Client Advisory

KELLEY DRYE

PRIVACY AND INFORMATION SECURITY PRACTICE GROUP FEBRUARY 17, 2009

Massachusetts (Again) Revises the State's Data Security Regulation; Compliance with Entire Regulation Extended Until Jan. 2010

On Thursday, February 12, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation ("OCABR") announced that it revised, for a second time, the state's data security regulation (the "Regulation") that requires businesses that handle certain sensitive "Personal Information" of Massachusetts residents to develop and implement a comprehensive, written information security program. These revisions provide some relief for businesses required to comply with the rigorous provisions of the Regulation.

SERVICE PROVIDER REQUIREMENTS

Specifically, the modifications remove:

1. The provision that businesses ***contractually*** require third-party service providers that handle consumers' "Personal Information" be capable of maintaining the safeguards necessary for the protection of that "Personal Information"; and
2. The requirement that businesses obtain express written certification stating that the third-party service provider has a written, comprehensive security program that complies with the Regulation.

Although the OCABR has removed these two express requirements, businesses are still required under the Regulation to take all reasonable steps to:

1. Verify that the third-party service provider has the capacity to protect consumers' personal information in the manner provided for in the Regulation; and
2. Ensure that the third-party service provider has implemented security measures at least as stringent as those required under the Regulation.

The modifications to the Regulation simply grant greater flexibility to businesses in how they accomplish these objectives.

Despite these changes, many businesses remain subject to other states' laws (as well as Section 5 of the FTC Act), which either expressly state, or have been interpreted, to require clear privacy and security contract terms with third party service providers that handle personal information on the company's behalf.

COMPLIANCE DEADLINE

In addition to the above-referenced revisions, the OCABR has extended the deadline for compliance with *all* provisions of the Regulation from May 1, 2009 to January 1, 2010. (Previously, this extension had applied only to mobile device encryption and vendor certification.)

KELLEY DRYE & WARREN LLP

Kelley Drye & Warren's Privacy and Information Security Practice is a leader in advising clients on privacy and information security issues and has been at the forefront of developments in this growing area of

the law. Our attorneys regularly counsel clients regarding all aspects of privacy and data security compliance, including drafting and amending privacy and information security policies, advising clients on interpreting their own policies, crafting data security programs for clients, performing privacy and/or data security audits of existing business practices, drafting agreements with third parties regarding their obligations in connection with handling clients' customer data, and representing clients in connection with federal and state regulator privacy investigations regarding their privacy and data security practices.

For more information about this Client Advisory, please contact:

D. REED FREEMAN
(202) 342-8880
rfreeman@kelleydrye.com

ALYSA Z. HUTNIK
(202) 342-8603
ahutnik@kelleydrye.com