Document hosted at JDSUPRA
http://www.jdsupra.com/post/documentViewer.aspx?fid=a4811a0e-1b0f-44e1-adef-0f4f87a722a0

MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

Privacy and Security Alert: Massachusetts New Data Security Regulations Effective January 1, 2009

10/2/2008

On September 22, 2008, the Office of Consumer Affairs and Business Regulation of the Commonwealth of Massachusetts promulgated final regulations regarding the standards to be met by persons or businesses who own, license, store, or maintain personal information about a resident of the Commonwealth. As we reported in our Privacy and Security Alert regarding the Massachusetts Data Breach Notification law, the penalties for noncompliance can be hefty.

The proposed regulations were the subject of a public hearing on January 11, 2008 and were heavily commented upon as being too burdensome and specific. The final regulations address many of the concerns of the commentators and differ from the proposed regulations in the following principal ways:

- The definition of "Encrypted" in § 17.02 has been revised to remove the minimum 128-bit-encryption-or-higher requirement and to generally make the definition more flexible and consistent with that found in most other state data breach notification statutes and regulations.
- The very specific and stringent standards for safeguarding personal information in § 17.03 and the computer system security requirements in § 17.04 previously imposed upon persons and businesses were reduced to a "reasonable" standard for the most part, making the requirements consistent with those of the Federal Trade Commission Safeguards Rule[1] for the protection of customer financial information.
- The requirements in §17.03(b) to upgrade information systems (including network, system, and software design, as well as information processing, storage, and transmission) and store records and data in locked facilities, storage areas, or containers, were deleted.
- The requirement in § 17.03(c) to develop security policies specifically for employees who telecommute was removed and replaced with a requirement that employers develop security policies that "take into account whether and how employees should be allowed to keep, access and transport records containing personal information outside of business premises."
- The requirement in § 17.04(1)(ii) of a seven-character password was removed and replaced with "a reasonably secure method of assigning and selecting passwords or use of unique identifier technologies, such as biometrics or token devices."
- The requirement in §17.04 to periodically review audit trails restricted to those with a job-related need to view audit trails was deleted.
- The requirements in §17.04 to restrict physical access to computerized records containing personal information, to develop a written procedure that sets forth the manner in which physical access to personal information is restricted, and to review the integrity of the computerized records when notified of any unauthorized entry into a secure area by either an employee or any other unauthorized person were deleted.

The full text of the regulations can be found here. Any company with personal information of Massachusetts residents should be aware of and become familiar with the provisions of the regulations in order to prepare for complying with the requirements before the effective date of January 1, 2009.

Endnotes

[1] Standards for Insuring the Security, Confidentiality, Integrity and Protection of Customer Records and Information, 16 C.F.R. Part 314.

For assistance in this area, please contact:

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

or any member of your Mintz Levin client service team.

© 1994-2008 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.