Law/Act:	Gramm-Leach-Bliley Act (aka Financial Services Modernization Act of 1999)	
U.S. Code Citation:	15 U.S.C. §§ 6801-6809	
Code of Federal Regulations Citation:	16 C.F.R. pts. 313-314	
Responsible Regulator(s):	Federal Trade Commission (FTC) Consumer Financial Protection Bureau (CFPB)	
BYU–Hawaii Responsible Officer(s)	Vice President for Administration	
	Updated: Feb. 2017	Updated By: DMA
	Version 2.0	Effective Date: Nov. 12, 1999

I. PURPOSE

The Gramm-Leach-Bliley Act (GLBA) is a federal law that imposes on "each financial institution . . . 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."[1] In fulfilling this purpose, GLBA established (1) a "Privacy Rule" that requires financial institutions to provide notice of their information-sharing practices to customers and gives customers the right to "opt out" of certain information sharing practices;[2] and (2) a "Safeguards Rule" that requires financial institutions to have specific measures in place to keep customer information secure.[3]

II. HISTORY

In response to the financial failures of the Great Depression, Congress passed the Glass-Steagall Act in 1933 to prohibit commercial banks from affiliating with securities companies.[4] Subsequent acts and revisions resulted in many American banks with unregulated privacy standards and a lack of consumer protection against unwanted information sharing.[5] After a series of high profile cases involving banks selling consumer information with adverse consequences for customers—including credit fraud and identity theft— GLBA was introduced by Senator Phil Gramm and Representatives James Leach.[6] GLBA was signed by President Bill Clinton on November 12, 1999.[7] The Federal Trade Commission (FTC) has promulgated implementing regulations under the GLBA, including regulations governing (1) the Privacy Rule, which took effect on July 1, 2001 and were recently amended in 2009;[8] and (2) the Safeguards

[1] 15 U.S.C. § 6801(a) (2016); *see also generally* FEDERAL TRADE COMMISSION, GRAMM-LEACH-BLILEY ACT, http://business.ftc.gov/tips-advice/privacy-and-security/gramm-leach-bliley-act (last visited Feb. 21, 2017) (outlining the purpose, scope, and requirements of the GLBA).

[2] 15 U.S.C. §§ 6802–6803 (2016); 16 C.F.R. pt. 313; *see also* FEDERAL TRADE COMMISSION, HOW TO COMPLY WITH THE PRIVACY OF CONSUMER FINANCIAL INFORMATION RULE OF THE GRAMM-LEACH-BLILEY ACT, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (last visited Feb. 21, 2017).

[3] 15 U.S.C. § 6801(b) (2016); 16 C.F.R. pt. 314; *see also* FEDERAL TRADE COMMISSION, FINANCIAL INSTITUTIONS AND CUSTOMER INFORMATION: COMPLYING WITH THE SAFEGUARDS RULE, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited Feb. 21, 2017) [hereafter SAFEGUARDS GUIDANCE].

[4] The Gramm-Leach-Bliley Act, ELECTRONIC PRIVACY INFORMATION CENTER, http://epic.org/privacy/glba/ (last visited Feb. 21, 2017).

[5] *Id.*

[6] *Id.*

[7] Gramm-Leach-Bliley Act, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

[8] 16 C.F.R. pt. 313.

Rule, which took effect on May 23, 2003.[9] The Consumer Financial Protection Bureau (CFPB) also has adopted implementing regulations with respect to entities under its jurisdiction.

III. APPLICABILITY TO BYU–HAWAII

Any institution that is "significantly engaged in financial activities" is considered a "financial institution" that is subject to GLBA.[10] "Financial activities" are broadly defined, encompassing things such as "lending, exchanging, transferring, investing for others, or safeguarding money."[11] GLBA does not apply to all information collected in business or commercial activities.[12] For example, "a retailer is not a financial institution merely because it accepts payment in the form of cash, checks, or credit cards that it did not issue."[13]

"The FTC has made it clear that it considers educational institutions to be 'financial institutions' subject to its jurisdiction for purposes of GLBA."[14] Further, the Department of Education (ED) requires universities to comply with GLBA in their Program Participation Agreements. On July 1, 2016, ED issued a Dear Colleague Letter with guidance on universities' GLBA compliance obligations.[15]

BYU–Hawaii likely would be considered a "financial institution" because the university engages in financial activities with, and collects and maintains financial information about, students and others. These activities include, for example, administering student loans and other financial aid programs. Also, BYU–Hawaii has entered into a Program Participation Agreement, through which BYU–Hawaii expressly agreed to comply with the Safeguards Rule under GLBA.[16]

IV. REQUIREMENTS

GLBA establishes two general rules governing financial institutions: (1) the Privacy Rule and (2) the Safeguards Rule. As outlined below, universities are deemed compliant with the Privacy Rule if they comply with the Family Educational Rights and Privacy Act (FERPA).[17] However, universities are not exempt from the Safeguards Rule.[18]

A. Privacy Rule

Under the Privacy Rule, financial institutions are required to do the following to protect consumer financial information:

---

[9] Financial Services Modernization Act of 1999, THE CATHOLIC UNIVERSITY OF AMERICA, http://counsel.cua.edu/FEDLAW/glb.cfm (last updated June 15, 2015) [hereafter CUA GLBA].
[10] 16 C.F.R. § 313.3(k).
[11] 15 U.S.C. § 6809(3)(A); 12 U.S.C. § 1843(k)(4).
[12] 16 C.F.R. § 313.1(b) (GLBA "does not apply to information about companies or individuals who obtain financial products or services for business, commercial, or agricultural purposes.")
[13] *Id.* § 313.3(k)(4)(ii).
[14] National Association of College and University Counsel, NACUAlerts, *FTC's Gramm-Leach Bliley Act Safeguards Rule: Guidelines for Compliance*, Vol. 1, No 4. (May 16, 2003) (hereafter "NACUAlert").
[15] Ted Mitchell, Undersecretary, U.S. Department of Education, *Protecting Student Information* (JULY 1, 2016) (hereafter "2016 Dear Colleague Letter").
[16] Program Participation Agreement between the U.S. Department of Education and Brigham Young University (signed by Kevin J. Worthen on June 18, 2015) (on file with the Office of the General Counsel).
[17] 16 C.F.R. § 313.1(b).
[18] CUA GLBA, *supra* note 9.

1. Provide annual notice to customers about the institution's privacy policies and practices;[19]
2. Describe the conditions under which the institution may disclose nonpublic personal information[20] about consumers to nonaffiliated third parties;[21] and
3. Provide a method for consumers to opt out of personal information disclosures to most nonaffiliated third parties.[22]

The FTC suggests that a business determine if the company's clients are consumers or customers. [23] A consumer is any individual who obtains or has obtained a financial product or service from the institution that is used primarily for personal, family, or household purposes, or that individual's legal representative.[24] A customer, however, is a consumer who has a continuing customer relationship with a financial institution.[25]

The distinction between consumer and customer is important because only customers are entitled to receive a financial institution's privacy notice every year for as long as the customer relationship lasts.[26] On the other hand, financial institutions must provide consumers with a privacy notice only if the financial institution shares the consumers' information with nonaffiliated third parties.[27]

Because institutions of higher education must already comply with FERPA regulations, an exhaustive list of privacy requirements are not included in this research memo.[28] Once again, a university that complies with FERPA and its regulations is deemed to have met the Privacy Rule of GLBA.[29]

B. Safeguards Rule

The Safeguards Rule of GLBA sets forth "standards for developing, implementing, and maintaining reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information."[30] These provisions apply to not only customers with whom a university

---

[19] 15 U.S.C. § 6803(a); 16 C.F.R. §§ 313.6, 313.9. A sample notice is available. *See* 16 C.F.R. § 313 App. A.
[20] Nonpublic personal information includes personally identifiable financial information and any list, description, or other grouping of consumers (and publicly available information pertaining to them) that is derived using any personally identifiable financial information that is not publicly available. 16 C.F.R. § 313.3(n)(1)(i)-(ii).
[21] 15 U.S.C. § 6803(c)(1). A nonaffiliated third party is defined as any person except the financial institution affiliate; or a person employed jointly by the financial institution and any company that is not the institution's affiliate (but *nonaffiliated third party* includes the other company that jointly employs the person). *Id.* § 313.3(m)(1)(i)-(ii).
[22] 15 U.S.C. § 6802(b); 16 C.F.R. § 313.1(a)(1)-(3).
[23] In Brief: The Financial Privacy Requirements of the Gramm-Leach-Bliley Act, FEDERAL TRADE COMMISSION, http://business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act (last updated July 2002).
[24] 15 U.S.C. § 6809(9); 16 C.F.R. § 313.3(e)(1).
[25] 15 U.S.C. § 6809(11); 16 C.F.R. § 313.3(h).
[26] 16 C.F.R. § 313.5(a)(1).
[27] *Id.* § 313.4(b)(1).
[28] 16 C.F.R. § 313.1(b).
[29] *Id.* § 313.1(b).
[30] *Id.* § 314.1(a).

has a customer relationship, but also to customers of other financial institutions that have provided such information to a university.[31]

To comply with GLBA, an institution must develop, implement, and maintain a comprehensive information security program.[32] This program must be written in one or more readily accessible parts and must contain administrative, technical, and physical safeguards appropriate for the size, complexity, nature, and scope of the financial institution's activities.[33] The purpose of establishing and maintaining an information security program is 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."[34]

1. Required Elements of an Information Security Program

To establish a GLBA-compliant information security program, a financial institution must do the following:

1. **Designate Coordinator(s):** Designate an employee or employees to coordinate the institution's information security program.[35]
2. **Identify Risks:** Identify 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.[36]
3. **Assess:** Assess the sufficiency of any safeguards in place to control the internal and external risks, including, *at a minimum*, consideration of risks in each relevant area of the institution's operations, including (a) employee training and management; (b) information systems, including network design, software design, information processing, storage, transmission, and disposal; and (c) detecting, preventing, and responding to systems failures.[37]
4. **Design Safeguards:** Design and implement information safeguards to control the risks identified through the risk assessment.[38]
5. **Test:** Regularly test and monitor the effectiveness of the safeguards' key controls, systems, and procedures.[39]
6. **Evaluate:** Evaluate and adjust the information security program pursuant to the required testing and monitoring, material changes to the operation or business arrangements, or any other circumstances that may have a material impact on the information security program.[40]
7. **Oversee service providers:** A financial institution must select and retain service providers capable of maintaining appropriate safeguards for the customer information at issue.[41] This

[31] *Id.* § 314.1(b).
[32] *Id.* § 314.3(a).
[33] *Id.*
[34] *Id.* § 314.3(b).
[35] *Id.* § 314.4(a).
[36] *Id.* § 314.4(b).
[37] *Id.* § 314.4(b)(1)-(3).
[38] *Id.* § 314.4(c).
[39] *Id.*
[40] *Id.* § 314.4(e).
[41] *Id.* § 314.4(d)(1)-(2).

includes requiring the service providers by contract to implement and maintain such safeguards. A service provider includes any person or entity that receives, maintains, processes, or otherwise is permitted access to customer information through its provisions of services directly to a financial institution.[42]

2. FTC Recommended Best Practices

In addition to the above *required* elements of an information security program, the FTC also recommends numerous other procedural and technological best practices for an information security program, including the following, among others[43]:

1. Limit data access to those employees with a need to know.
2. Require employees to use strong passwords that must be changed on a regular basis.
3. Develop policies for appropriate use and protection of laptops, cell phones, and other mobile devices.
4. Train employees to take basic steps to maintain the security, confidentiality, and integrity of data.
5. Impose disciplinary measures for security policy violations.
6. Take appropriate measures to prevent terminated employees from accessing data.
7. Take steps to ensure the secure transmission of data (e.g. SSL, encryption).
8. Dispose of customer information in a secure way, including when disposing of electronic devices.
9. Take appropriate steps to prevent cybersecurity attacks (e.g. intrusion detection system, activity logs, monitoring large data transmission, use of dummy accounts).
10. Quickly diagnose and respond to security incidents, including securing data in the event of a breach and possibly notifying consumers, law enforcement, and/or businesses of such breach.
11. Maintain up-to-date programs and controls (anti-virus and anti-spyware software, firewalls, etc.)
12. Use appropriate oversight and audit procedures to detect improper disclosure and theft of data.

3. NIST Standards Strongly Encouraged by ED

The National Institute of Standards and Technology (NIST), part of the U.S. Department of Commerce, has developed its own information security standards in NIST Special Publication 800-171 (NIST Standard).[44] The NIST Standard contains recommended federal data security requirements for what is known as "controlled unclassified information"—generally any non-public information that is not considered classified.[45] In a Dear Colleague Letter regarding the application of GLBA to institutions of higher education, the U.S. Department of Education "strongly encourage[d]" institutions of higher education to comply with the NIST standard.[46] Also, certain federal contractors who enter into agreements with the U.S. Department of Defense are required to comply with the NIST standard by no later than December 31, 2017.[47] These NIST Standards include specific requirements for each of the following categories:

---

[42] *Id.* § 314.2(d).
[43] *See* SAFEGUARDS GUIDANCE, *supra* note 3.
[44] NIST, *Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations*, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171.pdf (last visited Jan. 23, 2017).
[45] *Id.*
[46] Ted Mitchell, Undersecretary, U.S. Department of Education, *Dear Colleague Letter: Protecting Student Information* (July 1, 2016).
[47] 48 C.F.R. § 252.204-7012(b)(2)(ii)(A).

1. **Access Control Requirements**—limit information system access to authorized users.
2. **Awareness and Training Requirements**—ensure that system users are properly trained.
3. **Audit and Accountability Requirements**—create information system audit records.
4. **Configuration Management Requirements**—establish baseline configurations and system inventories.
5. **Identification and Authentication Requirements**—identify and authenticate users appropriately.
6. **Incident Response Requirements**—identify and authenticate users appropriately.
7. **Maintenance Requirements**—perform appropriate maintenance on information systems.
8. **Media Protection Requirements**—protect media, both paper and digital, containing sensitive information.
9. **Personnel Security Requirements**—screen individuals prior to authorizing access.
10. **Physical Protection Requirements**—limit physical access to systems.
11. **Risk Assessment Requirements**—conduct regular risk assessments.
12. **Security Assessment Requirements**—assess security controls periodically and implement action plans.
13. **System and Communication Protection Requirements**—monitor, control, and protect communications
14. **System and Information Integrity Requirements**—timely identify, report, and correct information flaws

V. PENALTIES

While GLBA itself establishes no private right of action,[48] "to the extent the Safeguards Rule is interpreted as imposing a general duty on educational institutions to safeguard covered financial information, it may prove relevant in actions brought under general negligence law [and other] theories in response to failures to maintain the confidentiality of such information."[49]

The FTC is generally authorized to enforce GLBA. However, the FTC has no jurisdiction over non-profits.[50] Nevertheless, failure to comply with the regulations of GLBA could result in a loss of federal funding under Title IV based on the inclusion of GLBA requirements in the Program Participation Agreement.[51]

[48] *See, e.g.*, *Wood v. Greenberry Financial Servs., Inc.*, 907 F. Supp. 2d 1165 (D. Hawaii 2012) (holding that there is no private cause of action under GLBA); *Abdelfattah v. U.S. Dept. of Homeland Sec.*, 893 F. Supp.2d 75 (D.D.C. 2012) (same).
[49] NACUAlert, *supra* note 14.
[50] 16 C.F.R. § 314.1(b).
[51] *See* Program Participation Agreement, *supra* note 16.

VI. COMPLIANCE CALANDER

In order to comply with the GLBA Privacy Rule, a university must annually notify students of their rights under FERPA.[52] The GLBA Safeguards Rule requires financial institutions to "regularly test or otherwise monitor the effectiveness of" the information safeguards the institution has established.[53]

VII. STAYING UP-TO-DATE

The following websites provide valuable information regarding this law and its applicability.

DOCUMENT/REFERENCE	DESCRIPTION
Federal Trade Commission: Gramm-Leach-Bliley Act	Overview GLBA. Also contains updated news regarding GLBA and companies who have charges brought against them for violations of GLBA.
The Catholic University of America: Gramm-Leach-Bliley Act	Catholic University of America's summary of GLBA.
Electronic Privacy Information Center: The Gramm-Leach-Bliley Act	Information about the GLBA from the Electronic Privacy Information Center.
Federal Trade Commission: How to Comply with the Privacy of Consumer Financial Information rule of the Gramm-Leach-Bliley Act	How to Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act.
U.S. Government Publishing Office: Privacy of Consumer Financial Information	Privacy of Consumer Financial Information, 65 Fed. Reg. 33646.
Federal Trade Commission: Financial Institutions and Customer Information—Complying with the Safeguards Rule	Financial Institutions and Customer Information: Complying with Safeguards Rule.

[52] 15 U.S.C. § 6803(a) (requiring annual disclosures to customers); 34 C.F.R. § 99.7(a)(1) (setting forth equivalent requirement under FERPA).

[53] 16 C.F.R. § 314.4(c). The regulation states that the information security program should be developed and maintained in a manner that is "appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue." *Id.* § 314.3. Thus "regularly" may be interpreted differently for each financial institution.