SecureStrux

WHITE PAPER

Impact of GLBA on Higher Education

Fact: The Gramm-Leach Bliley Act (GLBA) Directly Impacts Institutions of Higher Education.

GLBA requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.[1] Therefore, GLBA security requirements apply to Institutions of Higher Education (IHE) as well, since IHE is considered a financial institution that collects, stores, and processes student financial records containing non-public personal information (NPI). Note that this differs from the Family Educational Rights and Privacy Act (FERPA) objectives, which are designed to protect the privacy of student education records. GLBA and FERPA are federal laws with two different scopes.

Background

GLBA was enacted in 1999 under the jurisdiction of the Federal Trade Commission (FTC) to regulate the collection, storage, and transmission of sensitive data by financial institutions. It consists of three sections: the Financial Privacy Rule, the Safeguards Rule, and the Pretexting provisions[1].

1. Financial Privacy Rule

This rule calls for financial institutions to provide customers with written information explaining what information is collected about them, how the information is used, how it's shared, and how it's protected.

2. Safeguards Rule

This rule calls for financial institutions to develop, implement, and maintain an information security program to include technical, administrative, and physical safeguards to protect sensitive customer information, whether handled in paper, digital, or other format on behalf of the customer.

3. Pretexting Protection Provisions

This provision calls for financial institutions to implement safeguards against pretexting, also known more commonly as social engineering.

Many of the changes since 1999 revolved around the Safeguards Rule where activity has picked up over the past four years and counting.

Enter Higher Education

Colleges and universities of all sizes must comply with GLBA. The Department of Education (DE), under the jurisdiction of Federal Student Aid (FSA), requires postsecondary institutions and third-party service providers to protect student financial aid information in support of the administration of the Federal student financial aid programs (Title IV programs).[2] Any IHE that participates in Title IV programs has agreed in its Program Participation Agreement (PPA) to comply with the GLBA Safeguards Rule under 16 C.F.R. Part 314.3

How it Impacts Colleges and Universities

Essentially, the impact is along the traditional lines of the Comply or Face the Consequences principle.

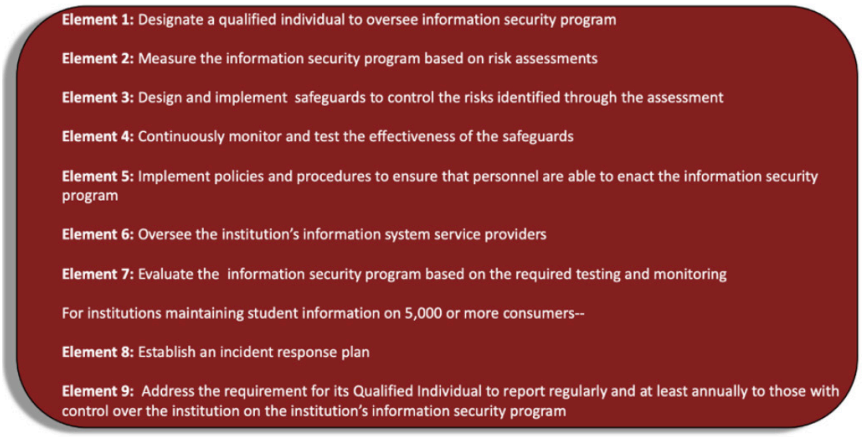
1. Comply with the Safeguards Rule

Since 2015, DE has been sending notices to IHEs reminding them of their GLBA safeguarding responsibilities. In 2020, the DE published an Electronic Announcement informing IHE that it will enforce the GLBA Safeguards Rule.

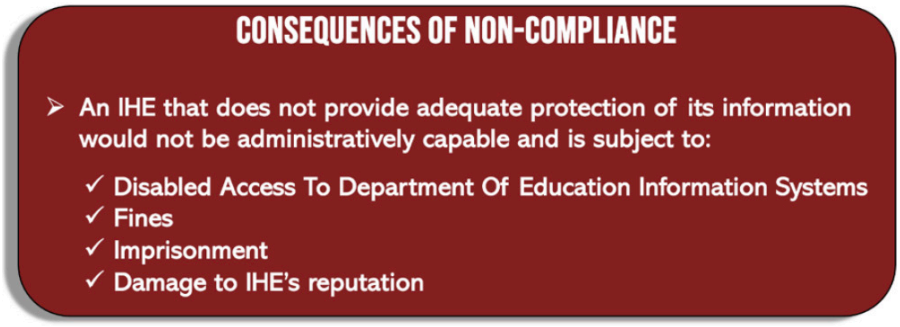
The objectives of the GLBA standards for safeguarding information are to[2]:

- Ensure the security and confidentiality of student information.
- Protect against any anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any student (16 C.F.R. 314.3(b)).

The Safeguards Rule consists of nine elements that must be met. For institutions with less than 5,000 consumers, only the first seven elements apply.



2. Face the Consequence of Non-Compliance



Is the GLBA Safeguards Rule enforceable? Yes—the intent is to add teeth to the Safeguards Rule for non-compliance.

Effective June 9, 2023, any GLBA findings discovered through a compliance audit will be resolved by the DE during the evaluation of the institution's information security safeguards as part of its final determination of an institution's administrative capability. GLBA-related findings will have the same effect on an institution's participation in Title IV programs as with any other determination of non-compliance.[2]

FSA's Postsecondary Institution Cybersecurity Team will also be informed of findings related to the GLBA Safeguards Rule and independently assess the level of risk to student data presented by the institution's information security system.

If the Cybersecurity Team determines that the IHE poses a substantial risk to the security of student data, the team may permanently or temporarily disable the IHE's access to the DE's information systems. Further, if the team determines that the IHE's administrative capability is impaired due to critical security weaknesses or it has a history of non-compliance, it may refer the IHE to the DE's Administrative Actions and Appeals Service Group for consideration of a fine or other appropriate administrative action.

What Can You Do?

Many colleges and universities are finding it difficult to meet the compliance requirements, but more specifically, face challenges finding the resources to dedicate to understanding and implementing the safeguarding requirements and its institutional responsibilities. There is a lot more activity required within each of the nine elements than is listed above, as they require specific administrative, operational, and technical security safeguards.

It's not too late to start now to get on board with the DE's requirements to comply with the GLBA Safeguards Rule. Contact SecureStrux for a free consultation today.

Sources

1. Gramm-Leach-Bliley Act, https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
2. Federal Student Aid (FSA), Electronic Announcement ID General-23-09, Subject: Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements, February 9, 2023, https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements
3. 16 C.F.R. Part 314, Standards for Safeguarding Customer Information, amended May 30, 2023, https://www.ecfr.gov/current/title-16/chapter-I/subchapter-C/part-314

Author

Tony Buenger (CCISO, CISSP, CISM, CGEIT)
Vice President, Cyber Advisory Services
SecureStrux

Former Chief Information Security Officer
Augusta University, Auburn University