Protecting Personal Information: The Massachusetts Data Security Regulation (201 CMR 17.00)

May 15, 2009
US Information Security Framework

- Historically industry-specific
  - HIPAA
  - Fair Credit Reporting Act
  - Gramm-Leach-Bliley
  - COPPA
  - PCI DSS

- Role of FTC
  - FTC Act § 5 (unfair trade and deceptive practices)
  - Enforcement actions

- State regulation
  - 44 states have security breach notification law
  - Consumer protection “Little FTC Acts”
  - Protection of specific types and uses of information (e.g., SSNs)
  - Reasonable measures to protect personal information (9 states)
MA Regulation (201 CMR 17.00)

• Overview
  – Adopted under Massachusetts Security Breach Law (M.G.L. c. 93H)
  – Office of Consumer Affairs and Business Regulations (“OCABR”)
  – Enforced by the Attorney General

• Scope
  – Any person who “owns, licenses, stores or maintains” personal information about a MA resident
    • Applies to individuals and entities
    • Not limited to Massachusetts companies
  – Paper and electronic records containing Personal Information
Personal Information Definition

- First Name/First Initial AND Last Name PLUS
  - Social Security Number
  - Driver’s License Number
  - State-issued ID Card Number
  - Financial Account Number
  - Credit or Debit Card Number

- Public Information Exception
  - Excludes information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public
Comprehensive Information Security Program

• Governance
  – Individual or Committee

• Risk Assessment
  – Employee training
  – Compliance with policies and procedures
  – Detecting and preventing system failures

• Administrative, Technical, Physical Safeguards

• Service Provider Process
  – Vetting Process
  – Ensure security at least as stringent as Regulation

• Ongoing Evaluation
Administrative Safeguards

• Information Security Policies
  – Document the Comprehensive Information Security Program
• Data Inventory
  – Identify paper and electronic records containing Personal Information
• Data Minimization & Retention
  – Collect and retain Personal Information only to extent reasonably necessary
• Need-to-Know Access
  – Limit access to Personal Information to those reasonably required to have access for a legitimate business or legal purpose
• Employee Management
  – Implement training, compliance monitoring, and disciplinary measures for employees
• Security Incidents
  – Document and assess incidents and incident response
Technical Safeguards

• User Authentication
  – Control of user IDs and passwords

• Access Controls
  – Restrict access to system resources

• Encryption
  – Encrypt Personal Information if:
    • stored on laptops and portable devices (CDs, DVDs, thumb drives)
    • transmitted over wireless systems and across public networks to the extent feasible

• Monitoring
  – Monitor systems for unauthorized access or use

• Antivirus Controls, Security Patching, Firewalls
  – Reasonably up-to-date versions
Physical Safeguards

• Maintain reasonable physical access restrictions on records containing Personal Information

• Develop a written procedure for physical access controls

• Store Personal Information in locked facilities, storage areas or containers

• Terminate former employees’ physical access immediately
Potential Consequences of Non-compliance

- **Attorney General Enforcement**
  - Under state consumer protection statute (M.G.L. c. 93A)
  - Injunctive Relief
  - Civil penalties of up to $5,000 per violation

- **Breach Context**
  - Basis for liability and penalties

- **Separate Penalties under Related MA Legal Requirements**
  - Disposal of Records (M.G.L. c. 93I)
  - Breach Notification Statute (M.G.L. c. 93H)
Interpretation

• Evaluation Factors
  – Size, scope, and type of business
  – Amount of resources available
  – Amount of stored data
  – Need for security and confidentiality

• Objectives
  – Be consistent with industry standards
  – Protect against anticipated threats or hazards
  – Protect against unauthorized access that creates a substantial risk of identity theft or fraud

• Other Considerations
  – Program must be reasonably consistent with industry standards
  – Safeguards must be consistent with applicable state or federal regulations
Interpretation (cont.)

• Interpretation From Enforcement Actions
• Potential Sources for Compliance Purposes
  – Statements by OCABR
  – Guidance from other regulatory bodies
    • Regulatory bodies work closely together
    • FTC Guidance
• Concept of “Reasonable Security”
  – Mitigating controls
  – Commercially available products
  – Vendor supplied security patches
  – Following through on existing security measures
If you have questions…

- OCABR Website
  
  http://www.mass.gov

- Ropes & Gray LLP
  
  http://www.ropesgray.com/privacydatasecurity/

Christine Santariga
Tel: 617.951.7185
Email: christine.santariga@ropesgray.com

Mit Spears
Tel: 202.508.4681
Email: mit.spears@ropesgray.com