Municipalities Must Comply With Portions of Massachusetts Data Security Law

Recently, much has been written about the data security laws and, in particular, the January 1, 2010, deadline for compliance with regulations promulgated by the Office of Consumer Affairs and Business Regulation ("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. (For more information, *see* Morgan, Brown & Joy's previous Client Alert: "Massachusetts Data Security Regulations: Deadline for Compliance Delayed Until January 1, 2010" dated February 17, 2009).

By their terms, the Standards for the Protection of Personal Information of Residents in the Commonwealth ("regulations"), established by the OCABR do not apply to municipalities. On September 19, 2008, Governor Deval Patrick required all state agencies, but not cities or towns, to comply with the regulations.

Although the regulations do not apply to municipalities, other provisions of the Massachusetts Data Security Law do. Chapter 93H of the Massachusetts General Laws imposes a reporting requirement on municipalities. It provides that a "person *or agency* that maintains, or stores, but does not own or license data that includes personal information about a resident of the commonwealth" must provide notice "as soon as practicable and without unreasonable delay" to the attorney general, the director of the OCABR, and any affected Massachusetts resident of a data security breach. Chapter 93H went into effect in October of 2007.

Further, Chapter 93I of the Massachusetts General Laws sets forth the manner in which personal information is to be disposed of and destroyed. Chapter 93I applies to "persons" and "agencies," including cities and towns, and sets forth the "minimum standards" for the proper disposal of records containing personal information:

(a) paper documents containing personal information shall be either redacted, burned, pulverized or shredded so that personal data cannot practicably be read or reconstructed;

(b) electronic media and other non-paper media containing personal information shall be destroyed or erased so that personal information cannot practicably be read or reconstructed.

Chapter 93I permits persons and agencies to contract with a third party to dispose of personal information in accordance with this chapter. Any third party hired to dispose of material containing personal information must implement and monitor compliance with policies and procedures that prohibit unauthorized access to personal information during the collection, transportation and disposal of personal information.

A violation of this chapter may result in a civil fine of $100.00 per data subject affected, not to exceed $50,000 for each instance of improper disposal. The Office of the Attorney General has the authority

to enforce both Chapter 93H and Chapter 93I.

Thus, although municipalities are not subject to the regulations, those who are responsible for data security on behalf of municipalities must be sure that their municipality is in compliance with other laws, including Chapter 93H and Chapter 93I. For more information about data security concerns, please contact your MBJ attorney.

Rachel E. Muñoz, Esq. is an attorney with Morgan, Brown & Joy, LLP. Rachel 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.