

MASSACHUSETTS DATA SECURITY REGULATIONS THE LATEST DEVELOPMENTS

January 20, 2009

On Friday, January 16, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) held a public hearing concerning the recently extended Massachusetts data security regulations (201 CMR 17.00). The Regulations, described by many speakers at the hearing as the nation's most cumbersome data security regulations, require all entities that license, store or maintain personal information about a Massachusetts resident to implement a comprehensive information security program. Compliance with many of the Regulation's provisions is required by May 1, 2009.

The standing-room-only crowd at the hearing included representatives of the Greater Boston Chamber of Commerce, Massachusetts Business Coalition, various nonprofits, colleges and universities, and others. They voiced practically the same concerns we have heard directly from our clients: the near impossibility (given technologies that are currently available) of complying with the encryption standards, the difficulty of obtaining third party vendor certifications, and the enormous investment of time, energy, and scarce cash required by this mammoth undertaking.

The oral testimony was transcribed and various participants submitted written testimony as well. The OCABR hearing officer did not comment on the testimony and there was no indication whether OCABR would further delay the implementation of the Regulations or make any other changes. We recommend, however, that persons affected by the Regulations (virtually every business with Massachusetts customers or employees) assume the May 1 date will hold and begin planning to comply. The first step in most cases is to begin an inventory of all files in which covered information (individual's name plus one of (a) SSN, (b) driver's license or state ID #, or (c) financial account number) is held. Since all records containing such information must be secured, a business must secure all records unless it can identify the records that do not contain covered information. This can be a time-consuming process and is a good place to start.

Brown Rudnick will keep you posted regarding further developments. In the meantime, please call your Brown Rudnick contact or one of the attorneys named below with any questions or for assistance in developing a compliance strategy.

Elizabeth A. Ritvo at +1.617.856.8249 / eritvo@brownrudnick.com
Nancy R. Wilsker at +1.617.856.8343 / nwilsker@brownrudnick.com

Jennifer A. Herz contributed to the development of this Alert.

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.