MINTZ LEVIN
Mintz Levin Cohn Ferris Glovsky and Popeo PC

# Privacy and Security Alert: Massachusetts Extends Deadline for Compliance with Data Security Regulations to January 1, 2010

2/18/2009

On February 12, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) amended the Commonwealth's Data Security Regulations (201 C.M.R. 17.00) (the "Regulations"). The Regulations mandate that any entity that stores personal information (a combination of name and Social Security number, bank account number, or credit card number) of Massachusetts residents must encrypt the information when the information is stored on portable devices, or transmitted wirelessly or on public networks. For a detailed description of compliance standards, see our previous alerts (January 22, 2008, October 2, 2008, October 31, 2008, and January 30, 2009).

The amendments to the Regulations come following widespread criticism of the Regulations' implementation schedule and substantive language. In particular, critics alleged that complying with the Regulations by May 1, 2009 (the compliance deadline prior to the recent amendments) would impose a heavy financial burden on covered entities, and implementation was not feasible for many businesses.

Critics also focused on the Regulations' requirements regarding third-party service providers. Prior to the recent amendments, the Regulations required covered entities to amend their contracts with service providers to include language stating that the service providers maintained safeguards for personal information in contracts with third-party service providers. The Regulations also required covered entities to obtain written certification from third-party service providers that the service providers have a written, comprehensive information security program that complies with the Regulations. Also, covered entities were required to obtain these contract provisions and certifications prior to any access to Massachusetts residents' personal information by the service provider.

The recent amendments to the Regulations address both of these issues. Specifically, the amendments consist of the following changes:

- The general compliance deadline is now January 1, 2010 (rather than May 1, 2009). The deadline for encrypting personal information on all portable devices, including laptops, is also January 1, 2010 (rather than May 1, 2009, for laptops).
- Covered entities must take "all reasonable steps" to verify that third-party service providers with access to personal information have "the capacity to protect such information." The Regulations no longer require covered entities to obtain written certification from third-party service providers, or to contractually require service providers to maintain safeguards for personal information, but the amendments do require that covered entities "ensure" that service providers apply "at least as stringent" controls as those in 201 CMR 17.00 to the personal information of Massachusetts residents.

The amended Regulations do *not* change the requirement that covered entities have a written comprehensive information security plan, nor do the amendments change the Computer System Security Requirements.

The full text of the amended Regulations can be found here. Any company with personal information of Massachusetts residents should become familiar with the Regulations' provisions in order to comply with the requirements prior to the effective date of January 1, 2010. Mintz Levin's Data Security Group can 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.

---

*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