ARHM&F | Avila Rodriguez Hernandez Mena & Ferri LLP

Safeguarding of Customer Information:

The GLBA Legal Perspective

Patricia M. Hernandez

XXVI Bank Security Conference - CELAES
September 16, 2011

Gramm Leach Bliley

- Financial Services Modernization Act of 1999
- Passed in 1999
- Largest banking legislation in 50 years – only surpassed now by the Dodd Frank Act
- Addressed, among other things, securities activities of banks and privacy of customer information

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

- Requires “financial institutions” to disclose their privacy policies to customers when they become a customer and annually thereafter and allows certain opt-out rights.

- Established comprehensive standards for requiring “financial institutions” to safeguard the security and confidentiality of customers’ personal information.

Financial Institutions

- Applies to banks, but also applies to securities firms, insurance companies, mortgage brokers and finance companies.
- Variety of regulators were tasked with adopting implementing regulations.
- Federal Reserve's Regulation P.

Privacy Rule

- 15 USC § § 6801-6809
- 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 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.

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.

Privacy Rule Compliance Programs

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

Safeguards Rule

- 15 USC § § 6801-6809.

- The GLBA and the Safeguards Rule require a financial institution to develop, implement and maintain a comprehensive 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.

Six Components of 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.

Component 1: The Coordinator/Privacy Officer

- The Security Program Coordinator/Privacy Officer ("Coordinator) is responsible for implementing the Customer Information Security Program.
- The Coordinator must ensure that risk assessments and monitoring are carried out for each unit or area that has customer data and that appropriate controls are in place for the identified risks.
- The Coordinator may require units with substantial access to customer information to further develop and implement comprehensive security plans specific to those units and to provide copies of the plan documents.
- The Coordinator may designate, as appropriate, responsible parties in each area or unit to carry out activities necessary to implement the Customer Information Security Program.

Component 2: Risk Assessments

- The Customer Information Security Program must identify reasonably foreseeable external and internal risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or otherwise compromise such information, and assess the sufficiency of any safeguards in place to control these risks.
- Risk assessments must include consideration of risks in each unit or area that has access to customer information.
- Risk assessments must include, but not be limited to, consideration of employee training and management; information systems, including network and software design, as well as information (both paper and electronic) processing, storage, transmission and disposal; and systems for detecting, preventing, and responding to attacks, intrusions, or other system failures.

Component 3: Testing

- The financial institution is required to regularly test the systems and procedures of the Customer Information Security Program.
- The tests should be conducted or reviewed by independent third parties or else by staff members independent of those that develop and maintain the security program.
- The frequency and nature of these tests should be based on the risk assessment the bank has prepared.
- Also, the bank should train staff regarding compliance with the Customer Information Security Program.

Component 4: Privacy Rule

- Ensuring compliance with Privacy Rule.

Component 5: Service Providers

- To the extent that the financial institution will use outside service providers for data processing and other activities that involve the handling of customer information, the institution will be required to exercise care in selecting its service provider(s).
- For example, the institution must require its service providers by contract to implement appropriate measures to safeguard customer information.
- And the institution should have a mechanism in place – by means of audits, summaries of test results, or equivalent methods – to monitor the service provider(s) compliance with their contractual obligations regarding the handling of customer information.

Component 6: Flexibility of Program

- The financial institution should report to the board relating to these issues at least annually.
- The report should discuss issues related to the program such as risk assessment, risk management and control decisions, service provider arrangements, results of testing, security breaches or violations and management's responses, and recommendations for changes to the overall information security program.
- Reporting of Violations to Customers and Regulators.
- Customer Information Security Program needs to be flexible to address new risks.

Common Issues from a Legal Perspective

- Employee misuse of information.
- Failure to report to customers and regulators.
- Failure to have Privacy Officer and Annual Report.
- Most fines have been by Federal Trade Commission.
- Bank regulatory actions have resulted in criticisms in ROEs.
- Potentially can have private causes of action (i.e. class action lawsuits).

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
Email: phernandez@arhmf.com