Massachusetts Regulators Propose Amendments to Information Security Regulations, Delay Enforcement Until March 1, 2010

August 18, 2009

SECURITY & PRIVACY ALERT - AUGUST 18, 2009

written by Colin J. Zick, Gabriel M. Helmer

On Monday, August 17, 2009, the Massachusetts Office of Consumer Affairs and Business Regulation (OCABR) indicated that it will be modifying some provisions of the strict Massachusetts information security regulations first promulgated last year, 201 CMR 17.00 et seq. Of most immediate concern to many businesses, OCABR will extend the deadline to comply with the regulations from January 1, 2010 to March 1, 2010.

The Massachusetts identity theft regulations affect any individual or business that receives, maintains or otherwise has access to personal information, but the proposed amendments limit the scope of the regulations to individuals and businesses that receive personal information in connection with the provision of goods or services or in connection with employment. This excludes anyone not engaged in commerce. As in prior versions of the regulations, personal information includes the Social Security numbers, state drivers license, identification card numbers or financial account information of Massachusetts residents.

To comply with the regulations, affected businesses will be required to implement a written information security program that is appropriate to the size of the business, available resources, the amount of sensitive personal information and the need for security to protect the information. Prior regulations stated that these factors would be considered by regulators in evaluating compliance, but the revised regulations make it clear that businesses are entitled to take these factors into account when deciding what security measures to put in place. For small businesses with little exposure to personal information and limited resources, this means that a compliant information security program should be less burdensome.

A key amendment for many businesses is that the technical security measures identified in the regulations, such as the encryption of emails and portable devices, will not be required in all circumstances. The amendments require businesses to adopt these protections for electronic information only when they are technically feasible and reasonable to implement.

Also, businesses that use service providers to process or handle personal information will be required to do more than merely take reasonable steps to ensure that service providers are taking reasonable security precautions. The revised regulations require businesses to enter into written agreements with those providers that obligate them to provide appropriate levels of security.

There will be a hearing for public comment on the proposed regulations on September 22, 2009.

Foley Hoag advises clients developing information security programs to comply with the Massachusetts regulations, as well as other federal, state and international laws regarding information security and identity theft.