MORRISON | FOERSTER

Legal Updates & News

Legal Updates

Massachusetts Amends Its Data Security Regulations Again: Burdensome Service Provider Oversight Requirements are Back

August 2009
by Miriam Wugmeister, Nathan D. Taylor

Related Practices:

- Privacy and Data Security

In an announcement released on Monday, August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") amended its data security regulations for the third time. OCABR's press release, and much of the press coverage,gives the impression that the amendments were limited in scope to an extended compliance date and a risk-based standard to alleviate the burden on small businesses. While the amended regulations include these changes, the regulations also include a number of additional substantive modifications that will have an impact on businesses that have been preparing to comply or are considering what steps to take to comply with the regulations. 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", and "Massachusetts Amends Burdensome Service Provider Oversight Requirements of New Data Security Regulations and Delays Compliance Date Again").

Scope

The amended regulations at first glance appear to narrow the scope of the persons to whom the regulations apply, but may in fact do just the opposite. Specifically, the amended regulations apply to any person that "owns or licenses" personal information, while the previous regulations applied to any person that "owns, licenses, stores or maintains" personal information. The amended regulations, however, define the phrase "owns or licenses" as receiving, maintaining, processing or otherwise having access to

personal information in connection with the provision of goods or services or in connection with employment. As a result, a business that would not have been covered under the previous regulations because it did not own, license, store or maintain personal information may be subject to the amended regulations if it processes or merely has access to such information.

Service Provider Oversight

In addition, the amended regulations have reintroduced the obligation that a business enter into contracts with its service providers to require the service providers to implement and maintain security measures that are consistent with the Massachusetts regulations and, in a new addition, any applicable federal regulation. Over the course of OCABR's various amendments to the regulations, we have gone from a service provider due diligence and contract requirement, to a due diligence and oversight requirement and now back to a due diligence and a contract requirement. This time, however, the due diligence and contract requirement extends to any applicable federal regulation. By extending these requirements to any applicable federal regulation, the amended regulations have greatly expanded the scope of the required service provider oversight because it covers Massachusetts law and any other federal regulation. This is substantially broader than the initial regulations.

The amended regulations include a safe harbor provision for certain contracts. Specifically, the amended regulations provide that any contract entered into with a service provider "prior to March 1, 2012" will be deemed in compliance with the regulation's contract requirement, even if the contract does not include a provision requiring compliance with the regulations or applicable federal regulation, "so long as the contract was entered into before March 1, 2010. The intent of this provision is not clear. On the one hand, the provision may have been intended to grandfather all service provider contracts that are entered into before the regulations become effective—this interpretation is plausible if it is assumed that the reference to March 1, 2012 was a drafting error. On the other hand, the provision may be intended to provide more limited relief and grandfather service provider contracts that are entered into before the regulations become effective, but only for a two-year period, and after 2012 all contracts must be updated to comply with the regulations. The meaning of this provision is not clear.

It is also worth noting that the amended regulations add a definition for the term "service provider." The definition would indicate that a service provider would likely be independently covered by the regulations because it receives, maintains, processes or is otherwise given access to personal information and thereby appears duplicative

Removal of Substantive Obligations

In response to significant comments and concerns raised by industry regarding the burden imposed by the regulations, OCABR has removed several substantive obligations that were previously included in the regulations. Specifically, the amended regulations no longer include the following substantive obligations: (1) the obligations to limit the amount of personal information that is collected, to limit the time period that personal information is retained and to limit access to personal information to those persons who are required to know such information; (2) the obligation to identify records that contain personal information; and (3) the obligation to implement a written procedure for how physical access to records containing personal information is restricted. While these may be best practices and potentially required by other laws, such as laws outside of the United

States, the removal of these substantive obligations will significantly reduce the compliance burden for businesses.

Effective Date

The amended regulations extend the mandatory compliance date to March 1, 2010. The previous effective date was January 1, 2010. As a result, OCABR has provided companies with an additional two months in which to come into compliance with the regulations.

Risk-Based Implementation

In addition, the amended regulations require that a business implement its security program in a risk-based fashion, taking into account, for example, the size of the business and the amount of data that it stores. The previous regulations had included the same risk-based language but it was for enforcement purposes to determine if an information security program was in compliance with the regulations and was not an actual requirement that businesses must take into account in developing their programs. OCABR indicated in its press release that this modification was intended to alleviate some of the compliance burden felt by small businesses.

Conclusion

The removal of certain substantive obligations from the regulations will alleviate some compliance burden for businesses. In addition, the extension of the compliance date is welcome, although not overly generous. The return of the service provider contract requirement, however, may impose a significant burden on companies, although the grandfathering provision may, at least temporarily, allow businesses to focus on ensuring that all new service provider contracts have appropriate language. Nonetheless, in light of the complexity and specificity of the regulations as a whole, as well as the frequent modifications that OCABR has made to the regulations, compliance efforts should remain a high priority for businesses that maintain personal information relating to Massachusetts residents.
