

## GLB Act

Financial Modernization Act of 1999  
known as  
Gramm-Leach-Bliley (GLB) Act  
Section 501 (b)



# Agenda

- GLB Act Definition
- GLB Act Timeline
- GLB Act – Privacy Rule
- GLB Act – Security Standards
- GLB Act – Policy Requirements



# GLB Act Definitions

- Financial Institution
  - Any institution the business of which is engaging in financial activities
  - Under GLB Act, an institution must be “significantly engaged” in financial activities to be considered a “financial institution”



# GLB Act Definition

- Financial Activities
  - Engaging in an activity that the Federal Reserve Board has determined to be closely related to banking:
    - Extending credit and servicing loans
    - Collection agency services
    - Real estate and personal property appraising
    - Check guaranty services
    - Credit bureau services
    - Real estate settlement services
    - Leasing real or personal property



# GLB Act Definition

- Examples of “financial institutions” that engage in “financial activities”
  - Mortgage lender or broker
  - Check casher
  - Pay-day lender
  - Credit counseling service and other financial advisors
  - Providers that establish long-term payment plans that involve interest charges
  - Retailers that issue credit cards
  - Auto dealers that lease and/or finance
  - Collection agency services
  - Sale of money orders, savings bonds, or travelers checks
  - Government entities that provide financial products such as student loans or mortgages



# GLB Act Definition

- If a “financial institution” is “significantly engaged” is a flexible standard
- Examples of businesses that are not “significantly engaged” for GLB Act:
  - Retailer that does not issue its own credit card
  - Grocery stores that allow cash back by writing a check
  - Merchant who allows an individual to “run a tab”



# GLB Act Definition

- Consumers
  - An individual who obtains or has obtained a financial product or service from a financial institution that is to be used primarily for personal, family, or household purposes, or that individual's legal representative.
- Customers
  - A consumer who has a continuing relationship with a financial institution



# GLB Act Definition

- Nonpublic Personal Information
  - Personally identifiable financial information:
    - Provided by a consumer to a financial institution
    - Resulting from any transaction with the consumer or any service performed for the consumer; or
    - Otherwise obtained by the financial institution
  - Publicly available information is not included



# GLB Act Definition

- Customer Information Systems
  - Any methods used to access, collect, store, use, transmit, protect, or dispose of customer information
- Service Provider
  - Any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the financial institution.



# GLB Act Timeline

- Reform and modernize the banking industry
- Signed November 12, 1999
- Title V, Subtitle A
  - “Disclosure of Nonpublic Personal Information”
    - Privacy of Consumer Financial Information
    - Standards for Safeguarding Customer Information
    - Interagency Guidelines Establishing Standards for Safeguarding Customer Information



# GLB Act Timeline

- Privacy of Consumer Financial Information
- Privacy Rule
  - Issued
    - May 12, 2000
  - Effective
    - November 13, 2000
  - Full Compliance Required
    - On or before July 1, 2001



# GLB Act Timeline

- Standards for Safeguarding Customer Information
- Security Standards
  - Advance Notice of Proposed Rulemaking
    - September 7, 2000
  - Proposed Rule
    - August 7, 2001
  - Final Rule
    - May 23, 2002
  - Compliance
    - On or before May 23, 2003



# GLB Act Timeline

- Interagency Guidelines Establishing Standards for Safeguarding Customer Information
- Policy Requirements
  - Final Rule
    - February 1, 2001
  - Effective Date
    - July 1, 2001
  - Two-year Grandfathering of Agreements with Service Providers
    - July 1, 2003



# GLB Act – Privacy Rule

- Addresses privacy notices, opt out rights and limits on use & disclosure
- Requires notice to consumers of a financial institution's privacy policies and practices
- Requires information security program for safeguarding Customer information
- Affords consumers right to prevent sharing of their information with 3rd parties under certain circumstances



# GLB Act – Security Standards

- Information Security Program
  - Develop, implement, and maintain a written information security program
  - Contain administrative, technical, and physical safeguards
  - Appropriate to size and complexity, the nature and scope of activities, and the sensitivity of the customer information
  - Reasonably designed to achieve the objectives



# GLB Act – Security Standards

- Objectives
  - Insure the security and confidentiality of customer information
  - Protect against any anticipated threats or hazards to the security or integrity of such information
  - Protect against unauthorized access to or use of information that could result in substantial harm or inconvenience to any customer



# GLB Act – Security Standards

- Required Elements
  - Designate an employee to coordinate information security program
  - Identify reasonably foreseeable internal and external risks
  - Assess the sufficiency of safeguards in place to control these risks



# GLB Act – Security Standards

- Required Elements (continued)
  - Risk Assessment needs to include:
    - Employee training and management
    - Information Systems
      - Network and software design
      - Information processing
      - Storage, transmission and disposal
    - Detecting, preventing and responding to attacks, intrusions, or other systems failures



# GLB Act – Security Standards

- Required Elements (continued)
  - Design and implement information safeguards to control the risks identified in the risk assessment
  - Regularly test or monitor the effectiveness of the safeguards' key controls, systems, and procedures



# GLB Act – Security Standards

- Required Elements (continued)
  - Oversee Service Providers
    - Take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards
    - Requiring service providers by contract to implement and maintain such safeguards



# GLB Act – Security Standards

- Required Elements (continued)
  - Evaluate and adjust information security program
    - Based on testing and monitoring
    - After material changes to operations or business arrangements
    - After other circumstances that may have a material impact on the information security program



# GLB Act – Policy Requirements

- Standards for Safeguarding Customer Information
  - Information Security Program
    - Implement a comprehensive written information security program
    - Includes administrative, technical, and physical safeguards
    - Appropriate to the size and complexity of the financial institution and the nature and scope of its activities



# GLB Act – Policy Requirements

- Standards for Safeguarding Customer Information (continued)
  - A security program shall be designed to:
    - Ensure the security and confidentiality of customer information
    - Protect against any anticipated threats or hazards to the security or integrity of such information
    - Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer



# GLB Act – Policy Requirements

- Development and Implementation of Information Security Program
  - Involve the Board of Directors
    - Approve the written information security program
    - Oversee the development, implementation, and maintenance of the information security program



# GLB Act – Policy Requirements

- Development and Implementation of Information Security Program (continued)
  - Access Risk
    - Identify reasonably foreseeable internal and external threats
    - Assess the likelihood and potential damage of these threats
    - Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks



# GLB Act – Policy Requirements

- Development and Implementation of Information Security Program (continued)
  - Manage and Control Risk
    - Design information security program to control the identified risks
    - Train staff
    - Regularly test the key controls, systems and procedures of the information security program



# GLB Act – Policy Requirements

- Development and Implementation of Information Security Program (continued)
  - Oversee Service Provider Arrangements
    - Exercise appropriate due diligence in selecting service providers
    - Require service providers by contract to implement appropriate measures
    - Monitor service providers to confirm that they have satisfied their obligations



# GLB Act – Policy Requirements

- Development and Implementation of Information Security Program (continued)
  - Adjust the Program
    - Monitor, evaluate and adjust as appropriate
  - Report to the Board
    - At least annually
    - Describe the overall status of the information security program



# Resources

- Federal Financial Institutions Examination Council (FFIEC)  
[www.ffiec.gov](http://www.ffiec.gov)
- Federal Deposit Insurance Corporation (FDIC)  
[www.fdic.gov](http://www.fdic.gov)
- National Credit Union Administration  
[www.ncua.gov](http://www.ncua.gov)
- Maine Association of Community Banks  
[www.mecb.com](http://www.mecb.com)



# Questions?

Patrick A. Morin, CPA, CISM

Principal

Baker Newman & Noyes

Information Technology Consulting Division

(800) 244-7444

[pmorin@bnn CPA.com](mailto:pmorin@bnn CPA.com)

