# Global Information Assurance Certification Paper

**Gramm Leach Bliley Act of 1999**
**What Information Security Professionals Need to Know**
**By Marion Lang**
**GSEC (v1.2)**

July 1st, 2001 is fast approaching. If you are an information security professional working at a financial institution, you probably already heard about the Gramm Leach Bliley Act of 1999 (referred here as GLBA or the Act) and also known as the Financial Services Modernization Act of 1999. Everyone in the banking industry knows about the part of the Act that requires banks to develop privacy notices and give their customers the option to prohibit the banks from sharing their customer information with non affiliated third parties. But, did you know that the Act also requires financial institutions to have a comprehensive written information security program in place by July 1, 2001. Hopefully, you already have one or are well along the way to finalizing your program by the deadline. Dan Juneau at CastleGarde, a provider of information security solutions, stated in an interview with this writer that many financial organizations he talked to are not prepared for or are unaware of the information security program requirements of the Act.

Whether the Office of the Comptroller of the Currency (OCC), the Federal Reserve System (Fed), the Federal Deposit Insurance Corporation (FDIC) or the Office of Thrift Supervision (OTS) is your supervisory authority you better be ready before your next bank examiners' audit. Is your financial institution ready?

The Fed, OTS, OCC and FDIC published a joint final rule entitled "Interagency Guidelines Establishing Standards for Safeguarding Customer Information". [1] By attaching the guidelines as an appendix to their safety and soundness regulations, the agencies made it clear that complying with the guidelines, or the failure to do so, would affect the safety and soundness of the institution. Since all four agencies agreed on a common terminology and interpretation of the Act with only slight differences, luckily for us, financial institutions have virtually the same requirements to comply with the Act.

## SCOPE and PURPOSE of ACT

The GLBA applies to all national banks and federal branches of foreign bank that are subject to the supervision of the Fed, OTS, OCC or FDIC. The purpose of the Act is to the protection of customer information.

## DEFINITIONS

[1] Federal Register 12 CFR Part 30, et al. Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness; Final Rule http:\\www.ots.treas.gov/rules.html (February 1, 2001)

Since the terminology used in the Act can be a little confusing, it's important to first understand the following key terms and phrases used throughout the Act.

- Customers and consumers
- Customer information
- Customer Information System
- Nonpublic personal information
- Service provider

The guidelines define the difference between a consumer and a customer as follows. "Under the Privacy Rule, a **customer** is a **consumer** who has established a continuing relationship with an institution under which the institution provided one or more financial products or services to the **consumer** to be used primarily for personal, family or household purposes. **Customer** does not include a business, nor does it include a **consumer** who has not established an ongoing relationship with a financial institution (e.g., an individual who merely uses an institution's ATM or applies for a loan). See sections _.3(h) and (i) of the Privacy Rule." It is very important to remember that the GLBA does not apply to business entities.

**Customer information** is defined as "any records containing nonpublic personal information, as defined in section _.3(n) of the Privacy Rule for each Agency, about a customer." Since the GLBA refers to the protection of customer records and information, the guidelines uses **customer information** to refer to both information and records.

In the FDIC's Privacy Rule Handbook[2] **nonpublic personally identifiable information** is defined as personally identifiable financial information that is not available publicly and is either created or contains nonpublic personal information. Examples of nonpublic personally identifiable information would be lists containing such information as loan balances or overdraft information. While a list of public personal information would only contain such things as name, address, phone number and other publicly available types of account information (such as mortgages) held at the bank.

**Customer information system** is defined to be "any methods used to access, collect, store, use, transmit, protect, or dispose of customer information."

The guidelines define a **service provider** as "any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to you" the bank.

## STANDARDS for SAFEGUARDING CUSTOMER INFORMATION

*1. Written Information Security Program*

[2] FDIC Privacy Rule Handbook http://www.fdic.gov/news/financial/2001/fil0103a.html (January 22, 2001)

Each financial institution is required to implement a comprehensive written information security program that includes the following types of safeguards appropriate to the size and complexity of the institution and the nature and scope of its activities:

- Administrative
- Technical
- Physical

This requirement extends to the bank's subsidiaries as well. The subsidiaries either need to implement their own program or be part of a uniform program covering both the bank and its subsidiaries. However, the elements of the program must be coordinated.

*2. Objectives*

The information security program must be designed to protect customer information by:

- Ensuring security and confidentiality of the data
- Protect against any risks to data
- Protect against unauthorized access or use of information that could harm customer

The objectives outlined above describe a comprehensive information security program based on best practices in our industry; however, note that the emphasis is on securing customer information.

**DEVELOP and IMPLEMENT a CUSTOMER INFORMATION SECURITY PROGRAM**

*1. Involve the Board of Directors & Report Annually*

The Board of Directors is responsible for approving the institution's written information security policy and program and overseeing the development, implementation and maintenance of the program. Note that the Board of Directors can assign an appropriate committee to approve the written security program and also permits the board to assign specific implementation responsibilities to either a committee or an individual.

The institution is not required to have an Information Security Officer however; they do need to staff appropriately based on the risk to its customer information. However, the lines of authority and responsibility for developing and implementing the information security program need to be well defined and clearly articulated.

At least annually management must provide a written report on the information security program to the Board of Directors or the appropriate committee. The more complex the program is, or if there is a material change to the program, the board should be advised on a more frequent basis.

*2. Assess, Manage and Control Risk*

Each financial institution is responsible for assessing, managing and controlling the risk to their customers' information. First and foremost, the Act requires the bank to design an information security program that adequately protects customer information based on the complexity and scope of the bank's activity. For example given the inherent risks of the Internet, banks that have Internet banking capabilities have a much higher potential risk to customer information than a traditional bricks and mortar bank.

Each institution must consider the following eight factors when designing their information security program. While they do not have to implement every suggestion, they need to adopt the appropriate ones for their bank's size and complexity.

The eight factors for protecting customer information are:

- Access control
- Physical security at locations where customer information is stored
- Encryption of electronic customer information (especially in transit)
- Implement a change management process for customer information system modifications
- Dual control, segregation of duties and employee background checks for employees with access to customer information
- Monitoring systems and procedures to detect any actual or attempted attacks or intrusions on customer information systems
- Develop an incident response program for how to handle attempted and actual unauthorized access to customer information
- Disaster recovery program for the protection against destruction of customer information due to physical hazards and technical failures

*3. Employee Training*

The Act requires all employees to attend security awareness training. While the initial scope of this Act is to safeguard customer information, the agencies amended the provision to require security awareness training to support the information security program in general, not just customer information. However, special emphasis in the security awareness training should include a component to train employees to about what they need to do to protect customer information. While most banks will have a separate GLBA and suspicious activities training classes, a part of the security awareness training should also cover safeguarding customer information. This part of the security awareness training should be considered to be a complementary training component to the other classes.

*4. Test and adjust program*

Each institution's information security program must regularly test the information security procedures and controls. The guideline gave the institutions some flexibility on the frequency leaving it up to discretion of management based on the results of the required risk assessment. However, any time there is a significant internal or external change to the security environment the program should be tested again. Independent

third parties, either internal or external, must conduct the testing and review. They should never be conducted or reviewed by the group or individuals operating or managing the system

The guidelines further require the institution to monitor, evaluate and adjust the information security program itself. Security professionals must keep current with new security technologies, any changes in the sensitivity of its customer information, and internal or external threats to their information security.

*5. Service Provider Arrangements*
When an institution uses a service provider they still have a responsibility to safeguard their customers' information while in the possession of the service provider. The financial institution must determine that the server provider has adequate controls to ensure that the service provider will protect the customer information in a way that meets the objectives of the Guidelines. To do this the institution must use due diligence in selecting, managing and monitoring the outsourcing arrangement to insure that their customers' information is protected including entering into contracts with the service providers when appropriate. Even if monitoring the service provider is warranted by the institution's risk assessment, the Act does not require on-site inspections. Reviews of SAS70s, audits, or other test results can be used to assess the service provider's level of information security.

The financial institutions have until July 1st, 2003 to bring their current outsourcing contracts into compliance. However, all contracts entered into after February 17th, 2001 must be in compliance at the onset.

*6. Implement the Standards*
As part of the Privacy Rule all financial institutions must disclose their policies and practices in regard to protecting their customers information. For this reason, the guidelines require the institutions to comply with the information security requirements of this Act by July 1st, 2001 as well. Otherwise the institution would need to provide an initial privacy notice stating how they safeguard customer information and then provide an amended privacy notice as soon as they are in full compliance.

## CONCLUSION

Patrick Thibodeau summed up the four requirements of an information security program under GLBA very nicely in his recent magazine article as follows:

"**Risk assessment**: Identify and assess risk.
**Put it in writing:** Policies and procedures for controlling risk are required.
**Update:** Keep pace with technology and threats.
**Make sure it works:** Implement and test the plan"[3]

[3] Thibodeau, Patrick "Feds Set Financial Security 'Guidelines'". (January 22, 2001) URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO56645,00.html

HIPPA and GLBA are great news for information security professionals. Both Acts require their respective industries to design and implement a comprehensive information security program. If your financial institution did not have a formal program in place before GLBA, now you finally have legislation to help you get one in place. However, there are only a couple of months left before all financial institutions need to be in full compliance.

Considering that European standards of privacy are more stringent than the United States and that European corporations are putting on U.S. corporations that do business in Europe, many privacy experts feel that the GLBA may be only the beginning of many privacy acts to come.

**References**


Public Law 106-102, 106th Congress, 1st Session
Gramm-Leach-Bliley Act of 1999 Title V Sections 501 and 505(b)
URL: http://www.finmod.state.tx.us/content/theact/title5.pdf (November 12, 1999)

Federal Register 12 CFR Part 30, et al.
"Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness: Final Rule"
URL: http://www.ots.treas.gov/rules.html Click on pdf # 73112 (February 1, 2001)

FDIC FIL-3-2001: Privacy of Consumer Financial Information "Privacy Rule Handbook"
URL: http://www.fdic.gov/news/news/financial/2001/fil0103a.html (January 22, 2001)

Office of Thrift Supervision's Memorandum to Chief Executive Officers titled
"Privacy Preparedness Check-up"
URL: http://www.ots.treas.gov/docs/48467.pdf (September 29, 2000)

Privacy Headquarters "Safeguarding Customer Information"
URL: http://www.privacyheadquarters.com/glb/a_safeguard.html

Privacy Headquarters "Glossary to Key Terms under the Privacy Regs"
URL: http://www.privacyheadquarters.com/tools/glossary.html

Thibodeau, Patrick "Feds Set Financial Security 'Guidelines'". (January 22, 2001)
URL: http://www.computerworld.com/cwi/story/0,1199,NAV47_STO56645,00.html