

*New Legal Requirements for  
Electronic Storage of Personal Information  
in Massachusetts*

Presented by:

*David M. Felper, Esq.*

*Bowditch & Dewey*



- I. Background/History
- II. Document Retention Requirements For HR Information Under Federal & State Laws
- III. Massachusetts Data Protection Law
- IV. New Regulations Effective March 1, 2010
- V. Third-Party Service Provider Regulations
- VI. Damages For Non-Compliance
- VII. Enforcement

# Background/History

## Recent High-Profile Security Breaches

### The TJX Companies:

- Massachusetts-based retailer with approx. 2,500 stores.
- Computer system first breached in July 2005 by hackers who placed unauthorized computer software on TJX's computer system, gaining access to information from customer transactions dating to January 2003.
- Information from 45.7 million cards was stolen from transactions from January through November 2003; TJX did not discover breach until late 2006.
- 455,000 customers who returned merchandise without receipts had their personal data stolen, including driver's license numbers.
- TJX settled in late 2007 and early 2008 with issuing banks of Visa and MasterCard for \$40.9 million and \$24 million, respectively.
- TJX reached an agreement with the FTC in April 2008 to immediately upgrade and implement comprehensive data security procedures and to submit to outside audits.
- In August 2008, 11 individuals were indicted for crimes in connection with what the Justice Department described as "the single largest and most complex identity theft case ever charged in this country."

# Background/History

## Recent High-Profile Security Breaches

### Hannaford Brothers Company:

- Maine-based supermarket chain with 165 stores in the Northeast.
- Security breach began in December 2007.
- Credit card numbers were stolen when shoppers swiped their cards and the information was transmitted to banks for approval
- Estimated 4.2 million credit and debit card numbers were exposed.
- The thefts occurred despite Hannaford's compliance with the Data Security Standards promulgated by the Payment Card Industry (PCI)—which do not require companies to encrypt data at the point of sale—raising doubts about the sufficiency of the PCI standards and merchants' reliance on them.
- 1,800 cases of reported fraud related to the breach.

# *Background/History*

## Impact of High-Profile Security Breach Cases

- Massachusetts and at least five other states have enacted or strengthened laws imposing liability on merchants in the event of a data breach.
- In 2008, five more states enacted breach notification laws, bringing the total number of states with such laws to 44.
- In addition to increasing merchant accountability in the event of a data breach, Massachusetts has enacted legislation intended to prevent the occurrence of such breaches.
- The Massachusetts Office of Consumer Affairs and Business Regulation (“OCABR”) released new rules in September 2008, which were mostly recently modified in August 2009. (Details about the new rules will be discussed in Part IV).
- The new rules, now effective March 1, 2010, are more specific than any other state’s data security regulations.
- Regulations like those enacted in Massachusetts likely signal a trend among the states, particularly with respect to data encryption.

# *To Whom Do Regulations Apply?*

- Entities Engaged In Commerce.
- More Specifically, To Entities Who Collect And Retain Personal Information As Part Of Provision Of Goods Or Services, Or For Employment Purposes.
- Agencies, Offices And Departments Of The Commonwealth Are Specifically Excluded From Coverage, As Are Municipalities.

# Document Retention Requirements For HR Information Under Federal & State Laws

## What Documents Need To Be Retained and For How Long?

A variety federal and state laws and regulations impose recordkeeping and records retention obligations on businesses. The following are among those that affect businesses broadly:

- FLSA –Employers are required to retain certain personnel records of non-exempt employees, such as payroll records and employment contracts, for a period of **3 years**. Other personnel records of non-exempt employees, such as timesheets, wage rate tables, and additions to or deductions from wages paid must be kept for a period of **2 years**. 29 C.F.R. §§ 516.2-516.6 and 516.11-29.
- Massachusetts Law- Employers must keep accurate records of the name, complete address, social security number and occupation of *each* employee, of the amount paid each pay period to each employee, the hours worked each day and the dates on which each employee worked each week. Such records must be kept on file for at least **2 years** after the entry date of the record. G.L. c. 151, § 15; 455 C.M.R. § 2.06(2).
- Civil Rights Act and Equal Pay Act - Employers covered by this act must maintain personnel records of hiring, promotion, demotion, termination, transfer, layoff, pay raises, et al. for **6 months** from the making of the record. The records must also be maintained until final disposition of any discrimination case. 29 C.F.R. § 1602.14

# Document Retention Requirements For HR Information Under Federal & State Laws

- ADEA – Employers must make and preserve records of employees and of the wages, hours, and other conditions and practices of employment necessary for the enforcement of the provisions of the ADEA. 29 U.S.C. §§ 201-219
- IRS - Employers should keep copies of employment tax records for **4 years** after the due date of the tax. 26 C.F.R. § 31.6001
- OSHA - Employers must retain records of both medical and other employees who are exposed to toxic substances and harmful agents for **30 years**. 29 C.F.R. § 1903 *et seq.*
- Title VII of the Civil Rights Act of 1964 – Employers subject to the act must retain records relevant to the determinations of whether unlawful employment practices have been committed. 42 U.S.C. 2000e *et seq.*
- ERISA - any employer that has an employee benefit or pension plan must retain relevant records for at least **6 years**. 29 U.S.C. Chapter 18.
- Welfare and Pension Plans Disclosure Act - records must be retained for **5 years**. 29 U.S.C. Chapter § 308
- HIPAA - employers are required to ensure the confidentiality, integrity and availability of all electronic protected health information they maintain. Pub. L. No. 104-191.

# *Massachusetts Data Protection Law*

- In addition to high-profile breaches such as TJX and Hannaford, there were more than 200 reported data breaches in 2008 alone at entities such as colleges and universities, hospitals, insurance companies, government agencies and financial institutions.
- In response to the increasing prevalence and scope of data security breaches, Massachusetts has joined 38 other states in enacting a data protection law which governs the security and disposal of “personal information” of its residents.
- For purposes of the law, “personal information” means a first name or initial and a last name, plus a Social Security, financial account, driver’s license or credit/debit card number.
- Risk-based approach to information security.

# Massachusetts Data Protection Law

- The first stage of the law, Chapter 93H, which became effective on October 31, 2007, requires notification to residents and state authorities if personal information is improperly accessed or used.
- The second stage of the law, Chapter 93I, which became effective on February 3, 2008, mandates destruction of hard copy and electronic data containing personal information, such as might be found in employee personnel records.
- The new data destruction law sets forth minimum standards for proper disposal of paper or electronic records containing personal information, including employee personnel records.
- Under the new law, "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.*"

# *Encryption Requirements For Portable Devices*

- Encryption Of Portable Devices Containing Personal Information Of Customers Or Employees Is Required, BUT Only If Technically Feasible.
- “Technically Feasible” Means If There Is A Reasonable Means Through Technology To Accomplish The Required Result.
- Backup Tapes That Are Transported From Current Storage Must Be Encrypted If It Is Technically Feasible.

# *New Regulations Effective March 1, 2010*

- The OCABR released new and amended rules that will require any person or entity who owns, licenses, stores or maintains personal information about Massachusetts residents to:
  1. Develop, implement, maintain and monitor a *comprehensive, written information security program*; and
  2. Meet specific information security requirements.
- The rules, now effective March 1, 2010, are more specific than any other state's data security regulations, and compliance will likely require changes for most businesses and organizations.

# *New Regulations Effective March 1, 2010*

## What Is A Comprehensive, Written Information Security Program?

- The regulations do not provide a specific definition for “a comprehensive, written information security program.” However, the regulations provide a non-exhaustive list of requirements that all organizations storing personal information electronically must comply with.
  
- Accordingly, under the new regulations, all entities that store personal information electronically must have in place a comprehensive, written information security program that requires them to:
  1. Regularly monitor the program and designate an individual to maintain the program;
  2. Identify and assess internal and external risks to information security;
  3. Take steps to ensure that contractors maintain safeguards for personal information;
  4. Limit the amount of information shared and the persons with whom that information is shared to what is reasonably necessary to accomplish legitimate purposes;
  5. Ensure that passwords used by each person with computer access reasonably maintain system security;
  6. Encrypt all personal information stored on laptops or other portable devices;
  7. Maintain reasonably up-to-date firewall protection for systems connected to the Internet, and system security agent software;
  8. Train employees and impose disciplinary measures for security violations;
  9. Review scope of security measures at least annually or if material change in business practices that could compromise security; and
  10. Document responsive actions taken in connection with any security breach.

# *New Regulations Effective March 1, 2010*

## Compliance With The New Regulations

- The enormous scope of the required new “comprehensive information security program” will require organizations to perform a wide-ranging and time-consuming survey of how they handle personal information.
- Whether a businesses’ comprehensive information security program is in compliance with the new regulations will depend on several factors, such as:
  1. The size, scope and type of business;
  2. The amount of resources available to the business;
  3. The amount of data stored by the business; and
  4. The need for security and confidentiality of both consumer and employee information.
- Although the effective date of the new regulations has been extended, it is rapidly approaching! In order to get ready, organizations need to address gaps in their internal processes, and identify outside vendors who have access to personal information, right away.

# Third-Party Service Provider Regulations

- Under the new data destruction law, entities *are permitted* to contract with a third-party to destroy paper and/or electronic documents containing PI. However, *any third-party hired to dispose of material containing PI must implement and monitor compliance* with policies and procedures that prohibit unauthorized access to or acquisition of or use of PI during the collection, transportation and disposal of PI.
- The new regulations issued by the OCABR require persons and entities who own, license, store or maintain PI about a resident of the Commonwealth to:
  1. Take all reasonable steps to verify that any third-party service provider with access to PI has the capacity to protect such personal information in the manner provided for in the regulations; and
  2. Take all reasonable steps to ensure that such third-party service provider is utilizing such protective security measures at least as stringent as those required to be applied to PI under the regulations.
- The deadline for compliance with the amended third-party service provider regulations has been extended to March 1, 2010.
- The most recent amended regulations added back in the specific language requiring you to *contractually bind* your third-party service providers to implement and maintain appropriate measures for protecting personal information.
- Two-year window to amend all applicable third-party service provider contracts.

# Damages For Non-Compliance

<u>Area of Non-Compliance</u>	<u>Monetary Damages</u>
Unreasonable delay/failure to provide notice of security breach to the attorney general, director of the OCABR and affected resident	\$5,000 fine; reasonable costs of investigation and litigation of such violation, including reasonable attorneys' fees.
Failure to maintain a written, comprehensive information security system	\$5,000 fine; reasonable costs of investigation and litigation of such violation, including reasonable attorneys' fees. (effective 3/01/10)
Improper disposal of records containing PI	\$100 fine per individual affected, maximum of \$50,000 per instance of improper disposal
Failure to take all reasonable steps to verify that third-party service with access to PI has capacity to protect PI	\$100 fine per individual affected, maximum of \$50,000 per instance of improper disposal (effective 3/01/10)
Failure to take all reasonable steps to ensure that third-party service is applying security measures to PI	\$100 fine per individual affected, maximum of \$50,000 per instance of improper disposal (effective 3/01/10)

# *Damages For Non-Compliance*

## Other Potential Claims That May Be Brought By Affected Individuals Against Entities

- **Unfair or deceptive trade practices pursuant to G.L. c. 93A, § 11-** an individual may seek injunctive relief and/or monetary damages, including double or treble damages, attorneys' fees and costs.
- **Negligence-** an individual may seek actual and consequential damages against a non-compliant entity under a common law negligence theory (punitive damages are not available in Massachusetts under an ordinary negligence theory).

# *Enforcement*

- The Attorney General of Massachusetts is responsible for enforcement of the new laws.
- The Attorney General may file a civil action in the superior or district court in the name of the Commonwealth to recover fines or obtain injunctive relief against an entity for non-compliance.
- Any district attorney or law enforcement officer receiving notice of any alleged violation of the new laws must immediately forward written notice of same, along with any relevant information, to the Attorney General.

*Thank you!*

David M. Felper  
Bowditch & Dewey, LLP  
dfelper@bowditch.com

Audrey Baker  
Networks Unlimited, Inc.  
audrey@NetworksUnlimited.com