MB&J | MORGAN BROWN&JOY

www.morganbrown.com

CLIENT ALERT: Massachusetts Data Security Regulations: Deadline for Compliance Delayed Until January 1, 2010

On February 12, 2009, the Office of Consumer Affairs and Business Regulation ("OCABR") issued a new deadline of **January 1, 2010**, for businesses that maintain personal information to be in compliance with the Standards for the Protection of Personal Information of Residents of the Commonwealth ("regulations") established by the OCABR. *See generally,* 201 C.M.R. 17.00, *et seq*. These regulations mandate that businesses develop, implement, maintain and monitor a comprehensive written information security program to protect personal information.

In 2007, Massachusetts, like forty-four other states, enacted data security laws. Effective October 31, 2007, Chapter 93H requires notice to the attorney general, the director of the OCABR, and any affected Massachusetts resident of a data security breach. In early 2008, Chapter 93I set forth the manner in which personal information is to be disposed and destroyed. The amended regulations are discussed below.

What is "Personal Information"?

The law defines "Personal Information" as a resident's first name and last name or first initial and last name in combination *with* any one or more of the following: (a) social security number; (b) driver's license number or Massachusetts identification card number; and/or (c) financial account number, or credit or debit card number.

Who is Covered?

The regulations apply to every "person that owns, licenses, stores or maintains personal information of a Massachusetts resident." These regulations are far-reaching and apply

to almost all Massachusetts employers that have personal data of Massachusetts residents, regardless of whether the business is in Massachusetts.

Security Program

Persons and businesses covered by the data security laws and regulations must have in place a *written* "Comprehensive Information Security Program" that is "reasonably consistent with industry standards." The program must have administrative, technical, and physical safeguards to ensure the security and confidentiality of records that contain personal information.

The Comprehensive Information Security Program requires:
• The designation of one or more employees to maintain the program.
• Risk assessment of all paper, electronic, or other records that contain personal

Information, including evaluating and improving the effectiveness of existing safeguards; this may include:

- ongoing employee training;
- monitoring, ensuring, and enforcing employee compliance with all policies and procedures; and
- a means of detecting and preventing security failures.

• The development of security policies for employees that take into account whether and how employees are allowed to keep, access, and transport records containing personal information outside of business premises.
• Disciplining employees that violate the security program.
• Preventing terminated employees' access to records containing personal information.
• Limiting the amount collected, time retained, and access to personal information to only those instances where it reasonably necessary to accomplish the legitimate purpose for which it is collected, stored, and accessed and to comply with state and federal law.
• Placing reasonable restrictions on physical access to records that contain personal information, including implementing a written procedure that describes how such access is restricted and the secure storage of such records.
• Monitoring and reviewing the operation of the program and upgrading the information safeguards annually or more frequently if there is a change in business practices that may reasonably implicate the security and integrity of the records that contain personal information.
• Addressing third-party service providers. Employers must take "all reasonable steps" to: 1) "verify that any third-party service provider with access to personal information has the capacity to protect such personal information" as required by the regulations; and, 2) "ensure that such third party service provider is applying to such personal information protective security measures at least as stringent as those required" by the regulations.
• Implementing a data security breach action plan. Document actions taken in response to a security breach, as well as any changes made in the policy or other business practices as a result of the breach. (As mentioned above, Chapter 93H requires notification to the Attorney General and the OCABR in the event of a security breach or unauthorized use/acquisition of personal information.)
• Addressing computer system security requirements. As part of the written information security policy, there must be a security system in place that covers all computers, including any wireless system. The following elements, at a minimum, must be in place:

- Secure user authentication protocols including control of user IDs, secure assignment and selection of passwords, restricting access to passwords, restricting access to active and authorized users only.
- Secure access control measures that permit access to records and files that contain personal information for only those persons that must access such information to carry out their job duties, assign unique computer identifications and passwords that are reasonably designed to preserve the integrity of the security controls.
- Encrypt all files and records that contain **personal information**, which will travel across public networks and wireless systems to the extent feasible. All personal information on laptops or other portable devices must be encrypted.

- Reasonable monitoring of systems for unauthorized use of access to personal information.
- Where files containing personal information are on a system connected to the internet, the system *must have* reasonably up-to-date firewall protection and operating system security patches.
- Reasonably-up-to-date versions of such software or software that can receive updates, including malware protection, patches, and virus definitions must be in place on the computer system.
- Employees must be trained and educated on the proper use of the computer security system and the importance of personal information security.

Compliance Will Be Measured on a Case-by-Case Basis

This overview of the data security laws and regulations touches on the *minimum* required of employers that employ Massachusetts residents. Compliance with these regulations will account for the size, scope, and type of business; the amount of resources available to the business; the amount of stored data to protect; and, the need for security and confidentiality of consumer and employee information. *See* 201 C.M.R. 17.03. As compliance will be measured on a case-by-case basis, it is essential that employers begin taking steps now to ensure compliance by **January 1, 2010**. If you have questions or concerns about the data security laws and regulations, please contact your MBJ attorney.

Notice of Schedule Change for Seminar and Updates to Regulations

The seminar, "Massachusetts Personal Information Law: Are You Ready?" originally scheduled for March 3, 2009 has been rescheduled for the fall of 2009. Details on the rescheduled seminar will be announced as the date approaches. Finally, it is anticipated that these regulations may continue to evolve, both in substance with respect to the date(s) of implementation. Please check our website for updates, or contact your MBJ attorney for the most up-to-date information.

Rachel Munoz, Esq. is an attorney with Morgan, Brown & Joy, LLP and may be reached at (617) 523-6666 or at rmunoz@morganbrown.com. Morgan, Brown & Joy, LLP focuses exclusively on representing employers in employment and labor matters.