COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Global Privacy & Data Security

March 1, 2010

MA DATA SECURITY REGULATIONS - EFFECTIVE 3.1.2010

We are writing to remind you that the much-discussed Massachusetts data security regulations issued by the Office of Consumer Affairs and Business Regulation (OCABR) become effective today, **March 1, 2010**. A summary of the regulations follows.

- **Covered Entities Defined.** The revised regulations apply to persons who "own or license" personal information about a Massachusetts resident. See 201 CMR 17.01(2). "Owns or licenses" is defined to include any person that "receives, stores, maintains, processes or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment." See 201 CMR 17.02. "Personal Information" is defined as "a Massachusetts resident's first name and last name or first initial and last name in combination with any one or more of [a list of] data elements that relate to such resident," including, for example, Social Security number, driver's license number, or credit or debit card number. See id.
- **Information Security Program.** Entities that own or license personal information about a Massachusetts resident must implement a comprehensive written information security program, similar to the federal Gramm-Leach-Bliley requirements for financial institutions. The information security program should account for personal information for employees, as well as customers, and cover both paper and electronic records. In designing a program, the OCABR regulations specifically permit businesses to consider: (1) the size, scope, and type of the business; (2) the company's available resources; (3) the amount of stored data; and (4) the need for security and confidentiality of consumer and employee information. See 201 CMR 17.03(1). OCABR Undersecretary Barbara Anthony indicated in a recent interview with BNA that in assessing the sufficiency of a written information security program, regulators are likely to look to industry standards and whether those standards are appropriate given a company's particular risks. See BNA Privacy Law Watch (Feb. 27, 2010), http://news.bna.com/pwdm/PWDMWB/split_display.adp?fedfid=16355072&vname=prabulallissues&fn=16355072&jd=a0c2e1a2n2&split=0 (subscription required).
- **Technical Feasibility Applied to All Computer Security Requirements.** The regulations limit computer system security requirements to those that are "technically feasible." See 201 CMR 17.04. OCABR has stated that "technically feasible" means "that if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used."
- **Encryption Standard.** The rules require that computer security systems "at a minimum, and to the extent technically feasible," provide for "[e]ncryption of all transmitted records and files containing personal information that will travel across public networks. . .encryption of all data containing personal information to be transmitted wirelessly. . . [and] [e]ncryption of all personal information stored on laptops or other portable devices." See 201 CMR 17.04. "Encrypted" is defined simply as "the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key." See 201 CMR 17.02.

  In last week's interview with BNA, Undersecretary Barbara Anthony acknowledged that encryption

technology may not yet be widely available for certain type of portable devices, such as Blackberries or cell phones. She emphasized the importance of written information security programs addressing the risks of nonetheless sending personal information using such technologies. In addition, while the regulations do not prescribe a specific encryption standard, she indicated that for encryption technology to be considered adequate, the text needs to be unreadable and impossible to decode without the use of some confidential processor key.

- **Service Provider Provisions.** The regulations require businesses to take "reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect such personal information consistent with [the] regulations and any applicable federal regulation" and to require "such third-party service providers by contract to implement and maintain such appropriate security measures for personal information." See 201 CMR 17.03(f)(1), (f)(2). The regulations include a grandfather clause stating that until March 1, 2012, contracts entered into prior to March 1, 2010 shall be deemed in compliance, even if a contract lacks the required contractual language. See 201 CMR 17.03(2)(f)(2).
- **Employee training.** Undersecretary Barbara Anthony also emphasized the importance of employee training: "[T]he culture security has to start at the top of each organization. . . . [Y]our security program is only as strong as your weakest employee."

If you have any questions concerning the material discussed in this client alert, please contact the following members of our global privacy & data security practice group:

Erin Egan	202.662.5145	eegan@cov.com
David Fagan	202.662.5291	dfagan@cov.com
Jamillia Ferris	202.662.5058	jferris@cov.com