MORRISON | FOERSTER

Morrison & Foerster Client Alert.

February 6, 2012

The Massachusetts Service Provider Contract Safe Harbor Set to Expire

By Nathan D. Taylor and Miriam H. Wugmeister

The Massachusetts data security regulations' "safe harbor" for certain pre-existing service provider contracts will expire on March 1, 2012. Companies should ensure that they have updated agreements with service providers, if necessary, by that date.

As we have previously reported over the past several years, the Massachusetts data security regulations, originally issued in September 2008 by the Massachusetts Office of Consumer Affairs and Business Regulation, impose far more detailed and comprehensive data security requirements than other U.S. states and most other countries. While the compliance date for the regulations (March 1, 2010) is nearly two years past, the safe harbor in the regulations relating to pre-existing service provider contracts is set to expire on March 1, 2012.

The Massachusetts data security regulations apply to any person that "own[s] or license[s]" personal information[1] about Massachusetts residents. 201 C.M.R. § 17.01(2). Despite its seemingly narrow ownership language, the regulations define this phrase broadly to include the acts of receiving, maintaining, processing, or otherwise having access to personal information in connection with providing goods or services or in connection with employment. 201 C.M.R. § 17.02. As a result, the regulations apply broadly to any person (or business) that receives, maintains, processes or otherwise has access to personal information relating to a resident of Massachusetts in connection with providing goods or services or in connection with employment.

[1] For purposes of the regulations, the term "personal information" is defined as an individual's first name or initial, and last name, in combination with any one of the following data elements: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) financial account, credit card number, or debit card number, with or without any required security code or password that would permit access to the account.

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
Matthew R. Galeotti (212) 336-4044
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

The regulations impose a number of significant administrative responsibilities on covered individuals or businesses, including requirements to maintain a comprehensive, written information security program and to educate and train employees regarding personal information security. (See here.) Beyond its general, risk-based information security program requirement and related administrative requirements, the Massachusetts data security regulations also require that a covered business implement a number of detailed and specific technical security controls, including, for example, encryption and password requirements.

Notable among the regulations' administrative requirements is service provider oversight. In this regard, the regulations require that a covered business take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the regulations and any applicable federal regulations. 201 C.M.R. § 17.03(f)(1). Further, the regulations require that a covered business require a third-party service provider *by contract* to implement and maintain "such appropriate security measures." 201 C.M.R. § 17.03(f)(2). Up until now, the regulations have included a safe harbor for certain pre-existing service provider contracts. Specifically, the regulations provide that until March 1, 2012, a contract into which a covered business had entered with a third-party service provider to perform services on behalf of the business satisfied the regulations' contract requirement so long as the contract was entered into before March 1, 2010.

California Breach Notification

Today, 46 states in the U.S., as well as the District of Columbia, Puerto Rico, and the U.S. Virgin Islands, require notice to individuals of certain security incidents. In addition, 15 states require notice to a state authority, such as the state Attorney General, when a business is required to provide security breach notices to individuals. While notice to state authorities is not a new requirement, a trend that may be developing is state-specific forms for submitting notice to state authorities. In response to the recent amendment of the California breach law to, among other things, require electronic notice to the California AG of breaches involving 500 or more California residents, the California AG has made available an online form for submitting notice to the AG when required. As a result, California now joins New York and North Carolina as states with special forms for submission of notice to state authorities. The California form can be found at https://oag.ca.gov/ecrime/databreach/report-a-breach.

As a result, the regulations have specifically exempted service provider contracts entered into before the regulations' compliance date of March 1, 2010 and gave businesses two years to ensure that all old contracts were updated to comply with the regulations. That two-year safe harbor is quickly ending. As of March 1, 2012, the safe harbor will expire, and all service provider relationships otherwise subject to the regulations' service provider oversight requirement will be subject to the contract requirement.

PRACTICAL IMPLICATIONS FOR BUSINESSES

There are some practical implications that businesses should consider as the expiration of the service provider contract safe harbor draws near.

- Covered businesses have been subject to the regulations' contract requirement for almost two years now with respect to any service provider contracts entered into on or after March 1, 2010. As a result, many businesses have already revised their contractual provisions for service providers to demonstrate compliance with the regulations' contract requirement. In this regard, the plainest reading of the requirement is that a contract with a service provider must include security measures that would be "consistent with" the Massachusetts regulations and any federal regulations that apply to the business. While seemingly innocuous, it can be difficult to draw the line or otherwise determine how many and which types of information security provisions are sufficient to meet the regulation's contract requirement.

- For any covered business that has already considered and/or revised its standard service provider contractual provisions to address the regulations' contract requirement, it is nonetheless important to review contracts entered into before March 1, 2010 to determine whether the regulations apply with respect to those contracts and, if so, whether those contracts include compliant information security provisions or need to be updated.
- Finally, it is always important to keep in mind that the Massachusetts AG takes the information security obligations imposed by the regulations seriously and appears intent on actively enforcing such regulations. (See here).

As we have previously indicated, businesses that have not taken steps to address compliance with the Massachusetts data security regulations should quickly begin to take such steps. Those businesses that have previously addressed their compliance with the regulations may wish to consider revisiting their compliance programs to ensure they comply with the detailed regulations. Nonetheless, while the Massachusetts data security regulations may be the most detailed state information security requirements, they are certainly not the only state requirement relating to the security of personal information, and they will not be the last.

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 eight 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 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.