

**GLBA Data Protection
Requirements -**
*An Overview of Emerging
Challenges*

ReymannGroup,
Inc.

CONTENTS

Prepared By:

Paul R. Reymann
CEO
ReymannGroup, Inc.

| | |
|---|------------|
| How Does GLBA apply to Information Security? | 1 |
| What Challenges are emerging? | 1 |
| Summary | 4 |
| Attachment: - Self Assessment Checklist | A-1 |

June 2002

How Does GLBA apply to Information security?

Privacy and security of customer information are receiving enhanced risk management attention in the financial services industry. The passage of the Gramm-Leach-Bliley Act (GLBA) in 1999, heightened attention to terrorist threats, in addition to regulations and guidance that has been issued relevant to emerging technology-, privacy-, and security-risk has increased the:

- Awareness of the consumer.
- Need for additional risk mitigation controls.
- Potential enforcement and liability exposure for financial service entities.

Without adequate physical, administrative, and technical security, institutions cannot begin to ensure a consumer that his or her information and privacy is protected effectively.

Effective July 2001, all federally insured financial institutions must demonstrate enterprise-wide compliance with the GLBA Data Protection provisions.

The data protection provisions are comprehensive and require the Regulators (Banking, Insurance, FTC & SEC) to establish appropriate standards for financial institutions relating to administrative, technical, and physical safeguards for customer records and information. GLBA affects an extremely wide range of organizations. Examples include banks, insurance companies, securities firms, tax preparers, mortgage brokers and lenders, real estate agents and appraisers, financial planners, and credit card companies.¹

The entire financial services industry is required to assess and possibly re-design their administrative, technical and physical security measures to comply with this new law and implementing regulations to protect customer information.

What Challenges are emerging?

The banking regulators have already begun to examine for compliance and will continue to ensure institutions maintain compliance continuously. A recently released FDIC survey on how financial institutions have fared during initial GLBA audits determined “almost all information security programs examined were found to have some deficiencies relating to board involvement, testing, and/or staff training.²” Other areas of confusion and risk are also emerging around the requirements for a formal risk assessment, oversight of service providers, and monitoring and adjusting the information security program.

Involve the Board of Directors

The fiduciary obligations and responsibilities of a board mandate that the board ensure management implements an effective information security program. This is an example of how technology has moved from an exclusive IT backroom operation to the boardroom.

The regulators mandate that you have a written information security program that is approved by the Board of Directors or an appropriate committee. You should:

¹ Section 4(k) of the Bank Holding Company Act and 12 CFR 211.5(d), 12 CFR 225.28, 12 CFR 225.86(a) and (b) define “financial institution” broadly to include not only depository institutions such as banks, thrifts, and credit unions, but also numerous types of non-depository institutions.

² Operations Alert, Americas Community Bankers, May 27, 2002

- Define a plan to achieve timely compliance and articulated the approach to your Board of Directors and functional regulator.
- Appoint someone in charge of your security preparedness plan. That individual should be held accountable for meeting and maintaining compliance with the requirements.
- Create a timetable with milestones to measure progress toward compliance

You should also report to your board (or committee), at least annually. This reporting should describe the overall status of the information security program and your compliance.

Test

Each institution must regularly test its key controls, systems, and procedures. The frequency and nature of such tests should be based on the risk assessment and change in internal and external conditions that may affect its information security program.

You should:

- Develop a plan that affords adequate time to test your information security program.
- Identify independent third parties that can conduct & review the tests.
- Document the test results and recommendations.

Train Staff

GLBA recognizes the importance of and requirement for training. Staff must be trained to understand the institution's information security program, recognize, respond to, and where appropriate, report to regulatory and law enforcement agencies, any unauthorized or fraudulent attempts to obtain customer information.

Many institutions have defined a well-written information security program that articulates the roles and responsibilities throughout the organization. But when it is time to execute the program, the employees frequently receive minimal instruction on how to properly execute the program. Training may be limited to a single orientation session or policy mailing.

The lack of adequate continuous training is emerging as a "sleeper" risk for financial institutions.

If every team member does not understand his or her enhanced roles and responsibilities under the new information security requirements, you will not execute a winning compliant information security program. Not only does each employee need to know the plan - they must be able to execute it! Proper training is crucial to your success.

You should:

- Establish a program to train personnel on the requirements of the new information security program rule.
- Establish programs to offer customized training to personnel in the handling of consumer information under your new information security program.
- Prepare materials for customer representatives to properly respond to consumer inquiries about the institution's information security program.
- Train your staff to:

- Understand his or her responsibilities under the new US Patriot Act and other anti-money laundering laws.
- Recognize and respond to attempts of pretext phone calling or identify theft.
- Complete a suspicious activity report.

Other areas of confusion that create noncompliance risk for many institutions include the:

- Risk assessment requirements.
- Third party contract provisions.
- Monitoring and adjustments.

Assess Risk that may threaten customer information

Each institution must consider the sensitivity of information and assess the likelihood of reasonably foreseeable internal and external threats causing significant damage. This assessment must evaluate the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks.

An effective risk assessment will include a review of your lines-of-business, applications, technology infrastructure, and service providers. You should follow a structured process to identify threats, controls and vulnerabilities for each of these four risk areas. Within each risk area, you should drill down on operational, fraud, reputation, compliance, and technology risk.

Oversee Service Provider Arrangements

The institution that holds the client's trust is always responsible for safeguarding customer information even when it uses a third party to provide services to its customers. In short, even if an institution outsources its information management operations, it is ultimately responsible for the safety of customer information.

If you have not done so already, it is time to establish appropriate oversight of your vendor relationships. Specifically, you should:

- Assess your outsourcing risks to identify your needs and requirements.
- Create and maintain an inventory list of each vendor relationship you have and its purpose.
- Prioritize the risk of each relationship consistent with the types of customer information the vendor can access.
- Perform proper due diligence of third party vendors.
- Execute written contracts that outline duties, obligations and responsibilities of all parties.
- Establish procedures for oversight of all outsourcing relationships and services.

Numerous institutions have expressed confusion on the July 1, 2002 deadline for ensuring all contracts are compliant with the new data protection requirements. Frequently, this confusion occurs when institutions have not clearly distinguished between both parts of the GLBA Privacy rules: (1) Privacy of Consumer Financial Information, pursuant to section 504 of the GLBA that deals with the privacy promise and delivery of a notice to customers; and (2) Privacy Data Protection Provisions, pursuant to section 501 of the GLBA – Standards for Safeguarding

Customer Information – that establishes standards relating to administrative, technical, and physical safeguards for customer records and information.

Each of these rules contains a similar two-year grand fathering clause of service agreements. However, since each rule was finalized at different times, the transitional effective date is different. Specifically:

- Privacy of Consumer Information requires all contracts to satisfy the provisions of Exception 13(a)(1)(ii) no later than July 1, 2002.
- Standards for Safeguarding Customer Information requires all contracts to satisfy the provisions of paragraph III.D (Oversee Service Provider Arrangements) no later than July 1, 2003.

Clearly, there is a difference of one year between the two rules.

On May 24, 2002, the FTC released its final Privacy Data Protection Rule – Standards for Safeguarding Customer Information (16 CFR Part 314). However, the rule has not been published in the Federal Register yet. The rule takes effect on the date it is published in the Federal Register. Similar to the banking agencies, FTC has included a two-year grand fathering of service contracts. (Refer to 314.5(b)). Once the rule is published in the Federal Register, all contracts must satisfy the provisions of section 314.4(d) (Oversee Service Providers) within 2 years of the published effective date.

Since the respective rules have different transition dates for the grand fathering of service agreements, you are not required to have all contracts updated by July 1, 2002. However, based on the nature of the contracts for handling customer information, the similarity of language that can be used to satisfy each rule, and the effort required to change contracts, you may find it easier to implement the contractual changes once (before July 1, 2002). Alternatively, you have until July 1, 2003 for those contracts that related only to the banking industry Standards for Safeguarding Customer Information. You have until sometime in mid 2004 for FTC related entities.

Monitor and Adjust the Program

The institution must adjust its information security practices on a continuing basis to account for changes in technology, changing business arrangements (such as mergers or acquisitions), the sensitivity of customer information, and internal and external threats to information security.

SUMMARY

The entire financial services industry must implement effective administrative, technical, and physical security measures to protect customer information. Clearly, information technology is no longer a back office operation, only; it is a subject upon which the board and senior management must be actively involved and aware, especially in the instance of material events that may threaten the safety, soundness, and security of the institution and its customer information.

Compliance with the GLBA regulations mandates continued vigilance from financial institutions. The regulators are focusing on financial institution compliance with the mandated requirements to audit, enforce, monitor, and report on events that threaten the security of customer information.

Failure to comply with the new regulations and establish a safe, sound, and secure customer information security program will expose an institution to compliance, reputation, operational, fraud, and enforcement risk.

ReymannGroup, Inc. has developed a simple and easy to follow GLBA Data Protection Self-Assessment Checklist. It will help you quickly review your progress in achieving compliance with the new information security program requirements. A complimentary copy is attached with this white paper for your use. (Please limit distribution of the checklist within your organization. If you would like additional copies, simply contact us.)

If you would like to learn more about how ReymannGroup, Inc. can assist you, contact or e-mail us at (410) 956 7334 or info@reymanngroup.com.

About the Author – Paul R. Reymann.

Mr. Reymann, CEO of ReymannGroup, Inc., is a financial institution regulatory consultant and co-author of Section 501 of the Gramm-Leach-Bliley Act Data Protection regulation. Mr. Reymann has more than eighteen years experience in the financial services industry, including thirteen years with the Department of Treasury's Office of Thrift Supervision (OTS) in Washington D.C. There he guided the regulatory agency's Technology Risk management activities and authored several key regulatory directives and advisories on emerging risk management issues, including the industry's first regulatory directive on "Transactional Internet Banking."

Fortune 500 companies have leveraged Mr. Reymann's subject matter expertise to develop successful go-to-market strategies for information security and technology products and services within key vertical markets. Mr. Reymann was also President, U.S.A. Operations for Compliance Coach, Inc., which has emerged as a national e-learning leader in blending web-based delivery with the best-in-class regulatory compliance education and consulting services for the financial services industry.

Mr. Reymann is recognized in the prestigious 2006 Heritage Registry of WHO's WHO. He is referenced frequently in industry news and magazine articles. He is also the author of numerous articles and papers on technology risk, transactional web sites, customer information, network security and other technology and safety and soundness topics.

About ReymannGroup, Inc.

ReymannGroup, Inc. is a team of high-caliber subject-matter experts in the vertical markets of financial services, healthcare, manufacturing, and other industries. We help our clients understand and successfully navigate the regulatory requirement opportunities within these vertical markets. If you would like to learn more about how ReymannGroup, Inc. can assist you, contact or e-mail us at (410) 956 7334 or info@reymanngroup.com.

OVERVIEW

The GLB Data Protection Preparedness Checklist will help you quickly:

- **Assess** whether you are taking the necessary steps to comply with the GLB Act Data Protection requirements.
- **Identify** additional steps that you should consider.
- **Measure** your progress in completing all recommended steps.

Complete an initial survey of your data protection preparedness efforts and track your compliance progress.

Effective compliance with the GLB Act Data Protection regulation requires an organization to:

- Involve the Board;
- Assign responsibility and accountability for executing the plan;
- Create a realistic timetable with milestones for accomplishing the plan;
- Assess the risks that may threaten customer information;
- Develop a plan containing policies and procedures to manage and control these risks;
- Oversee your outsourcing relationships;
- Implement an information security training program;
- Test your information security program;
- Adjust the plan on a continuing basis; and
- Report to the Board.

In achieving these objectives, you should follow a series of prudent steps that will help lead you to full compliance with the GLB Act Data Protection regulation. ReymannGroup's GLB Security Preparedness Checklist walks you through the general criteria for each of these prudent steps and helps you to track your progress in completing the steps and achieving compliance with the GLB Act Data Protection requirements.

INVOLVE THE BOARD

You should have a written information security program that is approved by the Board of Directors or an appropriate committee. The board or committee should oversee the development, implementation, and maintenance of your information security program. They should also assign specific responsibility for implementation and review reports from management.

Have you:

- Defined a plan to achieve timely compliance and articulated the approach to your Board of Directors and functional regulator?
- Appointed someone in charge of your security preparedness plan? That individual should be held accountable for meeting and maintaining compliance with the requirements.
- Created a timetable with milestones to measure progress toward compliance?

ASSESS RISKS

You should identify reasonably foreseeable threats that could result in authorized disclosure, misuse, alteration or destruction of your customer information or systems.

Have you:

- Identified your current uses of consumer information in order to understand the effect of the new security rule on your operations?
- Considered the sensitivity of your customer information and assessed the likelihood of internal and external threats causing significant damage?
- Assessed the sufficiency of your risk control practices, such as:
 - Policies and procedures?
 - Customer information systems?
 - Other arrangements?

MANAGE AND CONTROL RISK

You should design your information security program to control the identified risks, consistent with your sensitivity of the information and the complexity and scope of your activities.

Have you:

- Evaluated your current practices against the requirements of the new security rule?
- Evaluated the capability of your information systems to ensure that they are consistent with your new security policies and procedures? (You do not want to provide a security promise to your customers that your systems cannot deliver.)
- Taken the process of preparedness from evaluation to developing the necessary policies and systems that fulfill the compliance obligations of your organization?
- Considered the following security measures consistent with your risk profile and documented your decision to implement such practices, or not?
 - Access controls
 - Access restrictions
 - Encryption
 - Change control procedures
 - Dual control procedures
 - Segregation of duties
 - Employee background checks
 - Monitoring systems
 - Response programs
 - Protective measures against environmental hazards or technological failures

OVERSEE THIRD PARTIES

Your information and transaction processing and settlement activities involves risks. Whether you perform these activities internally or outsource them to a third party, your exposure can include threats to security, availability and integrity of systems and resources, confidentiality of information, and regulatory compliance.

ReymannGroup, Inc.
GLB Data Protection Checklist

Have you:

- Assessed your outsourcing risks to identify your needs and requirements?
- Created and maintained an inventory list of each vendor relationship you have and its purpose.
- Prioritized the risk of each relationship consistent with the types of customer information the vendor can access.
- Performed proper due diligence of third party vendors?
- Executed written contracts that outline duties, obligations and responsibilities of all parties?
- Established procedures for oversight of all outsourcing relationships and services?

IMPLEMENT AN INFORMATION SECURITY TRAINING PROGRAM

You should train staff to implement your information security program. Your training should also help employees to recognize and respond to fraudulent attempts to obtain customer information. Typically, your training should be tailored to your institution's practices and procedures.

Have you:

- Established a program to train personnel on the requirements of the new information security program rule?
- Established programs to offer customized training to personnel in the handling of consumer information under your new information security program?
- Prepared materials for customer representatives to properly respond to consumer inquiries about the institution's information security program?
- Trained your staff to recognize and respond to attempts of pretext phone calling or identify theft?
- Trained your staff how to complete a suspicious activity report?

TEST YOUR INFORMATION SECURITY PROGRAM

You should regularly test your key controls, systems and procedures. The frequency and nature of such tests should be based on the risk assessment and change in internal and external conditions that may affect your information security program.

Have you:

- Developed a plan that affords adequate time to test your information security program?

ReymannGroup, Inc.
GLB Data Protection Checklist

- Identified independent third parties that can conduct the tests?
- Identified independent third parties that can review the tests?
- Documented the test results and recommendations?

ADJUST

You should monitor, evaluate, and adjust the information security program, as needed.

Have you established a process to adjust the program in response to:

- Relevant changes in technology?
- Sensitive of customer information?
- Internal and external threats?
- Changes in our business arrangements?
- Changes to our customer information systems?

REPORT TO THE BOARD

You should report to your board (or committee), at least annually. This report should describe the overall status of the information security program and your compliance.

Have you:

- Established procedures for regularly reporting on your information security program to the board?
- Included material matters in the board reports related to the program, such as:
 - Risk assessment?
 - Risk management and control decisions?
 - Service provider arrangements?
 - Results of testing?
 - Security breaches or violations?
 - Management responses?
 - Recommendations for changes?