Title: Gramm-Leach-Bliley Act
Code: 5-100-100
Date: 5-15-04
Approved: WPL

Introduction

Signed into law by President Clinton on November 12, 1999, the Gramm-Leach-Bliley Act (GLB Act or the Act [15 USC § 6801]) reforms and modernizes the banking industry by permitting banks to engage in a variety of financial activities previously restricted by the Glass-Steagall Act and the Bank Holding Company Act of 1956. Additionally, the Act requires financial institutions to take steps to ensure the security and confidentiality of customer records and information. Colleges and universities, defined as financial institutions for purposes of the Act, are not subject to the *privacy* provisions of the Act if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). However, higher education institutions are subject to the provisions of the Act related to the administrative, technical, and physical *safeguarding* of customer records and information.

On May 23, 2002, the Federal Trade Commission (FTC) issued a final rule, "Standards for Safeguarding Customer Information" (Safeguards Rule [16 CFR 314]), which requires all covered financial institutions to have in place by May 23, 2003, a comprehensive, written information security program.

The general policies and procedures that follow have been formulated to facilitate Boston College's implementation of the requirements of the GLB Act.

Definitions

Customer information is defined by the Safeguards Rule as any record containing **nonpublic personal information**, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of the institution or its affiliates, about a customer of that institution. **Nonpublic personal information** is defined by the FTC's GLB Act Privacy Rule (16 CFR 313) to include **personally identifiable financial information**, which in turn is defined as any information a consumer provides to obtain a financial product or service from the institution, or that results from or is otherwise obtained in connection with a financial product or service transaction. In general, **customer information** would include names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and Social Security numbers that are provided to obtain a financial product or service. The **financial products or services** offered by a college or university include making student loans and other miscellaneous financial services as defined by the implementing regulations for the Bank Holding Company Act of 1956 (12 CFR 225.28)

Information security program is defined by the Safeguards Rule as the administrative, technical, or physical safeguards used by a financial institution to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Service provider is defined by the Safeguards Rule as any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a financial institution.

Policy

Boston College complies with the requirements of the Gramm-Leach-Bliley Act. The requirements of the Act are as follows:

1. Each covered financial institution is to develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the institution, the nature and scope of its activities, and the sensitivity of any customer information at issue. Safeguards are to be reasonably designed to achieve the following objectives:

   (a) To insure the security and confidentiality of customer information;

   (b) To protect against any anticipated threats or hazards to the security or integrity of such information; and

   (c) To protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

2. In developing, implementing, and maintaining the information security program, each covered institution is to:

   (a) Designate an employee or employees to coordinate the program.

   (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information; and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment is to include consideration of risks in each relevant area of an institution's operations, including:
      - Employee training and management;
      - Information systems, including network and software design, as well as information processing, storage, transmission, and disposal; and
      - Detecting, preventing, and responding to attacks, intrusions, or other systems failures.

   (c) Design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

   (d) Oversee service providers by:
      - Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and
      - Requiring service providers by contract to implement and maintain such safeguards.

   The Safeguards Rule provides for a two-year grandfathering of service contracts. Until May 24, 2004, a contract entered into with a nonaffiliated third party to perform services for an institution, or to function on behalf of an institution, satisfies the provisions of paragraph (2)(d), even if the contract does not include a requirement that the service provider maintain appropriate safeguards, as long as the contract was entered into not later than June 24, 2002.

(e) Evaluate and adjust the information security program in light of the results of the testing and monitoring required by paragraph (2)(c); any material changes to operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on the information security program.

Please see EXHIBIT A, the "Boston College Gramm-Leach-Bliley Act Information Security Program."

The University General Counsel has overall responsibility for implementing, monitoring, and enforcing the provisions of this policy.

Posted: May 21, 2004
