

Regulatory Update:

Protecting Personal Information of Massachusetts Residents

*201 CMR 17.00 Compliance Advisory
and Implementation Support*

Our Presenter



Matthew Pettine, CGEIT, CISA, ASE, MCSE, MSCBA
Managing Director, IT Advisory Practice
MFA Cornerstone Consulting

About MFA

- Proactive CPA and consulting firm with national and global reach
- Founded in 1982
- Nearly 100 professionals, including 14 partners
- Located in Tewksbury, Massachusetts

About MFA

- Audit & Assurance
- Taxation
- Valuation
- Transaction Services
- Accounting Advisory
- Wealth Advisory
- Professional Staffing
- Corporate Governance / Compliance Consulting
- Performance & Controls Consulting
- Fraud & Forensic Accounting
- Litigation Support
- IT Advisory

Defining the Massachusetts Personal Data Security Law

201 CMR 17.00



New Massachusetts Personal Data Security Law

- New law is designed to protect the personal information of Massachusetts citizens
- Intent of law is to prevent personal information from being breached in the first place
 - As opposed to merely addressing what must happen in the wake of a security breach
- Establishes reporting protocol

New Massachusetts Personal Data Security Law

- Personal information to be protected includes:
 - A citizen's name (first & last or first initial & last name) COMBINED with one or more of the following:
 - Credit card number
 - Social security number
 - Financial account number
 - State issued identification number

New Massachusetts Personal Data Security Law

- Applies to individuals and businesses that own, license, store or maintain “personal information” about a citizen of Massachusetts
 - HR Departments – I9s, Background Checks, Direct Deposits, Health and Life Insurance, 401(k)s
 - Companies dealing directly with credit card-based retail sales
 - Financial Services Companies
 - Health Care Providers
 - Real Estate Professionals & Mortgage Providers

Compliance Dates

- Originally it was January 1, 2009
- Delayed to May 1, 2009 with encryption compliance by January 1, 2010
- On February 12, 2009, full compliance date delayed yet again until January 1, 2010

Proposed Amendment

- Senate Bill 173 proposed in January 2009
 - Federal "privacy" standards would supersede MA regulation
 - Requires Massachusetts Office of Consumer Affairs and Business Regulation to adopt regulations relative to data security specifically for small businesses
 - Prohibits the regulation from requiring, "a specific technology or technologies, or a specific method or methods for protecting personal information"
 - Makes a willful violation of a federal or state "privacy law" just cause for the termination of an employee. This provision would apply to both private and public sector employees in Massachusetts

Proposed Amendment

- Federal "privacy" standards would supersede MA regulation
 - Organization would be deemed compliant without additional efforts specifically addressing 201 CMR 17.00
 - Federal Privacy Standards include:
 - HIPPA
 - PCI
 - Some Others

Proposed Amendment

- Small Businesses
 - Requires Massachusetts Office of Consumer Affairs and Business Regulation to adopt regulations relative to data security specifically for small businesses
 - Definition of “small business” to be determined
 - Specific requirements not specified at this time

Proposed Amendment

- Requirements for Specific Technologies
 - Prohibits the regulation from requiring, "a specific technology or technologies, or a specific method or methods for protecting personal information"
 - Current regulations define and require Encryption, Automated System and Definition Updates, "Strong Passwords"
 - Intention is to provide for alternate methods of securing information

Proposed Amendment

- Termination for Cause
 - Makes a willful violation of a federal or state "privacy law" just cause for the termination of an employee
 - This provision would apply to both private and public sector employees in Massachusetts
 - Strengthens policy-based controls
 - Provides some protection for employers
 - Repercussions for non-Mass employers is unclear

Proposed Amendment

- Risk-based Approach
 - Proposal suggests a risk-based approach
 - Comprehensive Data Inventory may be impractical
 - Risk-based approach allows efforts to be concentrated in areas of greatest exposure

Steps to Achieve Compliance

1. Assessment of the organization
 - Assessment of state of current compliance
 - Assessment of information handling processes
 - GAP analysis
2. Create a Written Information Security Plan (WISP)
3. Computer system security
4. Vendor management
5. Training employees
6. Monitoring protocols

Assessment of the Organization

- Assessment of state of current compliance
 - Review governing policies
 - Review existing compliance efforts
- Assessment of information handling processes
 - Identify where Massachusetts residents' information is handled and stored within the business
 - Assess current processes
 - Document key processes
 - Define information retention policies and practices
- GAP analysis
 - Identify risks and develop remediation plan

Written Information Security Plan (WISP)

- Define and document
 - Security coordinator with defined responsibilities
 - Information flows
 - General computer controls
 - Employee training
 - 3rd party vendor process review
 - Document retention and destruction
 - Notification protocols

Computer System Security

- Regulation includes specific requirements related to computer system security
 - Authentication
 - Access controls
 - Data transmission
 - Monitoring
 - Encryption
 - Firewalls & OS patches
 - Viruses & malware
 - Training

3rd Party Vendors

- Must ensure that third party providers have the capacity to protect personal information you give them access to
 - Payroll provider
 - Health insurance broker
 - Background check provider
 - 401(k) provider
 - Providers of business production services
 - Cleaners & disposal crews

Training Employees

- Law requires organizations to train their employees on an ongoing basis
 - Training event evidence and administration
 - Develop training materials
 - Conduct training sessions

Develop Monitoring Protocols

- Exception handling procedures
 - Internal / employees
 - External threats
 - Notification process
- Annual review and maintenance

Additional Resources

- **The new Massachusetts Personal Data Security Law**
 - <http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf>
- **Massachusetts Senate Bill 173**
 - <http://www.mass.gov/legis/bills/senate/186/st00pdf/st00173.pdf>
- **An MFA Perspective Article on the new Massachusetts Personal Data Security Law**
 - <http://www.mfa-cpa.com/mfa-news-and-resources/thought-leadership/Perspective-MA-Privacy-Law.pdf>
- **MFA Web Seminar Presentation on the new Massachusetts Personal Data Security Law**
 - http://www.mfa-cpa.com/mfa-news-and-resources/thought-leadership/ma_privacy_form.asp
- **Understand how MFA can help in your efforts toward compliance: MFA's Privacy and Data Protection Services**
 - <http://www.mfacornerstone.com/Solutions/IT-Advisory/MFAPrivacyAndDataProtectionServices.pdf>

Questions

Thank You!

Matthew Pettine
mpettine@mfacornerstone.com
978-557-5354

Michelle Mackey
mmackey@mfacornerstone.com
978-569-2909

MFA Cornerstone Consulting

IRC Circular 230 Disclosure: To ensure compliance with requirements imposed by the IRS, we inform you that any U.S. federal tax advice contained in this communication (including any attachments) is not intended or written to be used, and cannot be used, for the purpose of (i) avoiding penalties under the Internal Revenue Code or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.