XXVI Congreso de Seguridad Bancaria
CELAES 2011

Gramm-Leach Bliley Act Section 501(b)

and

Customer Notification

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

FLORIDA INTERNATIONAL
FIBA
BANKERS ASSOCIATION

Overview

- Background information
- Elements of a sound plan
- Customer notifications

Background – GLBA

Gramm-Leach-Bliley Act of 1999

- Protect customer financial information
- Enforcement by Federal and State agencies
- Examination guidance (2001)

Background – Where It Applies

- Guidelines apply only to non-public personal information of “customers”
- Customer is an individual (or the individual’s legal representative) who:
  - Obtains or has obtained a financial product or service from the institution, that is to be used primarily for personal, family household purposes; and
  - Has or had a continuing relationship with the institution
- GLBA requirements do not apply to:
  - Information relating to the institution
  - Business customers

Background – Covered Institutions

- GLBA 501(b) applies to:
  - Banks (Regulation H)
  - Bank holding companies (Regulation Y)
  - Edge corporations, agreement corporations, and uninsured state-licensed branches or agencies of foreign banks (Regulation K)

Background – Exceptions

- GLBA 501(b) is not applicable to:
  - Broker-dealers
  - Persons providing insurance
  - Investment companies and advisors

Examinations

- Every examination cycle requires an assessment of GLBA compliance
- Failure to adhere to the guidelines can result in regulatory violations

Elements of a Sound Program

- Documented written plan
- Involve board of directors
- Risk assessment - identify and assess risks to customer information
- Training
- Testing
- Oversee service providers
- Adjust program
- Review, approve, and annual reporting

Documented Plan

- **Written** information security program or policy
- Specifics outlined in Interagency Guidelines for establishing Safeguarding Customer Information that implements GLBA 501(b) under SR 01-15

Involve Board of Directors

- Review and approve information security program
- Oversee development, implementation and maintenance
- Assign specific responsibility for implementation
- Review reports from management

Risk Assessment

Identify & Assess Risk to Customer Information

- Identify where customer information exists
  - Hard copy - loan files, signature cards, applications, miscellaneous reports, garbage, etc.
  - Electronic - databases, workstations, servers, diskettes, CDs, transmissions, backup tapes, USB drives
- Assess risk
  - Identify reasonably foreseeable internal and external threats
  - Assess the likelihood and damage of the threats
  - Assess the sufficiency of policies and procedures to control risk

Training and Testing

- Employees must be trained to implement the bank's information security program
- Tests must be conducted of key controls, systems, and procedures
  - Security tests
  - Keep critical systems and application software patched
  - Maintain current awareness of new vulnerabilities and emerging threats
  - Business continuity plans
  - Conducted and reviewed by independent party

Oversee Service Providers

- Due diligence in selection
- Require by contract to implement appropriate safeguarding measures
- Ongoing monitoring
- Notifying bank of security breaches

Adjust the Program

- Monitor, evaluate, and adjust program
  - Changes in:
    - Technology
    - Business processes
    - Changes in products or services
    - Sensitivity of information
    - Internal or external threats
    - Business arrangements

Board Approval & Annual Reporting

- Board approval at least annually
- Overall status of information security program
- Discuss material matters
- Address various issues
  - Risk assessment
  - Service provider arrangements
  - Test results
  - Security breaches and violations
  - Recommendations for changes

Customer Notification

FELABAN
FEDERACION LATINOAMERICANA DE BANCOS

FLORIDA INTERNATIONAL
FIBA
BANKERS ASSOCIATION

Response Program

- Effective March 29, 2005
- The OCC, Board, FDIC, and OTS published an interpretation of the Gramm-Leach-Bliley Act (GLBA) and the Interagency Guidelines Establishing Information Security Standards (Security Guidelines) to include the development and implementation of a response program to address unauthorized access to, or use of customer information that could result in substantial harm or inconvenience to a customer.

Response Program

- At a minimum, the program should contain procedures for the following:
  - Assessing the nature and scope of an incident, and identifying what customer information systems and types of customer information have been accessed or misused
  - Notifying its primary Federal regulator as soon as possible when there is an incident involving sensitive customer information

Response Program

- Filing a Suspicious Activity Report ("SAR") and notifying law enforcement authorities when necessary
- Containing and controlling the incident to prevent further unauthorized access
- Notifying customers when warranted

Customer Notification

- An institution should notify affected customers when
  - It becomes aware of an incident of unauthorized access to sensitive customer information AND
  - Misuse of customer information has occurred or is reasonably possible

Customer Notification

- Law enforcement may delay notification if
  - Law enforcement believes that notification may interfere with a criminal investigation, AND
  - A written request is provided to the institution, but
  - Notification must be made as soon as this is no longer the case

Customer Notification

- Notification must be clear and conspicuous
  - Should be delivered in any manner designed to ensure that a customer can reasonably be expected to receive it.

Sensitive Customer Information

- Identifying information (customer name, address, telephone number) together with

- SSN/TIN, driver's license number, credit/debit card number, personal identification number or account number;

OR

- Any combination of customer information that would allow access to the customer's account (username and password)

When to Notify?

- The institution must notify if misuse is “reasonably possible” not “reasonably probable”
- Awareness is the trigger for regulatory notification, not extent of incident, culpability of institution, or likelihood of misuse

When to Notify?

- Notification is not required for incidents outside the institution's control
  - Accidental disclosure by customer
  - Disclosure by servicer independent of institution (credit card merchant processor)
- Many institutions notify anyway

Content of Customer Notice

- Description of the incident in general terms
- What kind of customer information was compromised
- What the institution has done to protect customers from further unauthorized access
- Telephone number to call for assistance
- Reminder to remain vigilant over the next 12 to 24 months

Customer Notice

- Recommendation to review account activity and report any suspicious activity
- Description of fraud alerts and how to place them in consumer credit reports
- Reminder to obtain credit reports and have fraudulent activity deleted
- Explanation of how to retrieve a credit report free of charge

Customer Notice

- FTC provides information on identity theft protection
  - How to use online guidance
  - How to report incidents of identity theft
  - Contact information

Supervisory Considerations

- Reasonably Possible vs. “Reasonably Probable”
- Definition of “sensitive customer information”
- Identifying affected customers may be an ongoing process

Supervisory Considerations

- Service providers
  - For notification to be required, service providers must maintain customer information “by or on behalf” of financial institutions
  - Institutions don’t have to trace back through chain of vendor relationships, but
  - Institutions may want to notify anyway because of public perception

Best Practices

- Make customer whole in the event of actual fraud arising from misuse
- Assist customers in pulling credit reports
- Monitor account activity
  - Implement anti-fraud monitoring technology
- Notification through multiple media
- Publicize positive steps taken to protect customers
- DO NOT include sensitive customer information in the notification

QUESTIONS?

Thank You.