Proskauer

Massachusetts Data Security Regulations: Deadline To Update Service Provider Contracts Is Fast Approaching

January 24, 2012

The deadline for compliance with a key requirement of the Massachusetts Data Security Regulations ("Regulations") is only a month away. By March 1, 2012, contracts must require that certain service providers implement and maintain appropriate security measures to protect personal information. [1] *See* 201 CMR 17.03(2)(f).

This requirement pertains to entities that “own or license" personal information of Massachusetts residents. Regardless of location, an entity must comply if it receives, stores, maintains, processes, or otherwise has access to personal information of Massachusetts residents in connection with the provision of goods and services or in connection with employment. Because the Regulations contain such broad definitions for terms such as “own and license," most service providers – from your payroll provider to your e-commerce hosting provider – are likely subject to this requirement.

The Regulations require entities that own or license personal information of Massachusetts residents to oversee service providers by taking reasonable steps to select and retain service providers that are capable of maintaining appropriate security measures to protect personal information. In addition, those service providers must be required by contract to implement and maintain appropriate security measures to protect personal information.

Contracts with service providers entered into after the effective date of the Regulations, March 1, 2010, have been and continue to be required to contain a representation of compliance. However, to ease the burden on entities with already-existing service provider contracts, the Regulations include a carve-out for contracts that predate the effective date of the Regulations. Specifically, any service provider contract entered into before March 1, 2010 is deemed to be in compliance, even without an express contractual provision, as long as it is updated by March 1, 2012.

Entities that own or license personal information of Massachusetts residents bear the burden of ensuring that their service providers are in compliance. As such, consider whether you rely on your service providers to receive, store, maintain or process personal information of Massachusetts residents, or whether you otherwise give service providers access to such information. If you do, now is the time to ensure that those service provider contracts contain a representation that appropriate safeguards are maintained to protect personal information.

In addition, to satisfy the due diligence requirement set forth in the Regulations, consider asking for a copy of the service provider's written information security program (“WISP"). All entities that own or license personal information of Massachusetts residents are required to develop, implement and maintain a WISP, which sets forth administrative, technical and physical safeguards to protect personal information. For all entities, the Regulations encourage a risk-based analysis, where the WISP is appropriate to (1) the size, scope and type of business of the person obligated to safeguard the personal information; (2) the amount of resources available to that entity; (3) the amount of stored data; and (4) the need for security and confidentiality of both consumer and employee information.

For more information on the requirements of the Regulations, please see our previous client alert, New Massachusetts Data Security Regulations Go Into Effect on March 1, 2010.

[1] “*Personal information*" is defined by the Regulations as a Massachusetts resident's first and last name, or first initial and last name, in connection with any of the following: (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. Personal information does not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.