

September 25, 2009

MASSACHUSETTS DATA SECURITY REGULATIONS

The Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) held what is likely to be its last public hearing on the proposed Data Security Regulations on September 22, 2009. The Regulations are expected to be finalized, substantially in their current form, during the month of October. Compliance is mandatory by March 1, 2010.

Read on for a brief outline of the Regulations as currently written (incorporating changes issued in August 2009) and a summary of the comments made at the hearing.

THE REGULATIONS

The Regulations require every person who owns, licenses, receives, maintains, processes, or otherwise has access to personal information in connection with the provision of goods or services or in connection with employment to implement a comprehensive information security program. This captures anyone who has customers or employees who are Massachusetts residents, as well as many of those persons' service providers. Personal information is defined as a Massachusetts resident's name in combination with a social security number, driver's license or other state-issued identification number, or financial account number or credit or debit card number.

An information security program must contain administrative, technical, and physical safeguards that are appropriate to (a) the size, scope, and type of business; (b) the business's available resources; (c) the amount of stored data; and (d) the need for security and confidentiality of the information. OCABR views these factors as the elements of a "risk-based approach" to information security, consistent with the Massachusetts statute and applicable federal law.



ALERT

In essence, development of an information security program (sometimes referred to as a “written information security program” or “WISP”) must include:

1. Identifying where the organization has personal information (including in paper, electronic, and other forms), what the risks to the security of the information are, and what current safeguards the organization has in place;
2. Developing security policies for the storage of, access to, and transportation of personal information;
3. Overseeing service providers that have access to the organization’s personal information, including selecting service providers that are capable of maintaining appropriate security measures and then requiring them to make a contractual commitment to do so;
4. Establishing appropriate computer system security requirements, including, to the extent technically feasible, implementing:
 - a. secure user authentication protocols;
 - b. secure access controls;
 - c. encryption of all personal information to be transmitted across public networks or to be transmitted wirelessly;
 - d. encryption of all information to be stored on laptops or wireless devices;
 - e. monitoring of security systems; and
 - f. maintenance of up-to-date firewall and malware protections;

5. Establishing appropriate employee training, supervision, and disciplinary policies;
6. Establishing procedures for monitoring the program regularly and reviewing the scope of the program at least annually; and
7. Documenting the response to and post-incident review of any breach of security.

The complete text of the Regulations and OCABR’s FAQs are available at

<http://www.mass.gov/?pageID=ocahomepage&L=I&L0=Home&sid=Eoca>. Follow the links to “Identity Theft.”

THE PUBLIC HEARING COMMENTS

At the public hearing, several people testified that the Regulations are still too prescriptive and should be modified, principally by making the Regulations more consistent with comparable federal regulations (such as the FTC’s Safeguards Rule) or simply by providing that compliance with any applicable federal regulation (such as HIPAA, the FTC Safeguards Rule, or Federal Reserve Board Regulation P) constitutes compliance with the State Regulations. We believe wholesale changes along these lines are extremely unlikely.

There were also a significant number of comments regarding the third party service providers provisions and, specifically, that the Regulations were overly burdensome in requiring a contractual commitment by the provider to maintain appropriate security measures. The Undersecretary of OCABR repeatedly pointed out that all service providers cited by commenters already have



contracts with the organization whose information they can access, so the Regulation is not adding a significant burden by requiring the addition of an information security provision to such contracts.

The Undersecretary did acknowledge that the provision regarding the grace period for implementing the required contract provision in existing contracts is unclear. She commented that OCABR had intended to provide a 2-year grace period for bringing existing contracts into compliance and that one of the tweaks in the final Regulations would be to make that clear.

The Undersecretary was keenly interested in certain types of third party relationships, such as insurance agency relationships with their insurance providers. Testimony was offered that insurance providers should not be considered “third party providers” at all (because an agent is an alter ego of its principal), and therefore agents should not be subject to the service provider provisions of the Regulations when dealing with their providers. The Undersecretary seemed unpersuaded by this argument. While the final Regulations may include some clarification with respect to agency relationships, we think any such clarification is more likely to confirm the applicability of the Regulations than to create an exemption.

Several commenters focused on the “technical feasibility” language with respect to computer system security requirements and sought clarification regarding whether this created an obligation to adopt new technologies as soon as they became available. For example, if a new technology to encrypt data on a PDA were

developed tomorrow, would everyone be obligated to adopt that technology before March 1, 2010? Although the Undersecretary made no explicit statement regarding her view of this issue, her comments and questions suggested that the Regulations were not intended to have that result. We think it is possible that OCABR may address this issue in its FAQs or other guidance, if not expressly in the Regulations.

All in all, the comments presented at the hearing did not raise any new or fundamental issue that is likely to cause a substantive revision to the Regulations. The Undersecretary confirmed as much in brief conversation after the hearing. We believe the final Regulations will be issued in October with no substantive changes from the draft that was released in August.

PLANNING FOR COMPLIANCE

With the summer behind us and just over five months to go before March 1, 2010, any person who “owns or licenses, receives, maintains, processes, or otherwise has access to personal information” regarding Massachusetts residents – including customers, employees, or both – should be well on their way to establishing a written information security program that complies with the OCABR Regulations. According to their terms, the Regulations apply to businesses located both inside and outside of Massachusetts. Please call us if you have questions about whether the Regulations apply to you or how to implement an appropriate WISP.

New York

Seven Times Square
New York, NY 10036
+1.212.209.4800
+1.212.209.4801 [fax]

Boston

One Financial Center
Boston, MA 02111
+1.617.856.8200
+1.617.856.8201 [fax]

Washington, DC

601 Thirteenth Street NW,
Suite 600
Washington, DC 20005
+1.202.347.2222
+1.202.347.4242 [fax]

Hartford

City Place I
185 Asylum Street
Hartford, CT 06103
+1.860.509.6500
+1.860.509.6501 [fax]

Providence

121 South Main Street
Providence, RI 02903
+1.401.276.2600
+1.401.276.2601 [fax]

London

8 Clifford Street
London, W1S 2LQ
United Kingdom
+44.20.7851.6000
+44.20.7851.6100 [fax]

Dublin

Alexandra House
The Sweepstakes
Ballsbridge, Dublin 4
Ireland
+353.1.664.1738
+353.1.664.1838 [fax]

www.brownrudnick.com

Watch this space for updates, or contact our Data Security Team leaders:

Nancy R. Wilsker nwilsker@brownrudnick.com (617) 856-8343

Elizabeth A. Ritvo eritvo@brownrudnick.com (617) 856-8249

BROWN RUDNICK is an international law firm with offices in the United States and Europe. Our 200 attorneys provide assistance across key areas of the law, including corporate and securities, intellectual property, complex litigation and arbitration, finance, bankruptcy and restructuring, government law and strategies, tax, climate and energy, and real estate.

Information contained in this Alert is not intended to constitute legal advice by the author or the attorneys at Brown Rudnick LLP, and they expressly disclaim any such interpretation by any party. Specific legal advice depends on the facts of each situation and may vary from situation to situation.

Distribution of this Alert to interested parties does not establish an attorney-client relationship. The views expressed herein are solely the views of the authors and do not represent the views of Brown Rudnick LLP, those parties represented by the authors, or those parties represented by Brown Rudnick LLP.

