GREEN·SEIFTER ATTORNEYS, PLLC

Alert

Business Law/Not-for-Profit Organizations

Protection of Personal Information – New Regulations in Massachusetts Can Affect New York Entities

Green & Seifter, Attorneys, PLLC **March 16, 2010**

In order to compel companies to protect the personal data of their employees and clients, Massachusetts has put into effect new information security regulations, effective as of March 1, 2010. Previous breach-notification laws address what happens after a security breach. These new regulations are intended to prevent personal information from being breached in the first place. The goal is to require companies to develop reasonable and effective administrative, technical, and physical safeguards in order to protect the personal information of residents of Massachusetts.

Who is affected by the new regulations?

The regulations apply to all persons or entities (deemed "service providers") with access to personal information of Massachusetts residents. A service provider is "any person that receives, stores, maintains, processes or otherwise is permitted to access personal information…" Personal information is defined as a combination of a resident's first and last name and any of the following:

- Social Security number
- financial account number
- driver's license or state ID number
- credit or debit card number

What does this mean for New York residents and entities that gather and/or retain personal information of Massachusetts residents?

While the New York Consumer Protection Board encourages businesses to have written policies to protect the personal information of employees and customers, such policies are not required by law in New York State. However, these Massachusetts laws do affect New York residents and require all businesses (regardless of location) to comply with respect to any Massachusetts resident's personal information.

The regulations require that all service providers with access to personal information must:

- Develop and implement a written security program,
- Follow administrative, technical, and physical safeguards included in the written information security program, and
- If information is maintained by a third party, they must also appropriately safeguard personal information.

When are the deadlines for compliance?

- Service Providers who collect/store their own data: Deadline was March 1, 2010.

continued

- Use of third party for data collection: When using a third party to handle data, businesses must contractually require their third party service providers to safeguard personal information in accordance with the new regulations. Third party service provider contracts entered into on or before March 1, 2010 are exempt from complying with this requirement until March 1, 2012. However, after March 1, 2010, any new contracts or renewals of existing contracts must incorporate the regulatory requirements.

What if I am not compliant?

The new law increases an entity's exposure to lawsuits. For example, if a company does not meet the compliance requirements, the Massachusetts Attorney General could file suit against the company. Additionally, civil penalties could be imposed for noncompliance, and, as always, a company's reputation can be tarnished by a failure to protect the personal information it holds. Voluntary compliance is the most cost-effective route to take when dealing with protections laws.

We suggest that you evaluate your existing security policies to determine the extent to which these regulations will affect you and identify the steps you need to take to be in compliance. The regulations, officially titled 201 CMR 17.0: Standards for the Protection of Personal Information of Residents of the Commonwealth, can be found at:
http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

If you have any questions about these new regulations and how they apply to your business, please contact your attorney by calling our office at 315.422.1391.