

# New Regulations on the Rise

**Richard E. Mackey, Jr.**

**Vice President, SystemExperts  
Corporation**

**dick.mackey@systemexperts.com**

**Sponsored By:**



# Agenda

- **Evolving regulatory requirements**
- **Red Flag Rules**
- **The Massachusetts ID theft law**
- **The Nevada Data Protection law**
- **Frameworks and programs**

# Evolving Regulatory Requirements

- **Every year new regulations appear**
- **Current regulations are interpreted differently**
  - Audit processes change
  - Enforcement changes
- **Regulations tend to focus on specific information, risk, or mitigation**
  - HIPAA – EPHI
  - Red Flag rules: identity theft detection
  - MA & NV Law: identity theft prevention
  - PCI: prevention of payment card information theft
- **Our job: recognize applicable regulations and come into compliance**

# Similarities & Differences

- **Many regulations have many similar requirements**
  - Governance
  - Risk assessment
  - Evaluation of effectiveness
  - Management of service providers
  - Documentation
- **This makes adapting to new regulations easier**
- **The challenge is to identify requirements specific to a regulation and fold them into a framework**
- **We'll look at three recent regulations for commonalities and differences**
  - Red Flag Rules
  - MA identity theft law
  - NV data protection law

# Red Flag Rules

- **FTC administered**
- **Designed to detect attempts to steal identity**
- **Apply to creditors maintaining “covered accounts”**
  - Banks
  - Finance companies
  - Automobile dealers
  - Mortgage brokers
  - Utility companies
  - Telecommunications companies
  - Anyone who extends credit
- **Require processes to recognize specific types of events that may signal (raise red flags) attempts to steal identity**
  - Suspicious address changes
  - Activities on known stolen identities
  - Suspicious activities on accounts (inactive accounts)
  - Suspicious documents

## RFR Covered Accounts

- **The Red Flag Rules apply to institutions that maintain “covered accounts”**
- **Definition: (1) an account primarily for personal, family, or household purposes, that involves or is designed to permit multiple payments or transactions, or (2) any other account for which there is a reasonably foreseeable risk to customers or the safety and soundness of the financial institution or creditor from identity theft.**
- **In other words, both individuals and companies**

## RFR: Required Elements

- **Maintain a written Program**
- **Identify relevant Red Flags for covered accounts and incorporate those Red Flags into the Program**
- **Detect Red Flags that have been incorporated into the Program**
- **Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft**
- **Ensure the Program is updated periodically, to reflect changes in risks to customers or to the safety and soundness of the financial institution or creditor from identity theft**

# RFR: Program Requirements

- **Acquire BoD approval ensuring oversight of the development, implementation, and administration of the Program**
- **Conduct risk assessments to identify whether the institution holds covered accounts**
- **Train staff**
  - Ensure that staff knows requirements of program and can execute responsibilities competently
- **Oversee service providers**
  - Ensure that service providers have good identity theft prevention practices
  - Require service providers to recognize and respond to red flags

## RFR: Good News and Bad News

- **Most financial institutions have these mechanisms in place**
- **Many smaller organizations do not**
- **Challenges:**
  - Documentation
  - Governance
  - Specific requirements of service providers

# MA ID Theft Law

- **201 CMR 17 is a regulation protecting personal identifying information of Massachusetts residents**
- **Requires**
  - Administrative controls
  - Written Information Security Program (WISP)
  - Governance
  - Processes to assess risk, respond to incidents, address vulnerability
  - Encryption
  - Control of service providers
- **Applies to persons or organizations that “own, license, store or maintain personal information about a resident of the Commonwealth of Massachusetts”**

## MA Law: Personal Information

- **First name and last name or first initial and last name in combination with any one or more of**
  - Social Security number
  - Driver's license number
  - State-issued identification card number
  - Financial account number
  - Credit or debit card number
- **With or without any required security code, access code, personal identification number or password, that would permit access to a resident's financial account**

## MA Law Governance

- **Organizations need to appoint a responsible party to run the program**
- **Organizations need to have a written program**
  - Policies
  - Controls in place, processes and technology
  - Lifecycle: Plan, Do, Check, Act

## MA Law: Administrative Controls

- A method for identifying, assessing, and treating risks
- A method for improving effectiveness of security controls
- A policy and procedure for disciplinary action in the event of policy infringement
- A reliable method of terminating access when employees leave or are fired
- A methodology to verify that third party service providers will take adequate steps to secure the personal information entrusted to them
- Training program

## MA Law: Technical Controls

- **Vulnerability management**
- **Encryption of portable devices / laptops**
- **Encryption of all records transmitted over untrusted networks**
- **Access controls**
- **Lockout after failed authentication**
- **Internet firewalls**
- **Monitoring of access**

## MA Law: Good News & Bad News

- **MA Law controls are consistent with HIPAA and ISO 27000**
- **A good security/compliance program would have these controls in place**
- **Challenges:**
  - **Unbounded applicability – all organizations and their service providers are responsible for compliance directly – HITECH Act similarly expands HIPAA**
  - **WISP – A document describing the structure and controls for the program**

# NV Data Protection Law

- **Nevada Revised Statute 603A is a regulation protecting personal identifying information of Nevada residents**
- **Requires**
  - Reasonable security mechanisms
  - Contracts with service providers
  - Notification of breach
  - PCI DSS compliance for all organizations that accept credit cards
  - Encryption of data transmitted outside the secure system of the data collector
  - Encryption of storage beyond the logical or physical controls of the data collector
- **Applies to any “data collector” that handles, collects, disseminates, or otherwise deals with nonpublic personal information**

# NV Law: Personal Information

- **First name and last name or first initial and last name in combination with any one or more of**
  - Social Security number
  - Driver's license number
  - State-issued identification card number
- **Account number, credit card number or debit card number, with any required security code, access code or password that would permit access to the person's financial account**
- **NOT the last four digits of a social security number or publicly available information that is lawfully made available to the general public**

## NV Law Governance

- **Vague reference to “security policy” in notification**
- **Piggybacks on PCI for merchants**
- **Refers to GLB for compliance requirements**
- **No standalone specification**

## NV Law: Good News & Bad News

- **No requirements for governance, policies, or prescriptive controls (except encryption)**
- **Specifically deals with data outside the secure boundaries of the data collector**
- **Challenges:**
  - **PCI DSS Compliance – vague reference accepts a payment card in connection with a sale of goods or services**
  - **May expand PCI compliance beyond what is contractually required today**

## How To Comply

- **Identify the affected information**
- **Understand the compliance requirements specific to the regulation**
- **Fold the specific requirements into the various sections of your existing program**
- **If you don't have a centralized compliance program, implement one**

# Compliance Program & Frameworks

- **ISO 27001&2 provide an excellent framework for compliance**
  - 27001 provides the lifecycle process
  - 27002 provides the list of potential controls
- **Model is based on information and risk**
  - Identify assets (identity info for RFR and MA Law)
  - Assess risks in your environment
  - Choose and implement controls (as you determine and as regulations dictate)
  - Monitor effectiveness of control
  - Respond to problems and improve system/program
- **This approach will fulfill the needs of all regulations and contracts**
  - PCI, HIPAA, GLB, etc.

# Summary

- **Two recent regulations focus on identity theft**
  - RFR focus on processes to detect and prevent
  - MA Law focuses on administrative and technical controls
  - NV Law requires “reasonable measures”
- **Program should contain:**
  - Governance
  - Risk assessment
  - Documentation
  - Lifecycle
- **A good framework-based compliance program will allow you to adapt to regulations like these and others as they appear**

## Thanks to our Sponsor



[Automated Linux Lock Down - Free Trial Download](#)