



**HIRSCH
ROBERTS
WEINSTEIN LLP**

ATTORNEYS AT LAW

C. MAX PERLMAN
(617) 348-4326
max@hrwlawyers.com

ANDREA C. KRAMER
(617) 348-4380
akramer@hrwlawyers.com

DAVID B. WILSON
(617) 348-4314
dwilson@hrwlawyers.com

ERIN D. REED
(617) 348-4385
ereed@hrwlawyers.com

**THE NEW DATA SECURITY LAWS AND REGULATIONS:
AN OVERVIEW FOR MASSACHUSETTS EMPLOYERS¹**

In the wake of the 2007 TJX data breach and the rash of identity theft that ensued, the Massachusetts legislature enacted two laws. Chapter 93H, which went into effect at the end of 2007, requires notification of unauthorized acquisition or use of Massachusetts residents' "Personal Information" to be made promptly to the Attorney General, the Office of Consumer Affairs and Business Regulation (OCABR) and the resident(s) affected. Chapter 93I took effect at the beginning of 2008, and 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, et seq., a significant and controversial set of regulations designed to further protect residents' Personal Information. The new regulations, effective May 1, 2009, require that businesses develop, implement and maintain a comprehensive, written data security program. These new regulations will have a profound and immediate impact on every employer in Massachusetts, as attempts to comply will be expensive and time-consuming.

This document and the accompanying presentation and materials are intended to give a brief overview of the new laws and regulations, and outline some considerations for Massachusetts employers.

A. PROTECTION OF "PERSONAL INFORMATION"

The new laws and regulations are intended to protect "Personal Information." "Personal Information," is defined as a combination of:

1. A Massachusetts resident's first name and last name or first initial and last name; and
2. Any of the following:
 - (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...

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



M.G.L. c. 93H, § 1, M.G.L. c. 93I, § 1 (incorporating also “biometric indicator[s]”), 201 C.M.R. 17.02.

It is clear from the definition of “Personal Information” that the new laws and regulations apply to all employers of Massachusetts residents, not just companies processing credit card transactions, like TJX or Hannaford. Every employer has Personal Information concerning its employees, including employment applications, tax forms, immigration forms, payroll information, benefits forms and direct deposit authorizations.

B. REQUIREMENTS OF THE LAW

Requirements of the new laws and regulations:

1. Program to safeguard Personal Information
2. Procedure for disposal of Personal Information
3. Actions required in the event of a data security breach

1. Program to Safeguard Personal Information

201 CMR 17.00, et seq. (included in materials) requires that by May 1, 2009, 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, in very abridged terms:

- 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 amount of Personal Information collected/maintained to accomplish the legitimate purpose
- Limit time Personal Information is retained to that reasonably necessary to accomplish such purpose
- 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
- 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 Office of Consumer Affairs and Business Regulation (OCABR) gives a little help; published a guide for small businesses and a compliance checklist (both are included in the materials). Neither of these documents are a substitute for the detailed analysis that must be done.

- The regulation provides for scalability:
 - 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.

2. Disposal of Personal Information

Massachusetts General Laws Chapter 93I (included in materials) requires each agency or person to meet the following minimum standards for 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; and
- (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.

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 (included in materials), which is in effect now, requires notification of 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." Also must notify the resident, 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 quasi-audit of Personal Information, with participation of entire team.
- Adopt proper administrative, technical and physical security measures and enact Program as required by 201 CMR 17.00, et seq.
- Adopt a Data Security Breach Action Plan.

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. Notify, generally, 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
 - Reconsider policies
 - 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 policy for data security