

# WAYNE, RICHARD & HURWITZ LLP

ATTORNEYS AT LAW  
ONE BOSTON PLACE  
BOSTON, MASSACHUSETTS 02108  
(617) 720-7870

## **LEGAL ADVISORY** **COMPLIANCE DEADLINE – MARCH 1, 2010**

- The Issues:** Identity Theft  
Confidentiality of Financial Records  
Misuse and Protection of Personal Data
- The Legislation:** Massachusetts Data Security Laws -  
Mass. Gen. Laws Chapters 93H and 93I; 201 CMR 17.01 *et seq.*
- Upcoming  
Compliance  
Deadline:** March 1, 2010 (for compliance with Data Security Regulations)
- Who Is Affected:** ALL Businesses that Receive, Maintain, Process or have Access to  
“Personal Information” about a Massachusetts resident
- What is “Personal  
Information”:** Personal Information is defined as:  
A First Name or Initial and a Last Name, AND any one of the  
following:
- Social Security number
  - Driver’s License number
  - State-Issued ID Card number
  - Credit Card number
  - Debit Card number
  - Financial Account number
- Who Must Comply:** All persons, business and agencies - if your business has  
employees or accepts payment by check or credit/debit card, the  
laws apply to you. Examples of this include but are not limited to:
- Stores – processing and storing credit card or bank  
account numbers of Massachusetts residents
  - Restaurants / Hotels – processing reservation  
information using credit card or bank account numbers;  
information transmitted across wireless networks  
offered to patrons/guests
  - Professional Offices – maintaining payroll information  
of staff residing in Massachusetts; employees’ and  
clients’ Personal Information stored on work computers

- Commercial Enterprises – processing mortgage, loan or applications for Massachusetts residents; customer/client information

**What Must Be Done:**

Under M.G.L. Ch. 93H - Breach Notification Law:  
Businesses must make notifications whenever Personal Information is acquired or used by an unauthorized person or for an unauthorized purpose.

Under M.G.L. Ch. 93I - Data Destruction/Disposal Law:  
Whenever records are destroyed or disposed, records containing Personal Information must be rendered such that “the data cannot practicably be read or reconstructed after disposal or destruction”.

Under 201 CMR 17.01 et seq. - Data Security Regulations  
EFFECTIVE MARCH 1, 2020

- Every person / business that owns or licenses Personal Information shall “*develop, implement, and maintain*” a “*comprehensive information security program*” (“The Program”).
- The Program must be in writing.
- An individual must be designated to manage and maintain the Program.
- The Program must be implemented, reviewed and modified as needed.

**Possible Penalties:**

- Civil fine of up to \$100 per data subject affected, up to \$50,000 for each instance of improper disposal
- Civil penalties up to \$5,000 for each violation
- Costs of investigation and litigation, including attorney’s fees
- Restitution

WHAT THREE STEPS SHOULD BE TAKEN IMMEDIATELY AND BEFORE MARCH 1, 2010:

1. Appoint an **Information Security Manager**.
2. Write and approve a written **Information Security Policy**.
3. Your Information Security Manger must **help your staff carry out** the Information Security Policy, and **audit compliance regularly**.

*Wayne, Richard & Hurwitz LLP can advise you in determining the best Security Program or Electronic Security Program for your business and assist you with drafting a Policy and implementing a Program.*