MASSACHUSETTS AGAIN REVISES ITS DATA SECURITY REGULATIONS AND EXTENDS COMPLIANCE DEADLINE UNTIL MARCH 1, 2010

On August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulations ("OCABR") proposed a number of revisions to the Commonwealth's expansive (and often controversial) data security regulations (the "Regulations"). Because these Regulations apply broadly to any company (including those located *outside* Massachusetts) that handles "personal information"[1] of Massachusetts customers or employees, the proposed changes should be of interest to a wide array of organizations across the U.S. Also of interest is that OCABR further extended the deadline for complying with the Regulations from January 1, 2010 until March 1, 2010.

According to OCABR, the Regulations were revised in an effort to make them more consistent with federal laws relating to personal information security practices and procedures and to address concerns raised by small businesses. The following are the key proposed changes to the Regulations, which can be found at: http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf. Companion FAQs can be found at: http://www.mass.gov/Eoca/docs/idtheft/201CMR17faqs.pdf.

- **Clarification of "Risk-Based" Approach.** The proposed revisions stress the "risk-based" nature of the Regulations. Under such an approach, a business, in developing its written information security program, should take into account its (1) size, scope, and type of business; (2) amount of resources; (3) amount of personal information stored; and (4) need for security and confidentiality of customer and employee information. While the existing version of the Regulations reference these risk-based factors, the proposed revisions clarify that these factors are not simply what regulators may consider in assessing a company's compliance; rather, they are things that companies can take into account when deciding what security measures they will put in place. Although this may provide some flexibility and relief for many small business with little exposure to personal information and limited resources, for most large businesses, the Regulations -- even as revised -- will likely still be among the most onerous in the country.

- **Revised Scope of Application.** A new definition of "owns or licenses" indicates that the Regulations apply only to Massachusetts residents who are customers or employees of a business: *i.e.*, "natural persons" not engaged in commerce are not covered. However, this definition may also expand the scope of the Regulations. Previously, they applied to all

[1] The Regulations' definition of "personal information" has not changed. It includes a Massachusetts resident's first name and last name or first initial and last name *in combination with* any one or more of the following data elements that relate to such resident: (1) Social Security number; (2) driver's license number or state-issued identification card number; or (3) 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.

persons that "own, license, store, or maintain personal information" about a Massachusetts resident, but no definition of own or license was provided. Under the new definition of "owns or licenses," businesses that "receive, maintain, process, *or otherwise have access to* personal information" are covered (emphasis added). The FAQs do not explain the reasoning behind this change, but it could wind up enlarging the scope of the already broad Regulations. At the same time, the FAQs indicate that businesses that merely swipe credit cards and do not "retain or store any of the personal information of its customers" are not covered by the Regulations, because "you do not have custody or control over the personal information" and therefore would not "own or license" it. This FAQ statement seems much narrower than the revised Regulations' definition of "owns or licenses" -- stressing as it does "custody and control" of the information as the key factor, rather than mere "access to" it -- and will likely trigger further debate and require further clarification.

- **"Technically Feasible" Qualifier for Computer System Security Requirements.** A key change to the Regulations' computer security requirements -- which include, among others, mandatory encryption for personal information transmitted wirelessly or over public networks and for storage on portable devices -- is that they now apply to businesses only "to the extent technically feasible." The FAQs define "technically feasible" to mean that "if there is a reasonable means through technology to accomplish a required result, then that reasonable means must be used." Thus, for most large organizations with comparatively greater resources, the Regulations will still likely be interpreted to impose fairly burdensome computer system security requirements.

- **Revised Definition of "Encryption."** The revised definition reads as follows: "the transformation of data into a form in which meaning cannot be assigned without the use of a confidential process or key." The FAQs explain that this change -- which removes the prior reference to an "algorithmic process" -- is intended to make it technology neutral, so that, as encryption technology evolves, the Regulations will not impede the adoption of such new technologies. While the Regulations require the encryption of portable devices where it is reasonable and technically feasible, the FAQs acknowledge that, aside from laptops, it may not be possible currently to encrypt most portable devices, such as cell phones, Blackberries, netbooks, and iPhones. At the same time, however, the FAQs indicate that "personal information should not be placed at risk in the use of such devices." The FAQs also instruct that backup tapes must be encrypted on a going-forward basis.

- **Definition of "Financial Account."** The FAQs define financial account as "an account that if access is gained by an unauthorized person to such account, an increase of financial burden, or a misappropriation of monies, credit or other assets could result." Examples provided include a checking account, savings account, mutual fund account or annuity account, any kind of investment account, or a credit or debit account. Many parties had asked OCABR for a definition of this term, since it is possible that the Regulations' key definition of personal information might not be triggered if a Massachusetts resident's financial account were not involved.

- **Oversight of Service Providers.** Under the revised Regulations, businesses would be required to oversee service providers by (1) taking reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures consistent with the Regulations and any applicable federal regulations; and (2) requiring such third-party service providers, *by contract*, to implement and maintain such security measures for personal information. However, the revised Regulations contain a grandfather provision specifying that such a contract requirement would apply only to contracts entered into on or after March 1, 2010, with contracts entered into prior to March 1, 2010 to be deemed in compliance until March 1, 2012. Although this provision is oddly worded, it appears to mean that, for noncompliant contracts entered into prior to March 1, 2010, the grace period expires on March 1, 2012.

A public hearing on the proposed changes to the Regulations will be held in Boston on Tuesday, September 22, at 10 AM. We would expect this hearing will include a spirited debate about some of the above changes, likely focusing on the fact that they do not go far enough to streamline or reduce the burdens associated with the Regulations.

CONCLUSION

Due to the many requirements imposed by the Regulations, even with the proposed revisions discussed above, businesses that have customers or employees in Massachusetts should closely review their written information security policies and data management practices to ensure that they will be compliant with the revised Regulations, which are still among the most detailed and onerous of their kind. Businesses should also continue to monitor the status of the Regulations, as we would expect further changes to come after the September 22nd hearing.

* * * * * * * * * * * * * * *

If you have any questions regarding this memorandum, please contact Francis M. Buono (202-303-1104, fbuono@willkie.com), McLean B. Sieverding (202-303-1163, msieverding @willkie.com), Marc J. Lederer (212-728-8624, mlederer@willkie.com), or the attorney with whom you regularly work.

Willkie Farr & Gallagher LLP is headquartered at 787 Seventh Avenue, New York, NY 10019-6099 and has an office located at 1875 K Street, NW, Washington, DC 20006-1238. Our New York telephone number is (212) 728-8000 and our facsimile number is (212) 728-8111. Our Washington, DC telephone number is (202) 303-1000 and our facsimile number is (202) 303-2000. Our website is located at www.willkie.com.

August 24, 2009