



*White paper*

## **THE DATA PROTECTION RULE OF THE GRAMM-LEACH-BLILEY ACT:**

A strategy for compliance

Prepared by:

**Paul Reymann**  
President  
ReymannGroup, Inc.

**Mitchell Ashley**  
VP of Engineering & CIO

July 2004

---

## Table of Contents

1. Introduction	.3
1.1 The purpose of GLBA	.3
1.2 Affected industries	.3
1.3 GLBA Data Protection Rule requirements	.3
1.4 Compliance deadlines	.3
1.5 Compliance monitoring	.3
1.6 Penalties for non-compliance	.3
2. Plotting a course to GLBA compliance	.3
3. How can StillSecure help achieve GLBA compliance?	.4
3.1 StillSecure Strata Guard	.5
3.2 StillSecure Server VAM	.5
4. Additional Resources	.6
5. About StillSecure	.6
6. About ReymannGroup, Inc.	.6
Appendix A.	
The ReymannGroup <i>GLBA security preparedness checklist</i>	.6

---

## About the author

Paul Reymann is one of the nation's leading financial industry regulatory experts and co-author of Section 501 of the Gramm-Leach-Bliley Act. Mr. Reymann has more than 18 years of 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.

Mitchell Ashley, as Vice President of Engineering & CIO of StillSecure, is responsible for the product strategy and development of the StillSecure™ suite of network security software. Mr. Ashley brings to Latis Networks more than twenty years of experience in data networking, network security and software development. Mr. Ashley is a graduate of the University of Nebraska, with Bachelor of Science degrees in Computer Science and Business Administration.

## 1. INTRODUCTION

On November 12, 1999, President Clinton signed the Gramm-Leach-Bliley Act (GLBA) into law. GLBA Section 501, 'Protection of Nonpublic Personal Information,' requires federal banking agencies, the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission to establish appropriate standards for financial institutions related to the administrative, technical, and physical safeguards of customer records and information.

### 1.1 The purpose of GLBA

The security of customer information is paramount. The GLBA Data Protection Rule and subsequent safeguards are mandated to:

1. Insure the security and confidentiality of customer data.
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such data.
3. Protect against unauthorized access to or use of such data that would result in substantial harm or inconvenience to any customer.

### 1.2 Affected industries

To comply with GLBA, all organizations within the financial services industry must implement a comprehensive written information security program<sup>1</sup> specifying how their customer information is protected. The following institutions<sup>2</sup> fall within the purview of the act:

- banks
- mortgage brokers
- mortgage lenders
- credit unions
- insurance companies
- real estate agents
- appraisers
- thrifts
- securities firms
- financial planners
- credit card companies

### 1.3 GLBA Data Protection Rule requirements

The GLBA's data protection requirements are comprehensive. In general, you must develop and implement an information security program appropriate to the size and complexity of your organization, the nature and scope of your activities, and the sensitivity of your customer information.

### 1.4 Compliance deadlines

Enterprise-wide compliance is required by the following dates for your respective type of financial institution:

<sup>1</sup> Information Security Program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

<sup>2</sup> 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.

Functional regulator	Effective compliance date
Federal Banking Agencies (OCC, FRB, FDIC, OTS, & NCUA)	July 1, 2001
Securities and Exchange	July 1, 2001
Federal Trade Commission	May 23, 2003

Although the deadlines for compliance for organizations regulated by federal banking agencies and the SEC have passed, many organizations have not developed information security programs that meet regulation's requirements. As compliance monitoring will be an ongoing activity, information security program managers should strive to continually update and improve their operations.

### 1.5 Compliance monitoring

Each of the respective regulatory agencies is responsible for enforcing compliance with the new GLBA Data Protection requirements for institutions under its functional jurisdiction. Many organizations have already been audited to assess the actions they have taken to comply with the rules. Oversight and examination activities will be ongoing, not a one-time event. A recently released FDIC survey on how financial institutions have fared during initial GLBA audits found numerous institutions in non-compliance.

### 1.6 Penalties for non-compliance

If you are found noncompliant with the rule or to have deficiencies in your administrative, technical, or physical safeguards, the regulatory agencies have the responsibility and authority to take enforcement measures ranging from corrective action to fines, sanctions and/or other penalties.

## 2. PLOTTING A COURSE TO GLBA COMPLIANCE

In drafting the GLBA, the regulators recognized that there is no single total solution for comprehensive information security. The complexity, sensitivity, and risk profile of each organization is unique. Security must be addressed through a layered approach that includes policies, procedures, practices, solutions and technologies. The regulation stipulates that you:

1. **Involve the board of directors** – Your organization's board of directors or an appropriate committee of the board shall approve the written information security program and oversee development, implementation and maintenance of the program, including specific responsibility for implementing the program and reviewing management reports.
2. **Assess risk that may threaten customer information** – In assessing risk, you must:
  - a. Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or systems.
  - b. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information.

- c. Assess the sufficiency of policies, procedures, systems, and other arrangements in place to control risks.

An effective risk assessment will include a review of your:

1. lines-of-business
2. applications
3. technology infrastructure
4. service providers.

You should follow a structured process to identify threats and vulnerabilities for each of these four risk areas. For example, within each risk area you should address operational, fraud, reputation, compliance, and technology risks.

**3. Manage and control risk** – You must have controls to manage the identified risk with effective security measures that are commensurate with the risk profile of your organization.

Example security measures include:

- a. Access controls and restrictions to authenticate and permit access by authorized users only.
- b. Encryption of data while in transit or storage on a network.
- c. Change control and dual control procedures.
- d. Segregation of duties.
- e. Employee background checks.
- f. Monitoring systems and procedures for intrusion detection.
- g. Response programs for unauthorized events.
- h. Protective measures against potential environmental hazards or technological failures.

**4. Train employees** – GLBA recognizes the importance of training. Staff must be trained to understand your information security program. They must also recognize, respond to, and where appropriate, report to regulatory and law enforcement agencies any unauthorized or fraudulent attempts to obtain customer information.

**5. Test your program** – You must regularly test your security program's key controls, systems, and procedures. The frequency and nature of such tests should be based on the risk assessment and any changes in internal and external conditions that may affect your information security program. Tests should be conducted and reviewed by independent third parties or staff independent of those who developed or maintain the security program.

**6. Oversee service providers** – If you have not done so already, you must establish appropriate oversight of your vendor relationships. Specifically, you should:

- a. Assess your outsourcing risks to determine which products and services are best outsourced and which should be handled inhouse.
- b. Create and maintain an inventory list of each vendor relationship you have and its purpose.
- c. Prioritize the risk of each relationship consistent with the types of customer information the vendor can access.

- d. Perform proper due diligence of third-party vendors.
- e. Execute written contracts that outline duties, obligations and responsibilities of all parties.
- f. Establish procedures for overseeing all outsourcing relationships and services.

**7. Adjust the program** - You must adjust your information security practices on a continuing basis to account for changes in technology, changing business arrangements (such as mergers, acquisitions, alliances, or joint ventures), the sensitivity of customer information and internal and external threats to information security.

**8. Report to the board** – You should report to the board (or committee) at least annually. This report should discuss material matters related to your information security program such as:

- a. risk assessment
- b. risk management and control decisions
- c. service provider arrangements
- d. testing results
- e. security breaches or violations
- f. management's responses to breaches and violations
- g. recommended changes in the program.

### 3. HOW CAN STILLSECURE™ HELP YOU ACHIEVE GLBA COMPLIANCE?

StillSecure can play an important role in helping your organization comply with the GLBA requirements. StillSecure provides affordable, easy-to-use network security software products for IT and security professionals at security-conscious mid-tier enterprises. The StillSecure suite, which includes Strata Guard intrusion prevention software and VAM vulnerability assessment and management software, reduces the risk and liability of damages from network attacks and increases the productivity and effectiveness of your IT resources.

The following table shows how the StillSecure product line can assist you in complying with GLBA. *StillSecure products are described in more detail in sections 3.1 and 3.2.*

GLBA requirement	Strata Guard	VAM
Involve the board of directors	–	–
Assess the risk that may threaten customers	●	●
Manage and control risk	●	●
Train employees	●	●
Test your program	●	●
Oversee service providers	●	●
Adjust the program	●	●
Report to the board	●	●
● Addresses requirement		
– Does not address requirement		

### 3.1 StillSecure Strata Guard

Strata Guard empowers your firewall to dynamically block malicious traffic. It reduces the risk and liability from network attacks by empowering the firewall to instantaneously terminate attacks and unwanted traffic. Strata Guard identifies, profiles and displays attacks on networks by utilizing its at-a-glance Web-based interface. Through StillSecure' exclusive *Dynamic Attack Suppression™* technology, Strata Guard automatically takes action against attacks by ordering the firewall to block malicious traffic that would otherwise be allowed through.

StillSecure Strata Guard responds to anomalous traffic patterns and intrusions that match its continuously updated directory of rules. It features comprehensive research and advice to help you determine how to respond to specific attacks. A robust database is included to ensure the logging of all network activity, and Strata Guard's built-in reporting engine offers a wide range of customizable, actionable reports. Strata Guard is managed by the StillSecure Console and features multi-user, multi-node management of all instances of the product throughout the network.

### 3.2 StillSecure VAM

VAM provides assessment and management that continuously ensures network security. VAM offers a multitude of vulnerability scans run at customizable intervals. It provides an accurate view of a dynamically changing infrastructure down to the OS level. Its built-in workflow environment allows tracking and assignment of security vulnerabilities from identification to repair. The comprehensive reporting engine delivers customizable reports generated for specific audiences – board members, auditors or regulators, executives or fellow IT professionals.

VAM's comprehensive vulnerability database is updated automatically as often as every hour. It features comprehensive research and advice to help you determine how to repair specific vulnerabilities. VAM allows for multi-tiered access with unique read and write privileges based on a user's role relative to network security. The StillSecure Console manages the application as well as the complete line of StillSecure products.

StillSecure recommends that each financial services entity seek independent counsel regarding GLBA compliance. Use of StillSecure applications may or may not ensure full GLBA compliance and depends upon your unique profile. The full-text of the GLBA is not contained herein, but the Act in its entirety is available via the Web or the link on the following page.

## 4. ADDITIONAL RESOURCES

ReymannGroup, Inc. has developed the *GLBA Security Preparedness Checklist*, which you'll find in Appendix A. It will help you to evaluate your preparedness for complying with these new requirements.

Additional public information and guidance on developing an information security program is available on line:

**Final rule** - The final GLBA regulations are available at the following regulatory agency sites:

- **Federal Banking Agencies**  
<http://www.occ.treas.gov/fr/fedregister/66fr8616.htm>
- **FTC**  
<http://ecfr.access.gpo.gov/otcqi/cfr/otfilter.cgi?DB=5&ACTION=View&QUERY=2002052330&SUBSET=SUBSET&FROM=1&SIZE=10&ITEM=1>
- **SEC**  
[http://www.sec.gov/rules/final/34-42974.htm#P454\\_179663](http://www.sec.gov/rules/final/34-42974.htm#P454_179663)

CERT/CC ([www.cert.org](http://www.cert.org))

The CERT® Coordination Center (CERT/CC) is a center of Internet security expertise, located at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. CERT/CC provides information that ranges from protecting your system against potential problems to reacting to current problems to predicting future problems. Its work involves handling computer security incidents and vulnerabilities, publishing security alerts, researching long-term changes in networked systems, and developing information and training to help you improve your site's security.

FS-ISAC ([www.fsicac.com](http://www.fsicac.com))

The Financial Services Information Sharing and Analysis Center (FS-ISAC) is the first industry-wide database of electronic security threats, vulnerabilities, incidents, and solutions. It offers a confidential venue for sharing security vulnerabilities and solutions. It facilitates trust among its participants. Members benefit from the FS-ISAC's unique proactive means of mitigating cyber-security risks. FS-ISAC is exclusively for, and designed by, professionals in the banking, securities and insurance industries. No US Government agency, regulator or law enforcement agency can access the FS-ISAC.

NIPC ([www.nipc.gov](http://www.nipc.gov))

The National Infrastructure Protection Center (NIPC) serves as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. The NIPC provides timely warnings of international threats, comprehensive analysis and law enforcement investigation and response.

**NIST** - The National Institute of Standards and Technology (NIST) is a resource for learning more about information security planning. These resources may be of particular interest:

- **Guide for Developing Security Plans for Information Technology Systems**
- **SP 800-27 Engineering Principles for Information Technology Security (A Baseline for Achieving Security).**

SANS ([www.sans.org](http://www.sans.org))

The SANS (SysAdmin, Audit, Network, Security) Institute enables security professionals, auditors, system administrators, and network administrators to share the lessons they are learning and find solutions to the challenges they face. At the heart of SANS are the many security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire information security community. Many SANS resources, such as news digests, research summaries, security alerts and papers are free.

## APPENDIX A. THE REYMANNGROUP GLBA SECURITY PREPAREDNESS CHECKLIST

In achieving these objectives, you should follow a series of steps that will help lead you to full compliance with the GLBA Data Protection regulation. ReymannGroup checklist, which follows, walks you through the general criteria for each of these steps and helps you track your progress in completing the steps and achieving compliance with the GLBA 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?
- Assigned an individual to take responsibility for 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 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 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 with regard to your risk profile and documented your decision to implement such practices? Or documented your decision not to implement such practices?
  - 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 involve 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.*

#### Have you:

- Assessed your outsourcing risks to identify your needs and requirements?
- 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 service representatives to properly respond to consumer inquiries about the institution's information security program?

## GLBA SECURITY PREPAREDNESS CHECKLIST, continued

- Trained your staff to recognize and respond to attempts of pre-text 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 changes 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?
- 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 business arrangements?
  - Changes to 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?

## 5. ABOUT STILLSECURE

StillSecure provides affordable, easy-to-use network security software products for IT and security professionals at security-conscious mid-tier enterprises. The StillSecure suite reduces the risk and liability of damages from network attacks and tangibly increases the productivity and effectiveness of your resources. StillSecure is available through StillSecure's direct sales force and channel partners. StillSecure is financed by Mobius Venture Capital, 3i and Feld Group Ventures. For more information please call (303) 381-3830, or visit our Web site at <http://www.stillsecure.com>.

## 6. ABOUT REYMANN GROUP

ReymannGroup, Inc. assists financial institutions in evaluating their information security infrastructure, determining exposure to vulnerabilities and threats, prioritizing solutions, and complying with the GLBA Data Protection requirements. Through its Customer Information Security Program (CISP) service, the ReymannGroup provides you with an 'independent' high-caliber professional, an author of the GLBA Data Protection Regulation, and an expert familiar with banking industry regulations and best practices. The CISP service will meet and exceed your business need to implement and maintain a safe, sound, and secure customer information security program. If you would like to learn more about how ReymannGroup, Inc. can assist you in establishing a compliant customer information security program, contact or e-mail Paul Reymann at [410] 867-1564 or [paul@reymann.name](mailto:paul@reymann.name). The ReymannGroup GLBA Security Preparedness Checklist helps you quickly:

- **Assess** whether you are taking the necessary steps to comply with the GLBA 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 GLBA Data Protection regulation requires an organization to:

- Involve the board of directors
- 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
- Report to the board of directors