BULLIVANTHOUSER

Ronald L. Richman
San Francisco,
Shareholder

Direct Dial: 415.352.2722
Fax: 415.352.2701
Email Attorney

For Companies Operating On The Web, New Data Security Regulations Have Broad Implications

By Ronald L. Richman

Does your company have an online presence with national reach? Sales on the East Coast? Customers in Boston?

If your company counts among its customers residents of Massachusetts, you have until March 1, 2010 to ensure that your data storage and transmission policies and practices are in compliance with new data security regulations issued by the State of Massachusetts.

On November 4, 2009, after significant revision and multiple delays amid criticism from national retailers and service providers, including Wal-Mart, Target, Microsoft, Google and others, the Office of Consumer Affairs and Business Regulation ("OCABR") of the State of Massachusetts issued a final set of regulations (201 CMR 17.00 et seq.) imposing new minimum data security standards on companies that collect, store or transmit personal information concerning Massachusetts residents. The regulations are the first of their kind to impose comprehensive data security requirements on retailers and represent an increasing trend toward state regulation of consumer data and privacy.[1]

The regulations implement Massachusetts General Law chapter 93H, enacted in October 2007 as part of a broader set of data security provisions designed to protect consumers against identity theft.[2] The 2007 law imposes certain obligations upon companies that possess personal data concerning Massachusetts residents, including an obligation to provide notification to affected individuals in the event of a data breach.[3] The law also authorizes the OCABR to implement regulations imposing data security requirements on any company that "owns or licenses personal information" concerning Massachusetts residents.[4] The regulations, originally set to take effect on January 1, 2009, have been revised several times amid concerns about the costs and burdens of implementation and compliance.

As issued, the final regulations require "[e]very person who owns or licenses personal information about a resident" of Massachusetts to develop, implement, and maintain a comprehensive written information security program ("WISP").[5] Covered by the regulations is any company that "receives, stores, maintains, processes, or otherwise has access to" personal information concerning a Massachusetts resident.[6] The regulations define "personal information" as including a resident's first and last name, or last name and first initial, and a Social Security number, driver's license or state-issued ID number, or a financial account number.[7] Accordingly, any business that accepts checks or credit cards from a Massachusetts resident, or otherwise obtains access to the foregoing information, must comply with the Massachusetts regulations, regardless of where the company is located.

In developing a WISP, the company must, among other things, identify and assess "reasonably foreseeable internal and external risks," develop comprehensive security policies and procedures for employees, and impose reasonable restrictions on physical access to records.[8] The company must regularly monitor the program for compliance and effectiveness, review the policy at least annually and document responsive actions taken in connection with any security breach.[9]

The regulations also specify certain minimum security standards for electronic records, including secure user authentication protocols and access control measures, and the use of reasonably up-to-date security software.[10] Companies subject to the regulations must also encrypt all personal information transmitted across public networks or stored on laptops or

other portable devices.[11]

Finally, in dealing with third party vendors, companies must select vendors that are capable of maintaining appropriate security measures and must include provisions in new contracts requiring the vendors to maintain appropriate security measures.[12]

Violators are subject to an enforcement action by the Massachusetts attorney general's office and may also be vulnerable to civil suits brought by private plaintiffs. Although MGL 93H does not expressly provide for a private right of action, private plaintiffs may be permitted to sue under Massachusetts' broad unfair and deceptive business practices statute.

---

[1] Since October 1, 2008, the state of Nevada has imposed an encryption requirement for the transmission of personal information, but to date has not enacted a comprehensive data security scheme. See Nevada, NRS 597.970 (businesses operating in the state are prohibited from "transfer[ing] any personal information of a customer through an electronic transmission other than a facsimile to a person outside of the secure system of the business unless the business uses encryption to ensure the security of electronic transmission").
[2] Also enacted in October 2007 was MGL ch. 93I, which created mandatory guidelines for the destruction of personal information contained in businesses records.
[3] MGL ch. 93H, §3.
[4] MGL ch. 93H, §2.
[5] 201 CMR 17.03(1).
[6] 201 CMR 17.03(1).
[7] Id.
[8] See 201 CMR 17.03, passim.
[9] Id.
[10] 201 CMR 17.04.
[11] Id.
[12] 201 CMR 17.03(1). The rules concerning data vendors were relaxed in response to criticism to permit companies an additional two years to implement the regulations with respect to existing contracts.