MB&J | MORGAN BROWN&JOY

www.morganbrown.com

CLIENT ALERT: March 1, 2012 Deadline for Data Security Measures in Third-Party Service Provider Contracts Approaching

Since March 1, 2010, businesses that own or license personal information have been required to comply with the Standards for the Protection of Personal Information of Residents of the Commonwealth ("regulations") established by the Office of Consumer Affairs and Business Regulation ("OCABR"). *See generally, 201 C.M.R. 17.00, et seq.* On March 1, 2012 the final phase of the regulations takes effect, and businesses will need to require by contract that third-party service providers with whom they contract for services or business functions have in place security measures consistent with the regulations.

Background

In 2007, Massachusetts enacted data security laws designed to protect the personal information of residents of Massachusetts. The laws provided for the development of regulations which were intended to ensure the confidentiality of consumer and employee personal information and protect against threats to the security of that information, including unauthorized access to or use of the information.

The regulations apply to every person or business that "owns or licenses, receives, stores, maintains, processes, or otherwise has access to personal information" of a Massachusetts resident. Personal information is defined under the regulations as an individual's first and last name (or last name and first initial) in combination with any one or more of (a) a Social Security number, (b) a driver's license number or Massachusetts identification card number or (c) a financial account number, or credit or debit card number. In light of these provisions, the regulations apply to almost all employers who have personal data of Massachusetts residents, regardless of whether the business is located in Massachusetts. The regulations mandate that employers develop, implement, and maintain a comprehensive written information security program to protect personal information, and put in place certain security measures to safeguard the employer's computer system, including any wireless system. For more on the specifics of the requirements of the regulations, the written information security program ("WISP") and computer system security requirements, please see MBJ's Client Alert dated December 21, 2009.

Third-Party Service Providers

The regulations provide that employers must not only protect the personal information which is in their own possession but also confirm that third-party service providers with whom they contract will implement and maintain appropriate security measures to protect personal information. A service provider, under the regulations, is an entity that is permitted to access personal information through its provision of services to an employer covered by the law; examples would include an information technology service provider or a provider of payroll or staffing services.

Employers are required to take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect personal information consistent with the Massachusetts regulations and any applicable federal regulations. The regulations also state that employers must require third-party service providers by contract to implement and maintain appropriate security measures to protect personal information.

Compliance Terms in Contracts with Third-Party Service Providers

In deference to the business considerations posed by the requirements on contracts with third-party service providers, the regulations provided a carve-out for contracts which were in existence before the effective date of the regulations. The regulations provide that with respect to contracts entered into before March 1, 2010, the obligation to have in place a contractual requirement that the third-party provider maintain appropriate security measures would not attach until March 1, 2012.

As the March 1, 2012 deadline for ensuring that all contracts with third-party service providers comply with the regulations approaches, employers should examine which of their service providers may have access to employee personal information. Employers should ensure that contracts with these service providers contain provisions requiring the provider to implement and maintain security measures for the protection of personal information which are consistent with the Massachusetts regulations and any applicable federal regulations. If you have questions or concerns about ensuring that service provider contracts meet the requirements of the regulations, or other questions about the data security laws and regulations, please contact your MBJ attorney.

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