MORRISON | FOERSTER

Client Alert.

February 2010

Compliance Date for Massachusetts Data Security Regulations Rapidly Approaching: Are You Ready to Comply?

By Miriam H. Wugmeister and Nathan D. Taylor

Many U.S. state laws require that businesses adopt reasonable measures to protect personal information and/or dispose of personal information in an appropriate manner. The data security regulations issued by the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR"), however, impose far more detailed and comprehensive data security requirements than most, if not all, other states. With the compliance date for the Massachusetts data security regulations—**March 1, 2010**—only two weeks away, organizations would be well advised to take a fresh look at their policies and procedures.

The regulations were originally issued in September 2008, with an initial compliance date of January 1, 2009. OCABR, however, amended the regulations several times. In amending the regulations, OCABR not only made substantive changes, but also extended the compliance date several times. All indications are that OCABR will not extend the compliance date again and that compliance with the regulations will be required on March 1, 2010.

While the regulations (and the previous revisions to the regulations) are described at greater length in earlier Morrison & Foerster Legal Updates ("New Massachusetts Regulation Requires Encryption of Portable Devices and Comprehensive Data Security Programs," "Massachusetts Delays Effective Date of New Data Security Regulations," "Massachusetts Amends Burdensome Service Provider Oversight Requirements of New Data Security Regulations and Delays Compliance Date Again," and "Massachusetts Amends Its Data Security Regulations Again: Burdensome Service Provider Oversight Requirements are Back"), the following provides a brief overview of certain important requirements of the regulations.

The Massachusetts data security regulations apply to any person that receives, maintains, processes, or otherwise has access to "personal information" relating to a resident of Massachusetts in connection with the provision of goods or services, or in connection with employment. 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, or debit card number, with or without any required security code or password that would permit access to the account.

The Massachusetts data security regulations impose a number of significant administrative responsibilities on covered businesses. For example, a covered business must:

- develop, implement, maintain, and monitor a comprehensive, written information security program that contains administrative, technical, and physical safeguards to ensure the security and confidentiality of records containing personal information;
- conduct a risk assessment to identify and assess reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of electronic, paper, and other records containing personal information and evaluate and improve, where necessary, the effectiveness of its safeguards for limiting those internal and external risks;

- designate one or more employees to maintain the information security program;
- regularly monitor to ensure that the information security program is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of, personal information;
- 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, including requiring service providers by contract to implement and maintain such security measures (there is a limited safe harbor for the contract requirement until March 1, 2012); and
- educate and train employees regarding personal information security.

Beyond its general, risk-based information security program requirement and related administrative requirements, the Massachusetts data security regulations also require that a business implement a number of detailed and specific technical security controls. Among other things, the regulations require that an organization must:

- implement reasonable restrictions on physical access to records containing personal information and storage of such records in locked facilities, storage areas, or containers;
- implement secure user authentication protocols and access control measures for computer systems;
- encrypt all transmitted records and files containing personal information that will travel across public networks and that will be transmitted wirelessly;
- encrypt all personal information stored on laptops and other portable devices; and
- maintain firewall protections, operating system security patches, and malware and virus protection.

In light of the complexity and specificity of the regulations as a whole, as well as the fast-approaching compliance date, compliance efforts should remain a high priority for businesses that handle personal information relating to Massachusetts residents. Businesses that have not taken steps to address compliance with the Massachusetts data security regulations should quickly begin to take such steps. For those businesses that have taken steps to address their compliance with the regulations, consider revisiting the compliance program to ensure it complies with the detailed regulations set to take effect at the beginning of next month. Massachusetts law may be the most detailed, but it is certainly not the only state regulation relating to the security of personal information, and it will not be the last.

Morrison & Foerster has a world-class privacy and information 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, and subscription service Summit, please visit: http://www.mofo.com/privacy--data-security-services

Client Alert.

Contact:

Miriam H. Wugmeister
212) 506-7213
mwugmeister@mofo.com

Nathan D. Taylor
(202) 778-1644
ndtaylor@mofo.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, Fortune 100 companies, investment banks and technology and life science companies. Our clients count on us for innovative and business-minded solutions. Our commitment to serving client needs has resulted in enduring relationships and a record of high achievement. For the last six years, we've been included on *The American Lawyer*'s A-List. *Fortune* named us one of the "100 Best Companies to Work For." We are among the leaders in the profession for our longstanding commitment to pro bono work. Our lawyers share a commitment to achieving results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.