porterwright

Information Privacy & Data Security Law Alert

A Corporate Department Publication

March 2010

Massachusetts Data Security Law Goes Into Effect

A new Massachusetts data security law — the "Standards for the Protection of Personal Information of Residents of the Commonwealth"— has gone into effect as of March 1, 2010.

The new law is intended to apply to any business that collects or retains personal information of Massachusetts residents. Personal information, as defined under the law, includes a first name or first initial and last name in combination with any one of a (i) Social Security number; (ii) driver's license number or state identification card number; or (iii) financial account or credit card number with access codes.

Unlike the state data breach notification laws that have been adopted in most states, the Massachusetts law dictates with specificity how personal information and data should be stored and treated in the normal course of business. The law requires that businesses take proactive steps to protect the security of computerized and non-computerized personal information.

First, the regulation requires that each business implement a comprehensive, **written information security program**. Although the regulations generally state that the required complexity of the information security program is dependent on the size, scope, and type of business covered under the regulation, the law also specifically calls on covered businesses to, among other things, (i) designate an employee to maintain the program; (ii) identify and assess security risks; (iii) develop security policies for the storage, access, and transportation of records outside of the business premises; (iv) impose disciplinary measures for violations of the program; (v) prevent terminated employees from accessing records; (vi) take procedural and contractual steps to oversee service provider maintenance of appropriate security measures; and (vii) take other specified protective and preventative measures.

Second, the regulation outlines several **computer system security requirements**. To ensure compliance, any person, corporation, association, partnership, or other entity should analyze all of the technical requirements to ensure that its security measures comply. For example, the regulation requires (i) secure user authentication protocols; (ii) secure access control measures; (iii) encryption in certain circumstances; (iv) monitoring processes; (v) firewall protection; (vi) up-to-date security software; and (vii) education and training programs for employees regarding the business's computer systems and methodologies implemented to protect personal information.

While it has always been advisable to take steps to prevent a breach in security of personal information, all businesses that collect or retain personal information of Massachusetts residences should review the specific requirements of this new state law to ensure compliance.

Donna M. Ruscitti
614-227-2192
druscitti@porterwright.com

Brian D. Hall
614-227-2287
bhall@porterwright.com

Jeremy A. Logsdon
614-227-2093
jlogsdon@porterwright.com

Robert J. Morgan
614-227-2186
rmorgan@porterwright.com

Justin L. Root
614-227-2129
jroot@porterwright.com

Please see our other publications at www.porterwright.com/publications.

Porter Wright Morris & Arthur LLP
www.porterwright.com

Cincinnati, Ohio
800-582-5813
Cleveland, Ohio
800-824-1980
Columbus, Ohio
800-533-2794
Dayton, Ohio
800-533-4434
Naples, Florida
800-876-7962
Washington, DC
800-456-7962