

## How to Comply with the Information Security Requirements of the Gramm Leach Bliley Act (GLBA)

### Introduction

If you work for a financial services institution, you've no doubt heard of the Gramm-Leach-Bliley Act (GLBA). This regulatory legislation has specific requirements for the security of your customers' personal data, and requires that you must take measures to protect this confidential data. This responsibility includes the need to insulate this information from hackers that could break into your IT systems and steal or corrupt this data, as well as insure that data is not inadvertently accessible or disclosed without proper authorization.

### Establishing responsibility for information security

Your first step in compliance with GLBA is to designate a board or committee who will be responsible for reviewing your organization's GLBA compliance. The board, or its designated committee, should approve a written information security program and assign responsibility for its implementation, which includes a review of the staff involved to insure they have the knowledge, expertise, and authority to perform these tasks. The program should address the seven basic GLBA security directives as outlined below:

#### 1. Conduct an enterprise-wide risk assessment

This assessment of risk must include an evaluation of the non-public customer information systems. This definition is broader than automated systems, and includes all methods to access, collect, store, use, transmit, protect, or dispose of customer information. A risk assessment process should be logical, supportable, and appropriate for the institution, and should:

- **Identify all reasonably foreseeable internal and external threats** that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems. This assessment should also identify the potential damage those threats could cause, given the policies, procedures, systems, and other controls in place.
- **Be conducted by personnel with sufficient expertise**, who should use current relevant information such as: hardware and software

*This regulatory briefing is based on FDIC FIL-68-2001: Examination Procedures to Evaluate Compliance with the Guidelines to Safeguard Customer Information. Reviewing this summary of process recommendations will help you evaluate how your institution measures up.*

*Assess the risks of every non-public customer information system in your organization.*

*Determine and document access controls as well as intrusion monitoring and response systems and procedures necessary to protect customer information.*

vulnerabilities, methods of attack, network topology, contractual requirements with outside parties, controls and control environment (e.g., policies, procedures, practices, budgets, organizational charts, and training), and test results.

- **Use skills and knowledge from across the enterprise**, from technical staff to management, using outside expertise when necessary.
- **Use timelines and milestones** to ensure timely completion.
- **Identify and rank its information assets** (data and system components) according to sensitivity, and use this process in the risk assessment.
- **Identify the relative sensitivity of its information** and customer information system, and use that identification to determine how certain data elements or system components should be protected.
- **Support estimates of the potential damage** posed by various threats where the risk is not mitigated.
- **Consider the current administrative, physical, and technical safeguards** that prevent or mitigate potential damage, and use test results to support the assessment of the adequacy and effectiveness of those controls.
- **Identify and prioritize risk exposure**, decide on the risks to mitigate, and create a mitigation strategy.
- **Adequately support, document, and report business decisions** to accept risks, and document approval by the appropriate level of management.
- **Result in prompt action to mitigate risks** that pose the immediate possibility of material loss, with mitigation strategy reviewed by appropriate officials.
- **Provide guidance for the nature and extent of testing**, including vendor selection and oversight.

*Determine and document access controls as well as intrusion monitoring and response systems and procedures necessary to protect customer information.*

## **2. Document your efforts to manage and control risks**

To facilitate compliance with GLBA, it is important that documentation is available which demonstrates that that you have considered the following controls, adopted those considered appropriate, and assessed the adequacy of controls used to support risk mitigation judgments:

- **Access controls, such as controls to authenticate** and permit access to customer information systems to authorized persons only. Controls include both technical measures and procedures to guard against non-technical attacks, such as impersonation or identity theft.
- **Access restrictions at physical locations**, such as buildings and computer facilities, to permit access to authorized persons only. Physical locations include all places where customer data is kept in a retrievable form, including document disposal.
- **Encryption of electronically transmitted data** including stored customer data. The selection of data to encrypt and the encryption technique and level should be supported by the risk assessment.
- **Change control procedures** to ensure that system modifications are consistent with the approved security program.
- **Dual control procedures, segregation of duties**, and employee background checks to minimize fraud and other risks. In general, only employees should have access to customer information systems, and their access should be limited to that necessary to perform their job functions.
- **Monitoring systems and procedures** to detect actual and attempted attacks on or intrusions into customer information systems, including network and host intrusion detection systems (IDS), network traffic monitoring, and review of firewall and IDS logs.
- **Response programs that specify actions to be taken** when you suspect unauthorized access (i.e., incident response), with procedures to isolate, analyze, recover from, and appropriately report unauthorized access. Recovery involves technical as well as public relations elements, so develop appropriate internal and external reporting procedures (e.g., regulator, law enforcement, and news media).
- **Measures to protect against destruction, loss, or damage** of information from potential environmental hazards, such as fire and water damage or technological failures, including data and system backup and business resumption capabilities.

*The human element of your security program will be one of your most important assets – ensure your staff is properly trained and regularly conduct independent testing of security controls, systems and procedures.*

*Ensure any changes in your business systems are reviewed to comply with the requirements of GLBA.*

### **3. Implement a program to train your staff**

It is important to ensure that employees are adequately trained to implement policies and procedures required of your information security program:

- **Document existing staff qualifications**, as well as requirements for ongoing training to ensure that staff stays abreast of current technology and methods to safeguard customer information.
- **Training includes awareness programs** as well as classroom instruction, and training should be consistent with the user's security-related responsibility and function.

This component of the GLBA regulations applies to front-line staff, as well as employees who have network related responsibilities. It should be noted that training is particularly important for newly hired personnel, to insure that they understand the security measures that are necessary as they regularly access sensitive customer information.

### **4. Conduct periodic testing**

In light of the continually changing information technology environment, it is important that key controls, systems, and procedures of the information security program are regularly tested. The nature and frequency of testing should be consistent with the assessed risk.

- **Tests should be conducted or reviewed by independent** third parties or qualified staff independent of those that develop or maintain the security program.
- **Management should review test results** promptly and should take appropriate steps to address adverse test results.

The reports generated by vulnerability scans, assessments, penetration tests, and other measures, provide important insights. This documentation, along with subsequent remediation efforts should be organized and made available to the board committee responsible for GLBA compliance as well as for review by third-party auditors and examiners.

*The American Institute of Certified Public Accountants (AICPA) has established Statement on Auditing Standards (SAS) no. 70 –Service Organizations to provide authoritative guidance on the criteria used to evaluate the control processes of service providers. Choosing qualified service providers that are compliant with SAS-70 audit standards is one way to demonstrate due diligence in the selection of service providers.*

## 5. Oversee your service providers

Ensure that you exercise due diligence in selecting service providers. Include a review of the measures taken by a service provider to protect customer information, and list vendor(s) and the type of data that is shared with them. Ensure that contracts require service providers to implement appropriate measures to meet the objectives of GLBA. If your risk assessment dictates that it is prudent, ensure that for each applicable service provider:

- **The service provider has sufficient reporting** to allow you to appropriately evaluate their performance and security, both in ongoing operations and when malicious activity is suspected or known.
- You adequately control information supplied to the service provider, ensuring that the information is managed and secured properly.
- **Vendor management policies and procedures are adequate**, and document your reviews of service provider audits, test results, or other equivalent evaluations.
- The service provider is financially sound.

## 6. Update your Information Security Program as needed

The requirements of GLBA must be considered as changes in technology used, and its business function change. Such changes may include:

- Technology (e.g., software patches, new attack technologies and methodologies).
- Sensitivity of information.
- Threats (both nature and extent).
- Business arrangements (e.g., mergers and acquisitions, alliances and joint ventures, outsourcing arrangements).
- Customer information systems (e.g., new configurations or connectivity, new software).

The use of appropriate expertise is necessary to evaluate whether changes to your information security program are necessary. It is also essential that appropriate controls are implemented to ensure changes to the information security program are properly implemented in a timely, risk-based manner, thereby avoiding any potential lapses in the protection of customer information.

*Reviewing GLBA compliance is an ongoing issue – ensure that your board/committee reviews reports at least annually.*

### **Trust your network to SecurePipe**

- *Professional network security services since 1996*
- *Remote management of devices across six continents*
- *Compliant with SAS-70 audit standards*

**Network Operations Center  
Madison Wisconsin**

**[www.SecurePipe.com](http://www.SecurePipe.com)  
866.800.8901**

**Our business  
is securing yours.**

**SECURE PIPE**  
MANAGED NETWORK SECURITY

## **7. Prepare periodic reports to keep your board informed**

Based on input from their designated committee, the board of directors should review and update the information security program on an annual basis. In the course of this review, the board and its designated committee should review reports provided by management that adequately describe the following issues:

- The overall status of your information security program.
- Documentation concerning your enterprise-wide risk assessment.
- A discussion of material risks, risk management and control decisions.
- Evidence concerning service provider criteria, selection and oversight.
- Results of periodic testing, along with actions to address adverse results.
- A summary of any security breaches and management's response.
- Recommendations for program changes.

### **Summary**

The security requirements of the GLBA are numerous and will require a range of staff resources on an ongoing basis to review, document and ensure compliance as appropriate. Many companies lack the security expertise to research, implement, test and monitor their security requirements for GLBA, and rely on managed security service providers such as SecurePipe to complement their internal staff in order to help ensure they are in compliance with GLBA and other regulatory requirements.

### **About SecurePipe**

SecurePipe delivers managed network security services to financial institutions and enterprise clients wrestling with escalating regulatory compliance requirements. A best-of breed blend of disciplined process, expert people and proven technology underlies SecurePipe's comprehensive suite of managed services which are delivered from our network operations center staffed 24x7x365 by security engineers. No other managed network security service offers a comparable breadth and depth of services at such an affordable price.