

Additional information, including links to federal and state breach notification laws, may be found in Morrison & Foerster's free online privacy library, www.mofoprivacy.com.

About Morrison & Foerster:

We are Morrison & Foerster—a global firm of exceptional credentials in many areas. 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 seven 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.

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.

[9] These states include Hawaii, Illinois, Iowa, Maryland, Massachusetts, Michigan, Missouri, New Hampshire, New York, North Carolina, Oregon, Vermont, Virginia, West Virginia, Wisconsin, and Wyoming.

[10] These states include Alaska, Hawaii, Idaho, Indiana, Louisiana, Maine, Maryland, Massachusetts, Missouri, New Hampshire, New Jersey, New York, North Carolina, South Carolina, Vermont, and Virginia.