MANCHEL BRENNAN
COUNSELLORS AT LAW

CLIENT ALERT
(NOVEMBER, 2008)

DEADLINE FOR IMPLEMENTATION OF CERTAIN NEW STANDARDS REGARDING SECURITY OF PERSONAL INFORMATION EXTENDED TO MAY 1, 2009

This week, the Massachusetts Office of Consumer Affairs and Business Regulation extended the deadline for companies to comply with recently-issued regulations which implement a 2007 Massachusetts law regarding the protection of personal information of Massachusetts residents. Companies now have until May 1, 2009, rather than January 1, 2009, to implement the requirements of the regulations. However, it is important to note that the Act, which requires specific written notices of data security breaches and the proper disposal of personal information, has been in effect since October 31, 2007.

What Are These New Regulations?

The new regulations implement the Massachusetts law, "An Act Relative to Security Freezes and Notification of Data Breaches." The Act and the new regulations impact the maintenance of, access to, and disposal of records (in paper, electronic, or other form) that contain "personal information" regarding Massachusetts residents.

Is My Organization Covered?

The Act and the regulations broadly define "personal information" as a Massachusetts resident's first name or initial and last name in combination with any of the following:

- Social security number;
- Driver's license number or state-issued identification card number; or
- Financial account number or credit card number.

Based upon this definition, many Human Resources documents, such as I-9 forms, benefit enrollment forms and direct deposit forms, to name just a few examples, contain "personal information," subjecting the company that maintains them to the Act and the regulations. Almost every Massachusetts employer is covered by the Act and the regulations. Thus, Human Resources professionals, operations professionals, and Information Technology professionals all need to become familiar with the Act and the regulations, and act now to be sure to meet the May 1st deadline for compliance.

What Is Required?

In combination, the Act and the new regulations require the following: (1) implementation and documentation of a security program; (2) assessment of the computer system security in place and implementation of additional safeguards, if necessary; (3) specific notices in the event of a breach of the security or confidentiality of personal information or the system in which such information is housed; and (4) proper disposal of documents and records that contain personal information.

(1) Implementation Of A Security Program (eff. 5/1/09)

Every entity or person who owns, licenses, stores or maintains personal information of a Massachusetts resident must develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records which contain personal information. The program must be "reasonably consistent" with "industry standards" and must have administrative, technical, and physical safeguards to ensure the security and confidentiality of the records which contain personal information.

The regulations state that, at a minimum, the program must contain aspects:

- designating one or more employees to maintain the program;

- identifying and assessing any reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of the records, and evaluating and improving, where necessary, the effectiveness of the current safeguards to limit such risks;

Manchel & Brennan, P.C., 199 Wells Ave, Suite 301, Newton, MA, 02459 Tel 617-796-8920 Fax 617-796-8921 www.manchelbrennan.com

- developing security policies for employees that take into account whether and how employees should be allowed to keep, access, and transport records containing personal information outside of business premises;

- imposing disciplinary measures for violations of the program rules;

- preventing terminated employees from accessing records containing personal information, including deactivating their passwords and user names;

- taking reasonable steps to verify that third-party service providers with access to personal information have the capacity to protect such information;

- limiting the amount of personal information collected to that reasonably necessary to accomplish the legitimate purpose for which it is collected, limiting the time such information is retained, and limiting access to those persons who are reasonably required to know such information;

- identifying paper, electronic, and other records, computing systems, and storage media, including laptops and portable devices used to store personal information, to determine which records contain personal information;

- implementing reasonable restrictions upon physical access to records containing personal information;

- regular monitoring to ensure the program is operating in a manner reasonably calculated to prevent unauthorized access to or unauthorized use of personal information, and upgrading information safeguards as necessary to limit risks;

- reviewing the scope of the security measures at least annually and whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and

- documenting responsive actions taken in connection with any incident involving a breach of security, and mandatory post-incident reviews of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

(2) Computer System Security (eff. 5/1/09)

In addition to the above requirements, with respect to electronically stored or transmitted personal information, the security program must establish and maintain a security system covering computers and computer systems, including any wireless systems. The requirements for computer security are too numerous to address comprehensively in this Client Alert. In general terms, however, the computer system security requirements include authentication and access protocols for personal information stored electronically; firewall protections; security agent software; and, "to the extent technically feasible," encryption of records and files containing personal information which will travel across public networks and encryption of all data to be transmitted wirelessly or stored on laptops or other portable devices. Also, importantly, the regulations require that companies provide education and training of employees on the proper use of the computer security system and the importance of personal information security. All companies with employees in Massachusetts should work with their Information Technology professionals to review compliance with this requirement.

(3) Notice Of Breach (eff. 10/31/07)

The Act requires that any person or entity holding personal information must provide specific notices when they know or have reason to know of a security breach. A security breach is any unauthorized access to or use of the personal information. The exact contents of the notices vary; however, notices must be provided to the Attorney General, the Director of Consumer Affairs and Business Regulation, and the Massachusetts residents affected by the breach.

(4) Destruction Of Personal Information (eff. 10/31/07)

Finally, the Act details minimum standards for the proper disposal of paper documents and electronic media containing personal information. In general terms, the Act requires that when documents or media containing personal information are disposed of, they must be destroyed in a manner such that personal information cannot be discerned or reconstructed after disposal.

* * * * *

We hope that this information is useful. Please feel free to contact us if you have any questions or if we can be of any assistance.