ECKERT SEAMANS
ATTORNEYS AT LAW

FEBRUARY 2012

MASSACHUSETTS CORPORATE ALERT

A KEY GRACE PERIOD UNDER THE MASSACHUSETTS DATA SECURITY REGULATIONS EXPIRES ON MARCH 1, 2012

Background

The Massachusetts Data Security Regulations (the "Regulations") became effective on March 1, 2010. These Regulations were designed to reduce the rising tide of identity theft by requiring that all persons and entities which receive, store, process, maintain or have access to "personal information of a Massachusetts resident" adopt comprehensive written policies and procedures to protect that information. "Personal information" is defined as the names of Massachusetts residents "in combination with" social security numbers, driver's license numbers or financial account numbers (referred to below as "MPI").

The Regulations are technically detailed and go beyond many federal and state data protection requirements. Furthermore, the Regulations recognize that many service providers (for example, payroll services, accounting firms, investment advisors, etc.) will have access to the MPI of their clients and in some cases their clients' employees. Accordingly the Regulations include a requirement that persons and entities covered by the Regulations must take reasonable steps to ensure that their outside service providers implement and maintain their own security measures to protect MPI of their clients.

Grace Period for Service Provider Contracts Expires March 1, 2012

When the Regulations because effective nearly two years ago, they included a requirement that contracts for services to be rendered directly to a person or entity covered by the Regulations must include a provision which requires the service provider to adopt and maintain security procedures to protect the client's or customer's MPI. These security procedures must comply with the Regulations and applicable federal law. This requirement applied to all contracts with service providers entered into on or after March 10, 2010. The Regulations provided a two year grace period for contracts with service providers which were entered into before the Regulations became effective (March 1, 2010) but that grace period expires on March 1, 2012.

Persons and entities which are subject to these Regulations (as a practical matter, anyone who employs Massachusetts residents is covered whether or not they are doing business in Massachusetts) should review their service provider agreements to ensure that the necessary provision is included. If not, a simple amendment to the agreement will be necessary to ensure that their existing written information security plan remains in compliance with the Regulations.

In the event a plan has not yet been adopted, immediate action should be taken to adopt a plan which complies with the Regulations. Failure to comply with the Regulations can result in a penalty of up to $5,000 per violation, plus attorneys fees and expenses.

For persons or entities which have not yet adopted a plan, the general requirements are summarized below.

General Requirements of the Regulation

The written plan must include a variety of specific safeguards, including but not limited to (i) identification and evaluation of foreseeable risks; (ii) limitations on physical access to MPI; (iii) regular monitoring of the effectiveness of the plan; (iv) security policies for any off-site use of MPI; (v) documentation of responses to any actual security breaches involving MPI, (vi) an employee training program and (vii) provisions for dealing with outside service providers with access to MPI.

Any business which electronically stores or transmits MPI is also subject to detailed electronic security requirements with respect to its computers and related systems. Among other things, (a) all MPI stored on laptops or other portable devices must be encrypted; (b) access to electronically stored MPI must be controlled by means of user names and passwords issued only to those persons whose job description requires that they have access to MPI and (c) businesses must maintain reasonably up-to-date firewalls, anti-virus software and security patches.

The statute authorizes the Massachusetts Attorney General to enforce the Regulations by bringing action under MGL chapter 93A, which prohibits "unfair and deceptive business practices" and provides for triple damages in some cases.

If you have any questions, please contact Don Burnham at 617.342.6843 or Bill Miller at 617.342.6837 in the Boston office, or any other Eckert Seamans attorney with whom you have been working.