Client Advisory

KELLEY DRYE

PRIVACY & INFORMATION SECURITY PRACTICE GROUP NOVEMBER 18, 2008

Extension Provided For Compliance With New Massachusetts Data Security Regulation – Tiered Compliance Dates Now In Effect

The Massachusetts Office of Consumer Affairs and Business Regulation (the "Office") has extended the deadline for compliance with the state's new data security regulation (the "Regulation") requiring businesses that handle certain sensitive "Personal Information" of Massachusetts residents to develop and implement a comprehensive, written information security program, and to encrypt such information. The Office, concerned that the original January 1, 2009 deadline could be economically burdensome to small businesses, has created tiered deadlines for compliance, as discussed below.[1]

Extension to May 1, 2009 – Applies To All requirements *Except* For Contractor Certification and General Mobile Device Encryption

The Office extended the compliance deadline for the Regulation from January 1, 2009 to May 1, 2009 for all aspects of the Regulation, *except for an additional extension (as discussed below) for third party contractor certification and general mobile device encryption compliance dates*.

Specifically, by **May 1, 2009**, businesses will need to ensure the following requirements are satisfied:

- Business must have in place a comprehensive, written information security program that reasonably protects "Personal Information" maintained by the business.[2] A full discussion of the controls that must be implemented in the mandated security program are addressed in Kelley Drye's previous client advisory, which is available here.
- Businesses must ensure that all third-party contractors that handle Personal Information on the business's behalf are capable of protecting the Personal Information, and that the business has contractual terms in place with the contractors requiring such protection.
- All Personal Information stored on a laptop must be encrypted.

Extension to January 1, 2010 – Applies Only To Contractor Certification and General Mobile Device Encryption Compliance Date

The Office further extended the compliance deadline to **January 1, 2010** on the following two Regulation requirements:

- Businesses must obtain written certifications from third-party contractors that handle Personal Information on the business's behalf that the provider has a written, comprehensive information security program that is in compliance with the provisions of the Regulation.

---

[1] A copy of the Office's Press Release is available here.

[2] "Personal Information" is defined as a person's first and last name or first initial and last name in combination with one or more of the following elements: Social Security number, driver's license or state identification card number, financial account number, credit card number, or debit card number (and excluding publicly available information).

- Businesses must ensure that Personal Information contained on **all** portable devices, including PDAs, memory sticks, etc., is encrypted.

PENALTIES

Violations of the Regulation are subject to enforcement under the Massachusetts Unfair Competition Statute.[3] The Massachusetts attorney general may seek a temporary restraining order or a preliminary or permanent injunction against a business that it believes is in violation of the Regulation. If found to be in violation of the law, a court may require that the business pay a civil penalty of up to $5,000 per violation, as well as the costs of the investigation and attorneys' fees. It remains to be seen what counts as a single violation under the Regulation, but it is likely the enforcers will assert that each aspect of non-compliance with the Regulation, and/or each day of non-compliance, should be considered a separate violation.

CIVIL REMEDIES

Businesses also face the potential of a private action for noncompliance with the Regulation. Massachusetts residents potentially can bring a claim for unfair or deceptive practices under Chapter 93A of the Massachusetts Laws, or a negligence claim using the Regulation (or the statute under which it was issued) to prove that the business had a duty that was breached. Under Massachusetts law, a violation of a statute may constitute per se negligence. If such a case is successfully brought, the exposure is the amount of actual damages or twenty-five dollars, whichever is greater. Additionally, if the court finds that the practice was a willful or knowing violation, the court may order treble damages.

KELLEY DRYE & WARREN

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) 342-8603
rfreeman@kelleydrye.com

ALYSA Z. HUTNIK
(202) 342-8880
ahutnik@kelleydrye.com