

# OVERVIEW OF MASSACHUSETTS DATA SECURITY LAWS

---

MCLE

*Navigating the New Federal and Massachusetts Data Security Laws*

September 17, 2009

Andrea C. Kramer

Hirsch Roberts Weinstein LLP

[www.hrwlawyers.com](http://www.hrwlawyers.com)



# Data Security Breaches

---

Boston Globe - 2006

Veterans Administration - 2006

TJX - 2007

Hannaford Bros. - 2008

BNY Mellon - 2008

Heartland Express - 2009

# Data Security Breaches

---

There are about 8 million victims of identity theft each year in the United States.

Over 263 million records containing sensitive personal information have been involved in security breaches in the United States since January 2005

Source: [www.privacyrights.org](http://www.privacyrights.org)

# What is Identity Theft?

---

Fraud that involves someone pretending to be someone else in order to steal or wrongfully obtain money or to get other benefits

- Use of another person's credit without authorization – account takeover
- Use of another person's identity to open a credit account – application fraud or true name fraud

# Massachusetts' Response

---

- Breach notification law - Chapter 93H
  - Effective October 31, 2007
- Data destruction/disposal law - Chapter 93I
  - Effective February 3, 2008
- Data security regulations - 200 C.M.R. 17.00
  - Final regulations initially issued September 2008
  - Effective date March 1, 2010

# Breach Notification Law

---

## Overview

Requires specific information in notification to

- Attorney General,
- Office of Consumer Affairs
- affected individuals

of

- data security breaches
- unauthorized use or acquisition of Personal Information

# Breach Notification Law

---

## To Whom Does Law Apply?

Individuals, Businesses, Government Agencies

That “License or Own” or “Store or Maintain”

“Personal Information”

# Personal Information

First Name or  
First Initial

+

Last Name

&

Social Security #

or

Driver's License #

or

State-Issued ID Card #

or

Credit Card #

or

Debit Card #

or

Financial Account #

# Breach Notification Law

---

## Notice Requirements

Detailed list of information to be included in notice with different requirements for

- Businesses That “License or Own”
- Businesses That “Store or Maintain”

# Breach Notification Law

---

## Notice Requirements

Notice by mail or “substitute notice” if

- Cost will exceed \$250,000, or
- Affected class exceeds 500,000 residents, or
- Do not have sufficient contact information

Substitute notice:

- Email
- Website
- Publication in statewide media

# Breach Notification Law

---

## What Triggers Requirement?

Person or agency knows or has reason to know

- of “Breach of Security” or
- that Personal Information
  - was acquired or used by an unauthorized person, or
  - was used for an unauthorized purpose

# Breach Notification Law

---

## Penalties/Enforcement

Attorney General may bring Chapter 93A action:

- Civil penalties up to \$5,000 for each violation
- Costs of investigation and litigation, including attorneys fees
- Restitution

# Breach Notification Law

---

## Compliance with Federal Law

A business that maintains procedures for responding to a security breach that comply with federal laws, rules, regulations, guidance, or guidelines will be deemed to be in compliance if it provides notice in compliance with those procedures

Must still notify Attorney General and Director of Consumer Affairs.

# Breach Notification Law

---

## Other States' Laws

45 states, the District of Columbia, Puerto Rico, and the Virgin Islands have enacted breach notification laws.

Most protect financial information, but some also protect medical information.

States have differing notice requirements for timing, content, and recipients.

Links to laws: [www.ncsl.org/default.aspx?tabid=13489](http://www.ncsl.org/default.aspx?tabid=13489)

# Breach Notification Law

---

## Massachusetts Data Security Breaches

October 2007 to December 2008

### 368 Notifications

321 by businesses

23 by educational institutions

24 by state government

### 626,004 Mass. Residents Affected

### Cause of Breach

220 from criminal activity

Remainder from employee error or sloppy internal handling

# Data Destruction/Disposal Law

---

## Chapter 93I – effective February 2008

All persons, businesses, agencies

must destroy records containing Personal Information

“such that the data cannot practicably be read or reconstructed after disposal or destruction”

# Data Destruction/Disposal Law

---

## Definition of Personal Information

Broader under Chapter 93I  
(Data Destruction/Disposal Law)  
than under 93H (Breach Notification Law)

Includes biometric identifiers

# Data Destruction/Disposal Law

---

## Paper Records

Must be  
Redacted,  
Burned,  
Pulverized, or  
Shredded

## Electronic Media

Must be  
Destroyed or  
Erased

# Data Destruction/Disposal Law

---

## Third Party Disposal Service Provider

Must implement and monitor

compliance with policies and procedures

that prohibit unauthorized access to, acquisition of, or  
use of Personal Information

during collection, transportation, and disposal

# Data Destruction/Disposal Law

---

## Penalties/Enforcement

- Civil fine of up to \$100 per data subject affected, up to \$50,000 for each instance of improper disposal
- Attorney General action under Chapter 93A
  - Civil penalties up to \$5,000 for each violation
  - Costs of investigation and litigation, including attorneys fees
  - Restitution

# Data Security Regulations

---

## Purpose/Objectives

- To insure the security and confidentiality of customer information in a manner fully consistent with industry standards
- To protect against anticipated threats or hazards to the security or integrity of such information
- To protect against unauthorized access to or use of such information that may result in substantial harm or inconvenience to any consumer.

# Data Security Regulations

---

## Coverage and Overview

Apply to all persons and businesses that  
“own or license” Personal Information

“Own or license”: Receive, maintain, process, or have access to Personal Information in connection with provision of goods or services or employment

Establish minimum standards to be met in connection with the safeguarding of Personal Information contained in both paper and electronic records

# Data Security Regulations

---

## The Basic Requirement

Every person and business that  
owns or licenses Personal Information shall  
“develop, implement, and maintain”  
a “comprehensive information security program”  
 (“The Program”)

# Data Security Regulations

---

## The Program

Must be

- Written in one or more readily accessible parts
- Consistent with the safeguards for protection of Personal Information set forth in any state or federal regulations to which Owner/Licensors is subject

# Data Security Regulations

---

## Risk-Based Approach

Administrative, technical, and physical safeguards appropriate to

- Size, scope, and type of business
- Amount of resources available to business
- Amount of data stored
- Need for security and confidentiality of both consumer and employee information

# The Program

---

## Specific Requirements

- Designate employee(s) to maintain Program
- Identify and assess reasonably foreseeable internal and external risks
- Evaluate and improve (where necessary) effectiveness of current safeguards for limiting risks
- Develop security policies for employees for storage, access, and transportation of Personal Information

# The Program

---

And ...

- Impose disciplinary measures for violations
- Prevent terminated employees from accessing records
- Oversee service providers
- Reasonably restrict physical access to, and storage of, records containing Personal Information

# The Program

---

And ...

- Regularly monitor Program and upgrade safeguards as necessary
- Review scope of security measures at least annually or whenever there is a material change in business practices
- Document responsive actions taken after any breach and conduct post-incident review of events and actions taken

# Data Security Regulations

---

## Oversee Service Providers

- Take reasonable steps to select and retain third-party service providers that are capable of maintaining appropriate security measures to protect Personal Information
- Require third-party service providers by contract to implement and maintain such security measures

# Data Security Regulations

---

## Computer System Security

To the extent technically feasible, must have

- “Secure user authentication protocols”
- “Secure access control measures”
- Encryption
- Reasonable monitoring
- Reasonably up-to-date firewall and malware protection, security patches, and virus definitions