



## **OVERVIEW OF THE NEW MASSACHUSETTS DATA SECURITY LAWS<sup>1</sup>**

In the wake of the 2007 TJX data breach and the rash of identity thefts that ensued, the Massachusetts legislature enacted two laws. Chapter 93H, which went into effect at the end of 2007, requires prompt notification of unauthorized acquisition or use of Massachusetts residents' "Personal Information" to the Attorney General, the Office of Consumer Affairs and Business Regulation (OCABR), and the resident(s) affected. Chapter 93I, which went into effect at the beginning of 2008, prescribes the manner in which such "Personal Information" must be discarded or destroyed.

Most recently, under the authority granted under Chapter 93H, the OCABR promulgated 201 C.M.R. 17.00, a significant set of regulations designed to further protect residents' Personal Information. The new regulations, which go into effect January 1, 2010, require businesses to develop, implement, and maintain a comprehensive, written data security program ("Program"). These new regulations will have a significant impact on every employer in Massachusetts.

This document is intended to give a brief overview of the new laws and regulations and to outline some considerations for Massachusetts employers.

### **A. PROTECTION OF "PERSONAL INFORMATION"**

All three of the new laws are intended to protect "Personal Information," which is defined as a combination of:

1. A Massachusetts resident's first name or initial *and* last name, plus
2. Any of the following numbers:
  - (a) Social Security number;
  - (b) Driver's license number or state-issued identification card number; or
  - (c) Financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number, or password, that would permit access to a resident's financial account...

M.G.L. c. 93H, § 1; M.G.L. c. 93I, § 1 (which also includes "biometric indicator[s]"); 201 C.M.R. 17.02.

---

<sup>1</sup> This document was prepared for educational purposes only. It should not be relied on as legal advice. Consult with counsel before making any decisions with respect to the issues discussed in this document.

Based on this definition, the new laws clearly apply to all employers of Massachusetts residents, not just companies processing credit card transactions. Every employer has Personal Information concerning its employees, including employment applications, tax forms, immigration forms, payroll information, benefits forms, and direct deposit authorizations. It also covers certain vendor information and other information that businesses may collect in the course of their operations.

## **B. REQUIREMENTS OF THE LAW**

The new Massachusetts data security rules require every business that stores, maintains, owns, or licenses Personal Information:

1. To have a program to safeguard Personal Information,
2. To dispose of Personal Information in specific ways, and
3. To give specific notification in case of a breach of data security.

### **1. Program to Safeguard Personal Information**

By January 1, 2010, every businesses must “develop, implement, maintain and monitor a comprehensive, written information security program applicable to any records containing ... personal information.” The Program requires an employer to do at least the following:

- Appoint an employee or employees to maintain the Program
- Identify all Personal Information owned, stored, licensed, or maintained (or treat every record as Personal Information)
- Identify risks to the Personal Information and evaluate current safeguards
- Limit the amount of Personal Information collected/maintained to accomplish the legitimate purpose for which it is collected/maintained
- Limit the time Personal Information is retained to that reasonably necessary to accomplish the purpose for which it is collected/maintained
- Limit access to Personal Information to those reasonably required to know
- Develop written security policies for electronic and physical files
- Impose disciplinary measures for employees who violate policies
- Verify that third-party service providers with access to Personal Information have the capacity to protect it and in fact are protecting it
- Implement computer system security requirements, detailed in 201 CMR 17.04
- Regularly monitor Program and review at least annually

How will you know if your Program is in compliance?

- The regulation provides that compliance will be judged by:
  - Size, scope and type of business
  - Resources available
  - Amount of stored data
  - Need for security and confidentiality
- Ultimately, whether or not an entity is deemed to be in compliance will depend on the unique facts and circumstances.s

## **2. Disposal of Personal Information**

Massachusetts General Laws Chapter 93I, which is in effect now, requires each business to meet the following minimum standards for proper disposal of records containing Personal Information:

- Paper documents must be redacted, burned, pulverized, or shredded so that Personal Information cannot practicably be read or reconstructed
- Electronic media and other non-paper media must be destroyed or erased so that Personal Information cannot practicably be read or reconstructed.

Violations can lead to civil penalties of \$100 per data subject, not to exceed \$50,000 per instance. Violators may also be liable under Chapter 93A, potentially subjecting noncompliant persons to injunction, restitution, civil penalties, and liability for the cost of the investigation and litigation of the violation, including attorney's fees.

## **3. Actions required in the event of a data security breach**

Massachusetts General Laws Chapter 93H, which is in effect now, requires notification to the Attorney General and OCABR in the event of a breach of security or unauthorized use or acquisition of Personal Information.

Notification must occur "as soon as practicable and without unreasonable delay" and "shall include, but not be limited to, the nature of the breach of security or unauthorized acquisition or use, the number of residents of the commonwealth affected by such incident at the time of notification, and any steps the person or agency has taken or plans to take relating to the incident." The resident must also be notified, unless law enforcement instructs you not to do so.

Breaches are considered violations of Chapter 93A, potentially subjecting noncompliant persons to injunction, restitution, civil penalties, and liability for the cost of the investigation and litigation of the violation, including attorney's fees.

## **C. CONSIDERATIONS FOR EMPLOYERS**

Steps that employers should take immediately:

- Assemble an internal data security team, with members from Operations, Human Resources, Information Technology, Accounting, Sales and Legal.
- Educate data security team on the requirements and details of the new laws and regulations.
- Perform assessment of Personal Information, with participation of entire team.
- Adopt proper administrative, technical, and physical security measures and enact required Program.
- Adopt a data security breach action plan.
- Ensure third-party service provider compliance
- Destroy old data that is no longer needed and implement a document destruction policy

Some employer-specific considerations for the Program required by 201 C.M.R. 17.00:

- Personnel files
  - Change employer-generated forms to exclude Personal Information
  - Segregate/redact name from other protected information
- Employee Handbook/Training
  - Create and publish policies regarding data security
  - Train all employees on such policies
  - Impose discipline for violations
  - Eliminate expectations of employee privacy. Notify employees that their electronic activities on company computers can and will be monitored by the company. Generally notify of other surveillance methods.
- Employee Contracts
  - Change to include obligation not to use or misappropriate others' Personal Information
- Implement/Improve Monitoring of Employees' Access
  - Must be able to trace an employee's steps
  - Electronic monitoring of downloads and views
  - Key-card access/security cameras
- Work-at-Home/Employee-Owned Computers
  - Evaluate and update policies as required
  - Restrict access
- Employee Exit Procedures
  - Immediate removal of employee's electronic and physical access
  - Check monitoring systems for unauthorized views/downloads of Personal Information
- Independent Contractors
  - Must be treated as third-party vendors
  - Contract and certification
- Insurance
  - Assess whether current E&O policy would cover the damages and expenses of a data security breach
  - Consider specific coverage for data security