Proskauer

New Massachusetts Data Security Regulations Go Into Effect on March 1, 2010

February 18, 2010

New regulations concerning the safeguarding of personal information with respect to persons residing in Massachusettswill go into effect on March 1, 2010 (the "**Regulations**"). The Regulations will apply to persons and businesses (each, a "**Company**") that "own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts" and, among other things, will prescribe requirements regarding the storage and transmittal of such "personal information" (201 CMR 17.00). The Regulations therefore may require action on the part of a Company, whether or not that Company maintains an office in Massachusetts.

If a Company "owns, licenses, stores or maintains" personal information about persons who reside in Massachusetts, the Regulations will impose specific information security requirements that may require that Company to increase its standard of care. The Regulations concern "personal information" of both consumers and employees. "Personal information" is generally defined as a Massachusetts resident's name in combination with his or her Social Security number, driver's license or state ID card number, or financial account or credit/debit card number that would permit access to the resident's financial accounts. The Regulations will apply to both paper and electronic records, and will require each Company to develop and maintain a written security policy to ensure the protection and confidentiality of the Company's records containing personal information.

The Regulations will affect both the storage and transmittal of personal information, requiring, among other things, "to the extent technically feasible," the encryption of such personal information, whether such information is being stored electronically (on portable devices such as laptops or hand held devices) or electronically transmitted over a public network such as the Internet. As of the effective date, March 1, 2010, no Company should electronically transmit, via e-mail or FTP over the Internet, documents containing personal information related to persons residing in Massachusetts, regardless of the intended recipient of such communications, unless the transmitted data has been encrypted in compliance with the Regulations.

As a threshold matter, your organization should begin to:

- Determine whether you have any Massachusetts residents as clients or employees.
- Determine who within your Company will be responsible for implementing and maintaining security policies and programs.
- Determine who within your Company should have access to personal information (and who can be excluded from access).
- Identify the paper, electronic, computing systems and portable devices that contain personal information.
- Consider appropriate measures to protect your Company's personal information, in light of your Company's size, scope and type of business, resources, amount of personal information and need.
- Determine whether your Company provides any personal information to others (such as accountants, lenders, or other vendors or service providers).
- Consult with your information technology providers to ensure that you have up-to-date firewall and other network protections, as well as data encryption capabilities (including on all portable devices).

Other federal laws and regulations address, in part, obligations with respect to personal information, and other states besides Massachusetts have enacted laws and regulations both with respect to protecting information and reporting potential data security breaches. You may already have adopted some form of information security program. In light of the new regulations, however, it is important that you review your security policies and procedures closely and make any necessary adjustments to ensure compliance. We can work with you to update such policies in keeping with your own needs and business model.