MORRISON | FOERSTER

Legal Updates & News

Bulletins

Massachusetts Amends Burdensome Service Provider Oversight Requirements of New Data Security Regulations and Delays Compliance Date Again

February 2009
by Nathan D. Taylor, Miriam Wugmeister

Related Practices:

- Financial Services Law
- Privacy and Data Security

Privacy and Data Security Update, February 12, 2009

In an announcement released late on Thursday, February 12, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") revised its new data security regulations for the second time. This development is a welcome change and will alleviate some of the obligations imposed by the regulations. The regulations (and the initial 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' and 'Massachusetts Delays Effective Date of New Data Security Regulation').

Service Provider Oversight

The announcement by the OCABR significantly modified the service provider oversight requirements of the regulations, which were among the most burdensome obligations of the initial regulations. Specifically, companies would have been required to take reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such personal information, including: (1) selecting and retaining service providers that are capable of maintaining safeguards for personal information; and (2) contractually requiring service providers to maintain such safeguards. Also, before granting a third-party service provider access to personal information, a company would have been required to "obtain from the third-party service provider a written certification that such service provider has a written, comprehensive information security program that is in compliance with the provisions of these regulations."
In a significant and positive change, the revised regulations remove the express contractual requirement and written certification requirement. Instead, the revised regulations provide that a company subject to the regulations must take all reasonable steps to: (1) verify that service providers with access to personal information are capable of maintaining safeguards for personal information in the manner provided in the regulations; and (2) ensure that the service provider's safeguards are 'at least as stringent' as those required under the regulations.

Effective Date

In addition, the revised regulations extended the general deadline for all requirements of the regulations to January 1, 2010. The previous general effective date was May 1, 2009. As a result, OCABR has provided companies with an additional eight months in which to come into compliance with the new regulations.

Conclusion

The simplification of the vendor oversight requirements likely will remove significant compliance burdens for businesses. In addition, the extension of the compliance date is a welcome development, especially in the uncertain economic environment facing U.S. businesses. Nonetheless, in light of the complexity and specificity of the regulations as a whole, compliance efforts should remain a high priority at companies that maintain personal information of Massachusetts residents.