Introduction

- A financial institution's most significant asset is not money: It's information about money, transactions and customers
- Protection of those information assets is necessary to establish the required trust for the institution to conduct business
- Institutions have a responsibility to protect their client's information and privacy from harm such as fraud and ID theft

The Gramm-Leach-Bliley Act (GLBA)

- Signed into law by President Clinton in 1999
- Also known as the Financial Modernization Act of 1999
- Meant to allow banks to engage in a wide array of financial services
- Banks can now merge with stock brokerage companies and insurance companies, which means that they can possess large amounts of private, personal client information

The Gramm-Leach-Bliley Act (GLBA) Cont.

- Title 5 of the GLBA specifically addresses protecting both the privacy and the security of non-public personal information (NPPI)
  - Privacy Rule
    - Limits the financial institutions disclosure of NPPI to unaffiliated third parties
  - Security Guidelines
    - Address safeguarding the confidentiality and security of customer NPPI and ensuring proper disposal of NPPI

The Gramm-Leach-Bliley Act (GLBA) Cont.

- What is NPPI?
  - Stands for non-public personal information
  - Includes the following information:
    - Names
    - Addresses
    - Phone numbers
    - Income and credit histories
    - Social Security numbers

What Is a Financial Institution?

- ***Financial institution*** is "Any institution the business of which is significantly engaged in financial activities as described in *Section 4(k) of the Bank Holding Company Act* (12 U.S.C. § 1843(k)."
- GLBA also applies to companies that provide financial products and/or services such as:
  - Automobile dealers
  - Check-cashing businesses
  - Consumer reporting agencies
  - Courier services
  - Debt collectors

Regulatory Oversight

- Seven federal agencies and the states have authority to administer and enforce the Financial Privacy Rule and Section 501(b)
- Which agency is tasked with enforcing the regulation, along with the severity of the penalty, is dependent upon the industry to which the business belongs
- Nontraditional financial services companies are regulated by the FTC but are not subject to scheduled, regular audits unless a complaint has been lodged against them

What Are Interagency Guidelines?

- The dependence of financial institutions upon information systems is a source of risks
- The interagency guidelines (IG) were created as a way to mitigate those risks related to information being compromised
- The IG require every covered institution to implement a comprehensive written information security program that includes administrative, technical, and physical safeguards

What Are Interagency Guidelines? Cont.

- Information Security Program Requirements
  - Involving the board of directors
  - Assessing risk
  - Managing and controlling risks
  - Overseeing service provider arrangements
  - Adjusting the program
  - Reporting to the board

Involve the Board of Directors

- The board must approve the bank's written information security program
- The board must oversee the development, implementation, and maintenance of the program
- As corporate officials, the board has a fiduciary and legal responsibility
- Banks should provide board members with appropriate training on information security
- The board may in turn delegate information security tasks to other roles and/or committees

Assess Risk

- Risk assessments start by creating an inventory of all information items and information systems
- Identifying threats is the next step
  - Threat: Potential for violation of security
  - Threat assessment: Identification of types of threats
  - Threat analysis: Systematic rating of threats based upon risk and probability
  - Threat probability: Likelihood that a threat will materialize
  - Residual risk: The level of risk after controls have been implemented

Manage and Control Risk

- The information security program should be designed to control the identified risks commensurate with the sensitivity of the information as well as the complexity and scope of its activities:
  - Access controls on customer information systems
  - Access restrictions at physical locations containing customer information
  - Encryption of electronic customer information
  - Separation of duties
  - Monitoring systems to identify attacks
  - Incident response program
  - Disaster recovery plan

Training

- Institutions must implement ongoing information security awareness program
- Staff should receive security training at least once a year
- Training can be instructor led or online
- Untrained staff are perfect targets for hackers!

Testing

- All controls must be tested
  - Priority should be given to high-risk, critical systems
  - Separation of duties applies to control testing
  - Three most commonly testing methodologies
    - Audit
      - Evidence-based examination that compares current practices against internal or external criteria
    - Assessments
      - A focused privileged inspection
    - Assurance test
      - Measures how well controls work by subjecting the system to an actual attack

Oversee Service Provider Arrangements

- Financial institutions must ensure that service providers have implemented security controls in accordance with GLBA
  - Recommended oversight procedures:
    - Conduct risk assessment
    - Use due diligence when selecting third parties
    - Implementing contractual assurances regarding security responsibilities, controls, and reporting
    - Requiring non-disclosure agreements
    - Providing third-party review of the service provider's security through audits and tests
    - Coordinating incident response policies and contractual notification requirements
    - Review third-party agreements and performance at least annually

Adjusting the Program

- Effective monitoring involves both technical and non-technical evaluations
- Change drivers include mergers and acquisitions, changes in technology, changes in data sensitivity
- Information security policy should be reviewed at least annually

Report to the Board

- Reporting to the board should take place at least annually and describe the overall status of the information security program and the organization's compliance with the interagency guidelines
  - The report needs to address risk assessment and management, control decisions, service provider arrangements, employee training, independent audits and testing, recommendation for change of the program

What Is Regulatory Examination?

- Regulatory agencies are responsible for oversight and supervision of financial institutions
- Exams are conducted every 12 to 18 months
- The exam includes evaluation of policies, processes, personnel, controls, and outcomes
- Financial institutions are given a rating on a scale of 1 to 5, with 1 representing the best rating and 5 the worst rating with the highest degree of concern

Personal and Corporate Identity Theft

- Personal identity theft occurs when someone possesses and uses any identifying information that is not his with the intent to commit fraud or other crimes
  - Identifying information includes:
  - Name
  - Date of birth
  - Social Security numbers
  - Credit card numbers
- Corporate identity theft when criminals attempt to impersonate authorized employees to access corporate bank accounts and steal money
  - Known as corporate account takeover

Personal and Corporate Identity Theft cont.

- Responding to identity theft: Supplement A, "Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice" ("the guidance")
- The guidance describes response programs, including customer notification procedures, that a financial institution should develop and implement to address unauthorized access to or use of customer information
- FTC supports identity theft criminal investigations and prosecution through its Identity Theft Data Clearinghouse

Personal and Corporate Identity Theft cont.

- Updated guidance on Internet banking safeguards was released October 2011
  - Financial institutions are required to review and update existing risk assessment at least every 12 months
  - Financial institutions must implemented a layered security model
  - Financial institutions must offer multifactor authentication to commercial cash management customers
  - Financial institutions must implement authentication and transactional fraud monitoring
  - Financial institutions must educate commercial account holders about risks associated with online banking