

GRAMM—LEACH—BLILEY ACT

PROVISIONS OF THE ACT DEALING WITH THE OBLIGATION TO SAFEGUARD CUSTOMER INFORMATION AND THE IMPLICATIONS FOR FINANCIAL INSTITUTIONS

ABSTRACT

The Gramm—Leach—Bliley Act of 1999 states that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information. The Act charges agencies with regulatory oversight responsibilities to establish appropriate standards for administrative, technical, and physical safeguards. The agencies have adopted "Guidelines Establishing Standards to Safeguard Customer Information". Banks were required to "...implement an information security program pursuant to these Guidelines by July 1, 2001". (Paragraph III.G.1) The agencies and the Federal Financial Institutions Examination Council have issued guidelines to support the examination and audit of the safeguards put in place by financial institutions. The regulations and the examination standards are the needs against which security tools can be measured.

INTRODUCTION

The Gramm—Leach—Bliley Act of 1999 sets out the current structure and regulatory requirements for the financial services industry. The subject of Title V of the Act is PRIVACY. Subtitle A (Sections 501—510), "Disclosure of Nonpublic Personal Information", places the obligation to protect nonpublic personal information on financial institutions. The various Federal agencies with financial industry regulatory responsibilities are charged with establishing information safeguard standards. Section 501, is short, but powerful, and is quoted here in its entirety:

"SEC. 501. PROTECTION OF NONPUBLIC PERSONAL INFORMATION.

(a) PRIVACY OBLIGATION POLICY.—It is the policy of the Congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information.

(b) FINANCIAL INSTITUTIONS SAFEGUARDS.—In furtherance of the policy in subsection(a), each agency or authority described in section 505(a) shall establish appropriate standards for the financial institutions subject to their jurisdiction relating to administrative, technical, and physical safeguards—

(1) to insure the security and confidentiality of customer records and information;

(2) to protect against any anticipated threats or hazards to the security or integrity of such records; and

(3) to protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.”

REGULATORY STRUCTURAL BACKGROUND

Several Federal agencies are charged with regulatory oversight responsibility for various sectors of the financial services industry. They are:

1. The Office of the Comptroller of the Currency,
2. The Board of Governors of the Federal Reserve System,
3. The Board of Directors of the Federal Deposit Insurance Corporation,
4. Director of the Office of Thrift Supervision,
5. The Board of the National Credit Union Administration,
6. The Securities and Exchange Commission,
7. The Federal Trade Commission, and
8. Applicable State insurance authorities.

The Federal Financial Institutions Examination Council (FFIEC) is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System ([FRB](#)), the Federal Deposit Insurance Corporation ([FDIC](#)), the National Credit Union Administration ([NCUA](#)), the Office of the Comptroller of the Currency ([OCC](#)), and the Office of Thrift Supervision ([OTS](#)) and to make recommendations to promote uniformity in the supervision of financial institutions. The FFIEC and the member agencies have created the necessary regulations to implement information safeguard requirements of the Gramm—Leach—Bliley Act.

INFORMATION SAFEGUARD REGULATIONS

The member agencies have published “Guidelines Establishing Standards to Safeguard Customer Information”. The Guidelines became effective July 1, 2001. The Guidelines “...address standards for developing and implementing administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.” (Interagency Guidelines) (A copy of the Guidelines as published by the Federal Reserve System is attached.)

Bank compliance with the standards is mandatory. While the title of the interagency document is “Interagency Guidelines for Establishing Standards For Safeguarding Customer Information”, the word “Guidelines” should not be interpreted as meaning optional. The mandatory nature is clear from the content. “Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities.” (Guidelines, Paragraph II.A) Elements of a security program may vary based on individual bank situations, but the security program is mandatory. The discussion of the comments received during the comment cycle before adoption confirms this mandatory intent. (Federal Register/ Vol. 66, No 22/Thursday, February 1, 2001/Rules and Regulations, beginning at page 8616.)

The FFIEC has issued a booklet entitled “Information Security—IT Examination Handbook, December 2002”, to support the examination functions of the various participating agencies. The agencies have issued their own information and direction to the institutions they regulate.

The Federal Reserve provides a good illustration of the oversight exercised in the information security area. The Federal Reserve transmitted the interagency guidelines to the District Federal Reserve Banks in a letter dated May 31, 2001, along with guidance for Federal Reserve examiners. The second paragraph of the letter addresses the heart of the issue.

“The Guidelines require institutions to establish an information security program to assess and control risks to customer information. Under the Guidelines, each institution may implement an information security program appropriate to its size and complexity and the nature and scope of its operations. The board of directors should oversee an institution's efforts to develop, implement, and maintain an effective information security program and approve written information security policies and programs.”

THE REQUIREMENTS FOR SAFEGUARDING CUSTOMER INFORMATION CONTAINED IN THE REGULATIONS

Although the Interagency Guidelines are worth reading in their entirety, a few extracts outlining the requirements for information protection are quoted here for convenience and emphasis:

“II. Standards for Safeguarding Customer Information

- A. *Information Security Program.* Each bank shall implement a comprehensive written information security program that includes administrative, technical, and physical safeguards appropriate to the size and complexity of the bank and the nature and scope of its activities...
- B. *Objectives.* A bank's information security program shall be designed to:
 - 1. Ensure the security and confidentiality of customer information;
 - 2. Protect against any anticipated threats or hazards to the security or integrity of such information; and
 - 3. Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

III. Development and Implementation of Information Security Program

- C. *Manage and Control Risk.* Each bank shall:
 - 1. Design its information security program to control the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope of the bank's activities. Each bank must consider whether the following security measures are appropriate for the bank and, if so, adopt those measures the bank concludes are appropriate:
 - a. Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer information to unauthorized individuals who may seek to obtain this information through fraudulent means.
 - b. Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals;
 - c. Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
 - d. Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
 - e. Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information;
 - f. Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems;
 - g. Response programs that specify actions to be taken when the bank suspects or detects that unauthorized individuals have gained access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
 - h. Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures.

D. *Oversee Service Provider Arrangements.* Each bank shall:

1. Exercise appropriate due diligence in selecting its service providers;
2. Require its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines; and
3. Where indicated by the bank's risk assessment, monitor its service providers to confirm that they have satisfied their obligations as required by paragraph D.2. As part of this monitoring, a bank should review audits, summaries of test results, or other equivalent evaluations of its service providers.

As part of its regulatory oversight function, the Federal Reserve System has issued instructions for its examiners. The instructions include a list of examiner questions that closely follow the points contained in the guidelines.

The FFIEC's booklet, "Information Security—IT Examination Handbook, December 2002", "...follows the same process-based approach, applies it to various aspects of the financial institution's operations, and serves as a supplement to agency GLBA 501(b) expectations." (Pages 1, 2) This booklet provides additional, clarifying direction for safeguarding personal, nonpublic information. It includes, among others, the following topics:

1. Electronic and Paper-Based Media Handling
2. Logical and Administrative Access Control,
3. Encryption; Systems Development, Acquisition, and Maintenance,
4. Service Provider Oversight,
5. Logging and Data Collection.