

# Standards for the Protection of Personal Information of Residents of the Commonwealth

*201 CMR 17.00 Compliance Advisory  
and Implementation Support*

# Seminar Logistics

- All attendees are muted during the presentation
  - We cannot hear you
- Audio difficulties
  - Hang up and redial 213-286-1201
  - Enter access code 654-569-214
  - Enter the Audio Pin displayed on your Attendee Control Panel
- We will take questions at end of presentation
  - During presentation you may type questions into the Question Screen on your Attendee Control Panel – click **Send Privately**

# About MFA

- Proactive CPA and consulting firm with national and global reach
- Founded in 1982
- Nearly 100 professionals, including 13 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

# Our Presenters



Richard Pacheco, CFE, AVA, CIA, MBA

*Partner and Managing Director*

MFA Cornerstone Consulting



Matthew Pettine, CGEIT, CISA, ASE, MCSE, MSCBA

*Managing Director, IT Advisory Practice*

MFA Cornerstone Consulting

# Scoping the Massachusetts Privacy Law



# A Perspective: Identity Theft Facts

- 40% of business costs for individual cases of identity theft exceed \$15,000
- An estimated \$221+ billion a year is lost by businesses worldwide due to identity theft
- Victims lose an average of \$1,820 to \$14,340 in wages dealing with their cases
- Victims spend an average of \$851 to \$1378 in expenses related to their case

# Landmark Breaches

- Data security breaches at major companies
  - **Boston Globe** – 240,000 subscriber numbers (2006)
  - **Monster.com** – 1.3 million job seeker info (2007)
  - **TJX** – 94 million credit cards (2007)
  - **Hannaford Supermarkets** – 4.2 million credit cards (2008)
  - **Countrywide** – 2 million credit cards (2008)
  - **Heartland Payment Systems** – as of 1/22/09 a potential for 100 million card numbers being stolen!

# The Origins of the Massachusetts Law

- Through October 2008, the State received 318 notifications of information breaches, effecting 325,000 Massachusetts citizens in 2008
  - 60% due to criminal behavior
  - 75% of data not encrypted or password protected

# Defining the Massachusetts Privacy Law

*201 CMR 17.00*



# New Massachusetts Privacy and Data Protection 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 Privacy and Data Protection 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 Privacy and Data Protection 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

# Failure to Comply \$\$

- If an information breach occurs, and no prescribed information security efforts were in place – companies will be subject to both criminal and civil penalties
- Fines established under Massachusetts General Law 93H
  - Civil penalty of \$5,000 per each violation
  - Up to a \$50,000 fine for each instance of improper disposal of information

# Other Consequences of Non-Compliance

- Damage to reputation if security breach occurs
- Significant time, resources and costs required to properly handle a security breach

# Becoming Compliant

# Steps to Achieve Compliance

---

1. Assessing state of current compliance
2. Assessing information handling processes
3. Encryption & data protection
4. Vendor management
5. Training employees
6. Monitoring protocols

# Assessing the Organization

# Assessing Your Organization

1. Assess your organization's current state of compliance
  - Review governing policies
  - Identify where Massachusetts residents' information is handled and stored within the business

# Assessing Your Organization

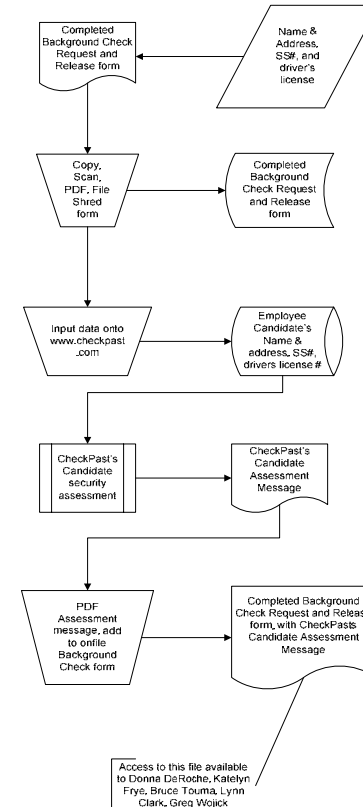
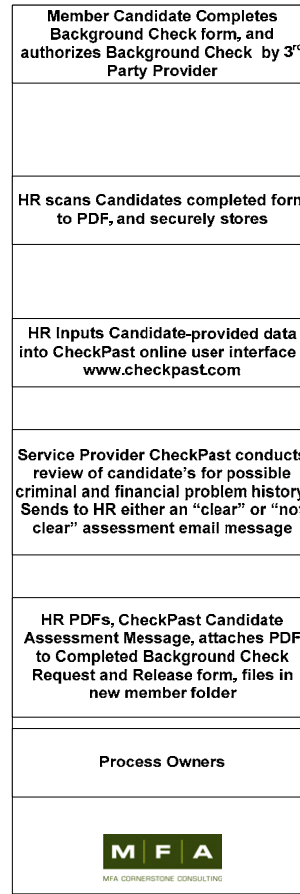
- Create a Written Information Security Plan (WISP)
  - Designate a security coordinator
  - Identify information flows – how they start, what is the process, where information is stored, who has access, how long data is stored, how is data destroyed
  - Conduct demonstrable employee training
  - Develop written employee consequences for non-adherence
  - Encrypt personal data on laptops and other portable storage devices
  - Ensure general network security
  - Obtain assurances that 3<sup>rd</sup> party providers have adequately safeguarded personal information

# Assessing Your Organization

2. Assess your organization's information handling processes
  - Assess current processes
  - Document the key processes
  - Define information retention policies & practices
  - **BOTTOM LINE: Be Prudent!**
    - Limit the information that is collected
    - Don't keep the information any longer than you need it

# Assessing Your Organization

## Information Process Flow



# Encryption & Data Protection

# Encryption & Data Protection

---

- Only Proactive State Breach Regulation
- Specific Technology-related Requirements

# Encryption & Data Protection

- Regulation includes specific requirements related to computer system security
  - Authentication
  - Access Controls
  - Data Transmission
  - Monitoring
  - Encryption
  - Firewalls & OS Patches
  - Viruses & Malware
  - Training

# Encryption & Data Protection

- Authentication
  - Control of User Accounts
    - “Control of IDs”
    - “Reasonably secure passwords”
    - Control of password security
    - Restrict access to active users
    - Block access after multiple attempts

# Encryption & Data Protection

- Access Controls
  - Restrict access to those who “need to know” to perform their jobs
    - File system security / permissions
    - Third-party tools available
  - Assign IDs and passwords
    - Unique (not shared)
    - “Not vendor supplied defaults”

# Encryption & Data Protection

- Data Transmission
  - Encryption of transmitted data
    - “Where technically feasible”
      - Web Sites (SSL / https)
      - Email (PGP / 3<sup>rd</sup> party services)
      - Remote Access Solutions
      - Online Service Providers
      - Wireless (“All Data”)

# Encryption & Data Protection

- Monitoring

- “Reasonable monitoring of systems for unauthorized use of or access to personal information”
  - Intrusion Detection
  - Application Logs
  - Server Firewalls
  - Network Security Logs
  - File System Auditing

# Encryption & Data Protection

- Encryption of Personal Information Stored on Portable Devices
  - Laptops
    - Encryption vs. Passwords
    - File-based vs. Entire Laptop
    - Operating System vs. Third Party Solutions
  - “Other Devices”
    - Portable Hard Drives (USB devices)
    - Backup Media
    - CDs, DVDs, Blackberries, PDAs

# Encryption & Data Protection

- Firewalls & OS Patches
  - Firewall Protection
    - “Reasonably up-to-date”
    - Vendor supported and routinely updated
  - Operating System Security Patches
    - Automatic update features
    - Servers & workstations
    - User considerations

# Encryption & Data Protection

- Viruses & Malware
  - “Reasonably up-to-date versions”
  - “Must include malware protection”
  - Supported by vendor
    - Up-to-date patches and definitions
    - “Set to receive the most current security updates on a regular basis”

# Encryption & Data Protection

- “Education and training of employees on the proper use of the computer security system and the importance of personal information security.”
  - New hire orientation
  - Specific routine organizational efforts

# Assessing 3<sup>rd</sup> Party Vendors, Training Employees & Monitoring Compliance

# Assessing 3<sup>rd</sup> Party Vendors

- Must ensure that third party providers have the capacity to protect personal information you give them access to
  - Health insurance broker
  - Background check provider
  - 401(k) provider
  - Providers of business production services
  - Cleaners & disposal crews
- Conduct due diligence
- Make safeguards a condition of your contract with them
- Secure a reasonable level of surety by January 1, 2010

# Training Employees

- Law requires organizations to train their employees on an ongoing basis
  - Training sessions need to be documented
  - Employee attendance at training sessions needs to be documented as well
  - Sanctions for violations need to be clear and contain disciplinary measures
  - Measures must be in place to prevent terminated employees from accessing records containing personal information

# Monitoring Compliance

- Ensuring employee training
- Executing on violations in a demonstrable and evidenced manner
- Regular review of policies for relevancy
- Reviewing organizational adherence to established operational protocol

# Q & A

# Further Information

- Contact MFA to discuss the new law and its affect on your organization
  - Richard Pacheco  
[rpacheco@mfacornerstone.com](mailto:rpacheco@mfacornerstone.com)  
978-557-5332
  - Matthew Pettine  
[mpettine@mfacornerstone.com](mailto:mpettine@mfacornerstone.com)  
978-557-5354

# Further Information

- *The new Massachusetts Privacy Law*
  - <http://www.mass.gov/Eoca/docs/idtheft/201CMR17amended.pdf>
- *An MFA Perspective article on the new Massachusetts Privacy Law*
  - <http://www.mfa-cpa.com/mfa-news-and-resources/thought-leadership/Perspective-MA-Privacy-Law.pdf>
- *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>

# 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.*