Title: Gramm-Leach-Bliley Act (GLBA) Standard

1. Overview

The Gramm-Leach-Bliley Act (GLBA) addresses the safeguarding and confidentiality of customer information held in the possession of financial institutions. It applies to higher education institutions because colleges and universities participate in certain types of financial activities that are defined in banking law. Administering federal student loans is one of the main types of activities that pull institutions under the GLBA umbrella. The law includes rules on how financial institutions have to protect consumer financial information. The GLBA separates individual privacy protection into three principal categories These rules are known as the Privacy Rule, the Safeguards Rule, and the Pretexting Rule.

2. Purpose

Ensure compliance with the Gramm-Leach-Bliley Act (GLBA).

3. Scope

The scope of GLBA compliance for institutions of higher education is student financial aid information. This standard expands the scope by applying to all information and information systems, institutional data, and networks of Middle Georgia State University and any person or device that gains access to these systems or data.

4. Standard

Privacy Rule

Colleges and universities do not entirely fit the traditional model of a financial institution. As a result the FTC has provided some flexibility on the privacy side.

The Privacy Rule regulations promulgated by the FTC specifically state that colleges and universities are deemed to be in compliance with the rule if they are in compliance with the Family Educational Rights and Privacy Act (FERPA). Thus, colleges and universities do not have to bear the unique burdens of the Privacy Rule in addition to those they must already address under FERPA.

MGA shall develop, implement, and maintain a comprehensive Privacy Program defined by policies, standards and procedures which include FERPA as a primary component. In addition, MGA shall designate a Chief Privacy Officer to coordinate the institution's Privacy Program.

Safeguards Rule

Higher education compliance with the Safeguards Rule, however, was not similarly exempted. In July 2015, the Federal Student Aid (FSA) Office of the U.S. Department of Education released new guidance (GEN 15-18) for colleges and universities on the security of student financial aid information. On July 2016, GEN-16-12 followed emphasizing Gramm-Leach-Bliley Act

(GLBA) compliance by stating that it will soon begin holding institutions accountable for fulfilling GLBA Safeguard Rule requirements. Spring 2017 the U.S. Department of Education announced GLBA Safeguard Rule is required for the Student Financial Assistance program (SFA) beginning January 1, 2018.

MGA shall develop, implement, and maintain a comprehensive Cybersecurity Program defined by policies, standards and procedures aligned with the standards and elements of the Safeguards Rule listed below.

§314.3 Standards for safeguarding customer information:

(a) Information security program. You shall 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 your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue. Such safeguards shall include the elements set forth in §314.4 and shall be reasonably designed to achieve the objectives of this part, as set forth in paragraph (b) of this section.

(b) Objectives. The objectives of section 501(b) of the Act, and of this part, are to:
   (1) Insure 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.

§314.4 Elements

In order to develop, implement, and maintain your information security program, you shall:

(a) Designate an employee or employees to coordinate your information security 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 should include consideration of risks in each relevant area of your operations, including:
   (1) Employee training and management;
   (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and
   (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

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

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

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

Pretexting Rule

Pretexting (sometimes referred to as "social engineering") occurs when someone tries to gain access to personal nonpublic information without proper authority to do so. This may entail requesting private information while impersonating the account holder, by phone, by mail, by email, or even by "phishing" (i.e., using a phony website or email to collect data). GLBA encourages the organizations covered by GLBA to implement safeguards against pretexting.

As part of the MGA Privacy Program, procedures from USG IT Handbook Section 5.14 "Identity Theft Prevention - Red Flag Rule" shall be implemented.

5. Enforcement

If an institution receives a GLBA audit finding based on regulations in 16 CFR Part 314 , the finding will be included in the audit report that the Department of Education's Office of Federal Student Aid (FSA) receives. FSA in turn will share the finding with the Federal Trade Commission (FTC) as well as its internal Cybersecurity Team (CT). If the CT thinks the situation is particularly egregious, it may cut off access to FSA systems and refer the issue to FSA's administrative compliance unit for a fine or some other form of administrative action.

Audit objectives are detailed in (OMB) Compliance Supplement (FY19) as follows:

Audit Objectives

Determine whether the institution designated an individual to coordinate the information security program; performed a risk assessment that addresses the three areas noted in 16 CFR 314.4 (b) and documented safeguards for identified risks.

Expected Audit Procedures

(a) Verify that the institution has designated an individual to coordinate the information security program.
(b) Verify that the institution has performed a risk assessment that addresses the three required areas noted in 16 CFR 314.4 (b), which are (1) Employee training and management; (2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and (3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.
(c) Verify that the institution has documented a safeguard for each risk identified from step b above.

Other Policies and Procedures

This standard incorporates by reference the following policies, standards and procedures:
URL: https://www.usg.edu/policymanual/section10/C442

- BOR Policy Manual 10.4.2 - Institutional- and Organizational-Level Responsibilities

URL: https://www.usg.edu/business_procedures_manual/section12/C2828

- University System of Georgia Business Procedures Manual

URL: https://www.usg.edu/information_technology_services/it_handbook/

- University System of Georgia IT Handbook Section 5.14 Identity Theft Prevention - Red Flag Rule

6. Revision History

02/26/2020 - Draft