



# Navigating the New MA Data Security Regulations

*Robert A. Fisher, Esq.*



# Data Security Law

- Chapter 93H
- Enacted after the TJX data breach became public
- Intended to protect Massachusetts residents from identity theft
- Applies to any business entity that owns, licenses, maintains or stores the “personal information” of a Massachusetts resident
- Effectively covers all businesses with Massachusetts employees, not just consumers

# “Personal Information”

A person’s first name and last name (or first initial and last name) **PLUS** any one of the following:

- Social Security number
- Driver’s license number (or other state issued ID card number)
- A financial account number or credit or debit card number, with or without any required security code, access code or PIN that would allow account access

# Data Security Law

- Statute requires notice to be given in the case of a data breach
- Notice should be given “as soon as practicable and without reasonable delay” to
  - Affected individuals
  - Massachusetts Attorney General
  - Director of Consumer Affairs and Business Regulation
- Breach of security is
  - Unauthorized acquisition or unauthorized use of personal information of Massachusetts residents that creates a substantial risk of identity theft or fraud against a Massachusetts resident
  - Examples include theft or loss of computer hardware, misuse of company information by a current or former employee, or incomplete destruction of records

# The Regulations

- All businesses with “personal information” must develop a “comprehensive, written information security program” by January 1, 2010
- Regulations contain specific requirements about what must be contained in the written security plan
- Create a duty of care
- No “one-size fits all” approach; plan must be tailored to your business
- May not require reinventing the wheel, but need to be systematic and document your current practices

# The Regulations

- Create a floor, not a ceiling
- Comply with other laws or legal obligations
- Reasonably consistent with industry practice
- Compliance also depends upon
  - Size, scope and type of business
  - Resources of the business
  - Amount of stored data
- But have to meet certain minimum requirements

# Designate a Security Officer

- Recommend designating a single person to be responsible
- May require input from a number of areas
  - IT
  - Legal
  - Human Resources
  - Outsourcing
  - Public Relations
  - Security
  - Records management
  - Operations

## Identify your risks

- Risks are both external and internal
- Regulations contemplate a self-assessment
  - What personal information do you have and where?
  - Who has access to it, who needs access and why?
  - What current safeguards are in place?
  - How effective are those safeguards?
- Safeguards include employee training, policies and procedures & means for detecting security failures
- Expectation is that safeguards will be evaluated and improved
- Concern about setting yourself up to fail

# Develop security policies

- Human resources component
- Should have written policies for employees on how to store, access and transport personal information
- Recognition that employees may be your greatest source of risk
- Establish disciplinary procedures for employees who violate policies
- Procedures for dealing with terminated employees
  - Terminate physical and electronic access
  - Deactivate user names and passwords
  - Return of company property

# Third-Party Service Providers

- Area of real risk of liability
- Many employers use payroll or benefits companies; have personal information
- Must take reasonable steps to verify that the vendor:
  - Has the capacity to protect personal information in the manner provided by the regulations
  - Is applying security measures at least as stringent as those required by the regulations
- No written certification/ contract requirements

# Limits on personal information

- Collect only what is reasonably necessary
- Retain only as long as necessary
- Limit access to employees who are reasonably required to access or retain such information
- Much of this will be addressed in self-assessment/ audit
- Watch out for employees who change jobs

# Physical Access

- Largely a lock and key issue
- Regulations contemplate a written policy on physical access to records

# Monitoring

- Need to review your plan at least annually
- Need to establish an incident response plan
- Document actions taken in response to security breaches
- Mandatory “post-incident” review
- Ensure that the program is operating in a manner “reasonably calculated to prevent unauthorized access or unauthorized use”

# Computer System Security Requirements

- Real area of controversy
- Cover all computers, wireless networks and PDAs
- Question whether these requirements will still be in place by the end of the year

# Secure Access

- Unique user IDs and passwords
- Restrict access to employees who need information
- Monitor system for unauthorized use or access to personal information
- Educate employees on proper use of computer security system and personal information security

# System Security Software

- “Reasonably up-to-date”
  - Malware protection
  - Patches and virus definitions
  - Firewall
  - Operating system patches
- Set to receive “most current” security updates on a regular basis

# Encryption

- “To the extent technically feasible,” all files or records that will travel across a public network or will be transmitted wirelessly must be encrypted
- All personal information stored on laptops or other portable devices must be encrypted

# Remedies

- Office of the Attorney General has authority to enforce statute
- May bring an action under Chapter 93A to remedy violations of the statute
  - Seek injunctive relief
  - Civil penalties of up to \$5000 per violation
  - Costs of the investigation, including attorneys' fees
- Unclear what happens if business fails to comply with regulations

# Private Right of Action?

- Nothing in the statute authorizes a private right of action
- But statute and regulations create minimum standards
- Common law negligence?
- Unfair trade practice under Chapter 93A?
  - Attorneys' fees
  - Treble damages

# Massachusetts Privacy Act (M.G.L. ch. 214, §1B)

- “A person shall have a right against unreasonable, substantial or serious interference with his privacy.”
- The statute permits a plaintiff to bring a claim for damages for invasion of privacy.
- Employers have a limited privilege under Massachusetts law
  - Facts must be highly personal or intimate
  - Employer has business need for disclosure
- But do the Data Security Law and regulations change that standard?