

Comprehensive New Massachusetts Data Security Regulation Going Into Effect on March 1, 2010 Will Affect Many National Businesses

February 9, 2010

The long-awaited and long-delayed Massachusetts regulation setting heightened standards for corporate data security will finally take effect on **March 1, 2010**. The regulation, "Standards for the Protection of Personal Information of Residents of the Commonwealth,"¹ (the "Regulation") applies to all businesses (i.e., not only businesses based in Massachusetts) that collect and retain "personal information"² of Massachusetts residents in connection with the provision of goods and services or for the purposes of employment. The requirements of the Regulation for safeguarding the security of computerized and non-computerized personal information, although designed to be flexible in their application, are the most thorough and detailed state regulations of this type in the nation to date. Initial enforcement measures, and litigation challenging the Regulation, may follow in the coming year.

Core Requirements of the Modified Massachusetts Regulation

In the face of numerous complaints from the business and technology community following the initial publication of the Regulation, the Massachusetts Office of Consumer Affairs and Business Regulation (the "OCA") conducted public hearings, delayed the initial enforcement date of the Regulation and partially rewrote the Regulation during 2009. The net effect of the revisions was to eliminate some of the more onerous requirements in the original Regulation, such as requiring businesses to prepare inventories of all paper and electronic records, and to make the Regulation's requirements for minimum computer security measures more flexible and "technology neutral."

Notwithstanding these changes, the Regulation retains most of its original core terms regarding standards and practices for protecting the security of personal information, including the requirement to create a

¹ 201 CMR 17.00

² Under the Regulation, "personal information" includes a Massachusetts resident's first name and last name (or first initial and last name) when in combination with one or more of the following data elements relating to that resident: Social Security number, driver's license or state-issued identification card number, financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password that would permit access to a resident's financial account. The definition excludes information lawfully obtained from publicly available sources or from generally available federal, state or local governmental records.

comprehensive, written information security program. Such required information security programs must address, at a minimum, the following measures:

- the appointment of specific employees to maintain the program;
- periodic risk assessments, monitoring of the security program and training of employees;
- means for detecting and preventing security system failures;
- specific security practices directed to storage and transportation of personal information records outside of business premises (e.g., transport of back-up tapes to offsite storage locations);
- preventing terminated employees from accessing records containing personal information;
- oversight of third party service providers (e.g., outsourcers) who have access to personal information maintained by the business and obtaining written covenants of compliant practices by third-party service providers (subject to a two-year grace period for service contracts entered into before March 1, 2010);
- annual reviews of the security program; and
- procedures for documenting incidents involving a breach of security.

Businesses that are already subject to extensive privacy and data security regulation, such as banks and other financial services companies, will find nothing dramatically new in the types of process requirements stated above.³ But the Regulation's broad reach will pull in many national businesses that, until now, have not had to comply with a detailed law or regulation specifying minimum information security requirements.

Requirements Specific to Computer Security Systems

In addition to the foregoing, the Regulation's controversial specification of minimum "computer system security requirements" exceeds in detail all current state and most existing federal regulatory requirements for private sector entities. The mandated elements of computer system security under the Regulation include implementation of:

- secure user authentication protocols (e.g., secure user IDs, secure methods of assigning and selecting passwords and other identifier technologies);

³ However, official guidance issued by the Commonwealth states that businesses subject to information security requirements under the Health Insurance Portability and Accountability Act ("HIPAA") will also be required to comply with the new Regulation and are not exempt. <http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf>

- secure access control measures (e.g., procedures to restrict access to records and files containing personal information of customers and employees);
- encryption of all transmitted records and files containing personal information when sent over public wired or wireless networks, such as the Internet;
- reasonable monitoring of computer systems for evidence of unauthorized use or access of personal information;
- encryption of all personal information stored on laptops or other portable devices;
- reasonably up-to-date system security technologies such as firewalls, system monitoring software, anti-virus protection, and system patches and updates; and
- education and training of employees on the proper use of the computer security system.

Unlike the original version of the Regulation, the amended version mandates these computer security requirements "to the extent technically feasible." This change was in response to criticisms that the minimum computer security requirements were inappropriate and too burdensome for businesses that in fact experience low security risk. However, in published guidance on the OCA website, "technically feasible" is defined to mean *"that if there is a reasonable means through technology to accomplish the desired result, then that reasonable means must be used."* Arguably, the many existing commercial security products for encryption, firewalls, intrusion detection and other security devices might be deemed to constitute "technically feasible" solutions to common computer security risks, and it is not clear how the "technically feasible" or "reasonable" limitations in the Regulation will help businesses determine how the minimum computer security requirements apply to them. OCA's basic guidance on this point is that "reasonable" shall be determined in light of all relevant circumstances affecting the business, including the amount and sensitivity of the personal information handled by a business.

In the OCA website guidance, the current dearth of generally accepted encryption technologies for portable devices is cited as an example of where "reasonable" technological means are not currently available. However, the same guidance notes that well-established laptop encryption methods do exist and warns that mere password protection of laptops containing personal information will not satisfy the Regulation's encryption requirement. The guidance also notes that, as of March 1, 2010, companies will be required to encrypt back-up tapes where technically feasible.

This memorandum is intended only as a general discussion of these issues. It is not considered to be legal advice. We would be pleased to provide additional details or advice about specific situations. For additional information on this important topic, please feel free to call upon your Dewey & LeBoeuf relationship partner.

Pursuant to US Treasury Department Circular 230, unless we expressly state otherwise, any tax advice contained in this communication (including any attachments) was not intended or written to be used, and cannot be used, for the purpose of (i) avoiding tax-related penalties or (ii) promoting, marketing or recommending to another party any matter(s) addressed herein.

No part of this publication may be reproduced, in whole or in part, in any form, without our prior written consent.

© 2009 Dewey & LeBoeuf LLP
All rights reserved.

For further information on Dewey & LeBoeuf, please visit www.dl.com

Enforcement Outlook

Businesses that collect and maintain personal information on Massachusetts residents – whether directly or through outsourced service providers – and that have not yet reviewed their practices for compliance with the Regulation, may wish to do so. Although enforcement measures are unlikely to be immediate, the OCA may eventually pursue test cases involving businesses that own or license significant amounts of personal information on Massachusetts residents. In light of earlier efforts in the business community to limit or delay adoption of the Regulation, it also seems likely that court challenges to the Regulation will follow. The OCA website includes a compliance checklist to assist businesses with the development of compliant information security programs as well as a guide for small business to develop a compliant written information security policy.

Please direct any inquiries regarding the Massachusetts Regulation to John Kennedy at + 1 212 259 8505 or jkennedy@dl.com, or Vivian Polak at + 1 212 259 8289 or vpolak@dl.com in the New York office of Dewey & LeBoeuf LLP.