XXVII Bank Security Conference

CELAES 2012

"MITIGATING RISKS AND CONVERTING THEM INTO BUSINESS OPPORTUNITIES"

FIBA

Organized by:

FELABAN

FEDERACION LATINOAMERICANA DE BANCOS

Gramm Leach Bliley Act:

The U.S. Legal Perspective for Financial Institutions

Patricia M. Hernandez

XXVII Bank Security Conference - CELAES
September 20, 2012

The Disclosure of Customer Information

Take your pick:

- Stolen laptop
- Confidential reports NOT Shredded
- Employee Misuse
- Unauthorized Sharing with Affiliates

Disclosures have legal consequences

- Customer and Regulatory Notification Process
- Potential Liability and Third Party Claims
- Response is based upon Specifics of Incident
- All based on the Gramm Leach Bliley Act

Gramm Leach Bliley Act

- Financial Services Modernization Act of 1999.
- Addressed, among other things, securities activities of banks and privacy of customer information.
- Rules on privacy and customer data applies to “Financial Institutions”

Prior to GLBA

- Privacy of customer information was state-specific.
- Federal law only addressed federal government agencies seeking customer information through the Right to Financial Privacy Act.
- Does not supersede stronger state laws.

Two Main Privacy Components of GLBA

- Privacy Rule.
- Safeguard Rule.
    - Includes regulatory guidance on response to incidents of inadvertent or willful misuse or disclosure

Part I: Privacy Rule

- Requires Privacy Notice to customers and consumers (in certain circumstances).
- Provides for opt-outs of sharing of information with unaffiliated third parties.
- Many exceptions to opt-out
  - Service Provider/Joint Marketing
  - Transaction Processing/Servicing
  - Governmental Investigations and Subpoenas.

Non-public Personal Information

The Privacy Rule defines "nonpublic personal information" as "personally identifiable financial information and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available."

Personally Identifiable Information

Personally identifiable financial information is defined under the Privacy Rule as:

- any information a consumer provides to a financial institution in order to obtain financial services or products;
- any information about a consumer resulting from any transaction involving a financial product or service provided by the financial institution; and
- any other information otherwise obtained by the financial institution in connection with providing a financial product or service to the consumer.

Customer:

- Is an individual who provides personal information to a financial institution to obtain a financial product for personal or household use.
- Is not a person providing information as part of a business transaction.

Redisclosure and Reuse

- Shared information is subject to same limitations of original recipient of information.
- Applies to vendors who have access to information.
- Requires the disclosing party to ensure confidentiality of information.
- Also applies to affiliates.

Privacy Rule Compliance Program

Requires:

- Assessment of Information Practices
- Development of Policies and Procedures
- Evaluate Third Party Relationships
- Handling Opt-Outs
- Training

Part II: Safeguards Rule

- The Safeguards Rule requires a financial institution to develop, implement and maintain a comprehensive Customer Information Security Program containing the administrative, technical and physical safeguards that are appropriate based upon the institution's size, complexity and the nature of its activities.

- Risk-based.

Six Components of Customer Information Security Programs

The Customer Information Security Program has ***six*** components:

1) designating an employee or office responsible for coordinating the program;
2) conducting risk assessments to identify reasonably foreseeable security and privacy risks;
3) ensuring that safeguards are employed to control the risks identified and that the effectiveness of these safeguards is regularly tested and monitored;
4) complying with the Privacy Rule;
5) overseeing service providers; and
6) maintaining and adjusting the Customer Information Security Program based upon the results of testing and monitoring conducted as well as changes in operations or operating systems.

Legal Response to a Disclosure

- The Disclosure of Customer Information requires specific responses both to customers and regulators
- Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- Look into available insurance
- Requires thorough investigation

Liability

- Potential Liability
  - Class Actions
- Third Party Claims
  - Ensure indemnification claims available
- Policies, Procedures, Controls and Response are essential to lessening risk of liability

Conclusion

- GLBA should be looked at as best practices
- Concern should be particular in sharing with vendors and affiliates

PATRICIA M. HERNANDEZ
Avila Rodriguez Hernandez Mena & Ferri LLP
2525 Ponce de Leon Blvd., Suite 1225
Coral Gables, FL 33134
tel 305.779.3566
fax 305.779.3561
phernandez@arhmf.com