

## **Client Advisory - Aggressive New Massachusetts Data Breach Law and Proposed Security Rules Require Company Action**

*Edwards Angell Palmer & Dodge*, February 1, 2008

Mark E. Schreiber, Robert G. Young

Massachusetts has become one of the most aggressive states in the country regarding protecting personal data. It has adopted a new data breach law, a new document destruction law and proposed regulations that may represent one of the most far-reaching information security requirements anywhere in the U.S.

Taken together, these will have major compliance implications and will likely require more rigorous, written security policies for any company doing business in Massachusetts or holding Massachusetts personal data, wherever located. The state's Office of Consumer Affairs and Business Regulation ("OCABR") has proposed a broad security regulation to implement the data breach law, and set relevant standards to be met by such businesses.

No industry sector or business size that has personal information, as defined, is exempted from these Massachusetts laws or proposed regulations. Thus, a range of businesses, not previously subject to regulation, will have to adhere to these rules and begin constructing or enhancing information security, incident response, data breach and data destruction policies. Certain retail, financial services, insurance, third party administrators, accounting and other employers or consumer service entities, whether or not previously subject to the Gramm-Leach-Bliley safeguards rule or the HIPAA security regulations, will have new obligations in Massachusetts.

The new Massachusetts data breach law, effective October 31, 2008, also creates new compliance obligations for companies when personal information of Massachusetts residents is improperly accessed and disclosed. Massachusetts is now the 39<sup>th</sup> state with a data breach law, joining states including New York, New Jersey, Rhode Island, Connecticut, Delaware and Florida.

Any data breach usually requires an evaluation of various states' breach laws because the potentially compromised consumer or employee data is rarely limited to one state. The Massachusetts law will require a breach notice in Massachusetts different from that in other states. See the linked article: "[Corporate Obligations Under The State's New Data Breach Law](http://www.eapdlaw.com/newsstand/)" under Articles/Whitepapers at <http://www.eapdlaw.com/newsstand/>. New electronic document destruction obligations also come into force on February 3, 2008 under another section of the Massachusetts law.

### **Highlights of New Data Breach Law**

New Mass. Gen. Laws Ch. 93H applies to any business entity or person that owns, licenses, maintains or stores "personal information" of any Massachusetts resident, regardless of where the entity or the personal information is located. Out-of-state businesses are subject to this act if Massachusetts resident data is affected.

"Personal information" is a person's first name and last name (or first initial and last name) in combination with any one of: (1) Social Security number; (2) driver's license number or other state-issued identification card number; or (3) a financial account number, or credit or debit card number, with or without any required security code, access code, or PIN that would allow account access.

A "breach of security" under Ch. 93H is an unauthorized acquisition or unauthorized use of personal information of Massachusetts residents that creates a substantial risk of identity theft or fraud against a Massachusetts resident.

A covered entity must provide notice "as soon as practicable, and without unreasonable delay" after that entity knows or has reason to know that its notice obligations have been triggered by a security breach. There is a delay exception if law enforcement determines that the breach notice may impede a criminal investigation and has notified the Mass. Attorney General of this determination.

The data owner (which may be an employer) must provide notice to the Mass. Attorney General, the Director of OCABR and each affected Massachusetts resident. The data storer (in the employment context, for example, a third party administrator) must give notice to the data owner.

The data owner's notice to the Attorney General, the Director of OCABR, and any applicable consumer reporting agencies or state agencies must include the nature of the breach, the number of Massachusetts residents affected, and any steps the data owner has taken or plans to take relating to the incident.

The data owner's notice to individual Massachusetts residents must include information concerning the individual's right to obtain a police report and how to request a security freeze on their consumer report and related fees.

Unlike many other states, the data owner's notice to Massachusetts individuals is prohibited from containing information concerning the nature of the breach, unauthorized acquisition or use or the number of residents affected.

### **Highlights of New Data Destruction Law**

New Ch. 93I, on disposition and destruction of records, expands the definition of personal information in Ch. 93H to also include biometric indicators, and requires that:

Paper documents containing personal information be redacted, burned, pulverized or shredded so that personal information cannot practically be read or reconstructed.

Electronic media and other non-paper media containing personal information be destroyed or erased so that personal information cannot practically be read or reconstructed.

Third parties who handle such disposal on behalf of businesses also implement policies and procedures that prohibit unauthorized access to the personal information.

Fines for violation up to \$100 per data subject affected and up to a maximum of \$50,000 for each instance of improper disposal may be imposed.

### **Highlights of New Proposed Security Regulations**

The planned new security regulation requires that companies adopt a comprehensive, written information security program applicable to any records containing such personal information and which is reasonably consistent with industry standards.

The proposed regulation details specific data and computer system security requirements (*e.g.*, use of 128-bit data encryption, including for wireless communications, firewalls, anti-spyware, audit trails, and access blocks for multiple failed login attempts).

There are also requirements for data minimization, records inventory, security for telecommuters, disciplinary rules for inappropriate access, and mandatory education and training of relevant staff.

The policy, which applies to paper and computer records, must be reviewed annually and contain other administrative, technical, and physical safeguards.

The planned regulations are meant to ensure the security and confidentiality of information in a manner consistent with industry standards, and protect against anticipated threats or hazards to data security or integrity. Numerous objections, however, have been submitted to OCABR, criticizing the proposed regulations.