

## **The New Massachusetts Data Protection Law – Changes to Business Operations**

The Commonwealth of Massachusetts enacted new data breach security regulations, which go into effect on March 1, 2010. These regulations apply to any person engaged in commerce that owns or licenses personal information of a resident of the Commonwealth. Owns or licenses means receives, maintains, processes, or otherwise has access to such personal information in connection with the provision of goods or services or in connection with employment.

The regulations have two primary requirements, which are to:

- 1) develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing such personal information; and
- 2) establish and maintain a comprehensive security system covering any computer (including any wireless system) which stores or electronically transmits personal information.

The written program need only be appropriate to the size of the business, available resources, the amount of stored data, and the need for security to protect the information. Though the computer security system must meet specific minimum criteria and include various elements (including, secure user authentication protocols, secure access control measures, encryption, monitoring systems for unauthorized access, up-to-date versions of system security agent software and education and training of employees), these elements must be met to the extent technically feasible.

The application of the regulations is geographically far-reaching and will affect many areas of a company's business operations.

Consider that the regulations are enforceable against companies located inside and outside of the Commonwealth (which raises the issue of jurisdiction and constitutionality of the regulations as applied to companies located outside of the Commonwealth).

As such, all companies, no matter where located, must determine whether the regulations are applicable and then take steps (involving time, resources and funds) to ensure compliance.

Some of the companies located outside of the Commonwealth which must review the personal information they own or license to determine if any is that of a resident of the Commonwealth include companies that:

- 1) have employees in the Commonwealth,
- 2) collect personal information through a Web site or other means about employee candidates who are Commonwealth residents, or
- 3) store personal information of one or more residents of the Commonwealth.

Given the regulations' requirements, a company subject to the regulations will need to develop a new employee training, monitoring and disciplinary program. Meeting this requirement and

remaining in compliance could prove burdensome and potentially overwhelming. The first question to ask is — who will provide the training?

Clearly, someone who understands the regulations and can transform that understanding into an effective training program should be given this responsibility. A company may invest the time and resources to train one of its own employees to conduct the training or a company may choose to engage an outside consultant.

Once the person to do the training is chosen and prepared, the training program for a company's employees must be created. The program should ensure that employees who have access to personal information of residents of the Commonwealth understand their obligations with respect to the regulations and can properly perform those obligations to keep their company in compliance. In addition, the regulations obligate a company to include in its written information security program the imposition of disciplinary measures for employees who violate the programs the company sets in place.

Employees will then need training to understand and perform under the program, including how to properly use the company's computer security system (especially if the company had to implement any new components to it).

A company will also need to train at least one designated employee to maintain and supervise the written information security program and monitor employees to ensure their compliance with the obligations connected to the regulations.

Considering the foregoing, a company would be wise to revise its employee handbook to account for the regulations and any of the related changes to that company's training, policy, procedure and disciplinary measures.

In addition to what must be undertaken as to a company's employees, a company to which the regulations apply will have to take reasonable steps to select and retain third-party service providers (each, a "service provider") that are capable of maintaining appropriate security measures to protect personal information consistent with the regulations and applicable federal regulations. The company must also require service providers by contract to implement and maintain such appropriate security measures for personal information.

The regulations add a layer of complexity to a company and service provider's business relationship and may strain the ability of a company and a service provider to do business.

The regulations will more likely than not lead to the use of additional time and resources before the business relationship even begins and throughout the working relationship. As such, a company subject to the regulations might have to review and revise the way it does business with service providers.

At the outset of a relationship with a new service provider, a company may have to take time for, and incur the expense of, auditing the service provider's information technology system and employee and security policies and practices to see if the service provider is up to par based on the requirements of the regulations.

The service provider will have to be agreeable to this intrusion into its business operations. The service provider may choose to forego the relationship with the company rather than agree to the intrusion.

The alternative, and what is the more likely course of action for a company, is to include in the company and service provider's written agreement representations and covenants given by the service provider as to what is required under the regulations.

The company may also wish to include the right to periodically audit the service provider's practices and/or require the service provider to provide certifications that it is complying with the covenants the service provider made in respect of the regulations.

As to service providers with which a company is already doing business, the company may choose to conduct the audit of the service provider's capability and application of security measures or require an amendment to any existing written agreement governing the service provider and the company's relationship to add representations and covenants given by the service provider.

The service provider may be agreeable to the audit or amendment or perhaps it may choose to terminate the relationship with the company. Overall, the regulations will likely make a company's ability to do business with service providers more complicated, costly and time consuming.

Given the regulations' requirements, a company may find that it needs or desires the services of an information technology specialist and an attorney.

Information technology specialists could help a company audit what personal information the company currently possesses, evaluate the effectiveness of the company's current safeguards, determine if the company's current computer system complies with the encryption requirements, determine whether the company needs new software or hardware, set up user identification protocols, and secure access control measures and firewalls.

Attorneys could assist with compliance and drafting proper policies and agreements. The specialist and the attorney should be introduced and encouraged to communicate as their respective work product should conform to and support one another when implemented.

Because the collection, use and storage, and protection of personal information does not usually take place in a centralized manner, the specialist and attorney will likely need assistance from a company's employees and service providers involved in the company's marketing, sales, human resources and information technology.

In summary, it is more likely than not that the regulations will increase expenses for companies that must comply, require using resources that may or may not be readily available within the company, require an audit of personal information owned or licensed by a company, result in an overhaul of employee practices and training, require changes in technology and security practices, and require a change in the company's business relationship with its service providers.

This raises three pertinent questions:

- 1) Will companies begin to specifically exclude hiring residents of the Commonwealth, specifically decline to do business with, or accept personal information of residents, of the Commonwealth, or purge their businesses and storage of residents of the Commonwealth so that compliance with the regulations is not an issue?
- 2) Will companies (at least those located outside of the Commonwealth) simply take no action as to the regulations come March 1, 2010, and wait to see whether the Commonwealth puts any teeth behind the regulations by pursuing those not in compliance (even outside the Commonwealth's borders)?
- 3) Will companies, particularly those located outside of the Commonwealth, wait to see if there are any successful attorney general actions instituted under Chapter 93A, the Commonwealth's consumer protection statute which allows for treble damages?

The answers cannot yet be determined, but it will be interesting to see what happens.

For more detailed information about the regulations, including FAQs, please visit:

[www.mass.gov/?pageID=ocatoptic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca](http://www.mass.gov/?pageID=ocatoptic&L=3&L0=Home&L1=Business&L2=Identity+Theft&sid=Eoca).

--By Debra L. Feldman, Gunster Yoakley & Stewart, PA

*Debra Feldman is an associate with Gunster in the firm's Fort Lauderdale office.*