

Privacy and Security Alert: Office of Consumer Affairs and Business Regulation Faces Growing Criticism Over Data Security Regulations' Content and Implementation Date

1/30/2009

As discussed in earlier alerts (January 22, 2008, October 2, 2008, and October 31, 2008), starting May 1, 2009, businesses will be held to a higher standard regarding the protection of Massachusetts residents' personal information and will now be required to implement written programs for the protection of personal information.

Recent Commentary from the Attorney General

In remarks to the Greater Boston Chamber of Commerce on Tuesday, January 27, 2009, Massachusetts Attorney General Martha Coakley voiced her concern over the Commonwealth's pending Data Security Regulations (201 C.M.R. 17.00) (the "Regulations"). Acknowledging recent criticisms brought forth by the business community, Coakley pledged that her agency will examine the Regulations' "practicality." She later told reporters, "We have some concerns and we always want to make sure, as the enforcing agency, that [the Regulations] will be fair and they will be doable."

Coakley's remarks came in the wake of a contentious public hearing held by the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR). The bitter cold and approaching holiday weekend did not prevent more than 300 interested parties from cramming into a hearing room at the Massachusetts Transportation Building on Friday, January 16, 2009. The hearing's purpose was to elicit public commentary on the Regulations' implementation date. Speakers not only opposed the various implementation dates, but also took the opportunity to attack the Regulations' substance.

Who Is Voicing Displeasure?

Representatives from the financial and insurance industries, small businesses, retailers, colleges and universities, and legal professionals have all taken issue with the Regulations. Most are concerned with ambiguous language and onerous compliance requirements. Virtually all who opposed the Regulations have requested both a delay in their implementation and a reworking of their substantive language.

Specific Concerns

Meeting attendees voiced the following concerns:

The Regulations' third-party service-provider certification and contractual requirements were too onerous and were unfair to small businesses.

The Regulations' encryption requirements are cost-prohibitive. If this provision remains, it should only apply on a "going forward" basis, rather than a retroactive basis.

Terms and conditions are vague. For instance, the terms "other portable devices" and "third-party service provider" are never defined.

The Regulations exceed the scope of the Commonwealth's authority by extending beyond state borders to entities with no ties to the Commonwealth other than personal information on its residents.

The Commonwealth and OCABR have not sufficiently communicated the existence of the new Data Security Law and Regulations to the business community as a whole.

The fact that state agencies are exempt from the Regulations is inequitable.

What Can Be Done to Improve the Regulations?

Along with delaying the effective date, some have suggested that OCABR seek the advice of an advisory committee comprised of business and technology professionals to amend vague language and lessen onerous provisions. Others have suggested that major portions of the Regulations be eliminated entirely. Still others have recommended more specific language and differing levels of requirement, depending on the size of the business.

Many detractors point to New Jersey's recent experience for instruction, where the state spent more than two years refining the language of its data security law. Along the way, authorities solicited advice from potentially covered entities. After much revision, the state eventually retracted one version and published draft regulations in December 2008 that appear to be more acceptable to all sides. Some of the individuals who provided testimony stated that they would like to see a similar scenario play out in Massachusetts.

How Do the Recent Developments Affect Your Organization?

To date, OCABR has not amended either the effective date or the substance of the Regulations. Many portions are set to take effect May 1, 2009. As such, covered entities should go forward with plans to comply. For a detailed description of compliance standards, see our previous alerts (January 22, 2008, October 2, 2008, and October 31, 2008).

In the meantime, companies should monitor any developments from both OCABR and the Massachusetts Attorney General. Mintz Levin's Data Security Group can also serve as a resource. Our attorneys have extensive experience in assisting clients with regulatory compliance in volatile environments. Should you have any questions, feel free to contact us.

Endnotes

¹ Appreciation to law clerk Peter Mee for work on this alert.

For assistance in this area, please contact one of the attorneys listed below or any member of your Mintz Levin client service team.

Cynthia Larose, CIPP
(617) 348-1732
CLarose@mintz.com

Elissa Flynn-Poppey
(617) 348-1868
EFlynn-Poppey@mintz.com

Julia M. Siripurapu
(617) 348-3039
JSiripurapu@mintz.com

© 1994-2009 Mintz, Levin, Cohn, Ferris, Glovsky and Popeo P.C. All Rights Reserved.

This website may constitute attorney advertising. Prior results do not guarantee a similar outcome. Any correspondence with this website does not constitute a client/attorney relationship. Neither the content on this web site nor transmissions between you and Mintz Levin Cohn Ferris Glovsky and Popeo PC through this web site are intended to provide legal or other advice or to create an attorney-client relationship. Images or photography appearing on this website may not be actual attorneys or images associated with Mintz Levin.