Gramm-Leach-Bliley Act
Postsecondary Institution
Data Governance Considerations

Executive Summary

The Gramm–Leach–Bliley Act (GLBA) was designed to ensure financial institutions maintain appropriate data privacy practices that protect individuals' nonpublic personal information (NPI) collected by those institutions. The Federal Trade Commission (FTC) has determined that institutions of higher education (institutions) may qualify as financial institutions under GLBA. In February 2023, the Office of Federal Student Aid (FSA) of the US Department of Education (ED) issued two announcements regarding institutions and GLBA. On February 9, 2023, GENERAL-23-09 was released to explain the FTC's December 2021 amendment of the GLBA cybersecurity requirements, effective June 9, 2023. On February 28, 2020, another announcement detailed the FSA's enforcement of GLBA, stating that institutions participating in the FSA program must comply with the GLBA and report this compliance in their annual audit, asserting that "[e]ach institution has agreed to comply with GLBA in its Program Participation Agreement with the Department" (Federal Student Aid, 2020).

As part of the updated guidelines, auditors of postsecondary institutions are to include three information safeguard requirements in their audits as specified in the United States Department Of Education Office Of Inspector General's letter to auditors CPA-19-01. Under these requirements, the institution must:

- Designate an individual to coordinate its information security program.
- Perform a risk assessment that addresses three required areas:
  - 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.
- Document a safeguard for each risk identified in the risk assessment.

In addition to audit requirements, institutions must ensure compliance with the three sections of the GLBA: Privacy Rule, Safeguard Rule, and Pretexting Provision. The FTC has ruled that complying with the Family Educational Rights and Privacy Act (FERPA) satisfies the Privacy Rule requirement of the GLBA but does not satisfy the Safeguard Rule provisions. It is important to note that two of the Safeguard requirements (direct report to the Board of Directors and Incident Response Plan) only apply to institutions that maintain information on 5,000 or more consumers (note: consumers may or may not be customers, see *Definitions*).

The data privacy practices required by the GLBA are aligned with NIST 800-171. In addition to compliance with GBLA, the US Department of Education, and subsequent Federal Student Aid program, strongly recommends integrating NIST 800-171 into the data privacy program developed under the GLBA.

The Privacy Rule

The GLBA Privacy Rule, 16 CFR Part 313, regulates how institutions inform their customers about how they use and share their NPI. Although the FTC and ED state that the privacy rule's requirements are met through FERPA compliance, it is recommended that the institution review its privacy practices to ensure full compliance. The following requirements of the Privacy Rule apply to higher education institutions:

- Establish a set of clear, concise privacy policies that include information about what data is collected, why it is collected, who it will be shared with, and under what conditions.
  - FERPA governs the sharing of data and its recipients. The educational institution must provide an annual FERPA notice of rights, which may outline data collection, purpose, and sharing. However,

if the notice does not cover all aspects, the institution should have a data privacy policy that includes this information.

- Before collecting personal information, ensure students have read the privacy notices and agreed to any data sharing requiring consent.
- Ensure you have a process for notifying students when their personal data is shared with another financial institution or third party for the purpose of completing a transaction.
- Periodically review policies (at least annually) to ensure they are still relevant.

The Safeguards Rule

The objectives of the Safeguards Rule, 16 CFR Part 314, standards are:

- Ensure the security and confidentiality of student information.
- Protect against any anticipated threats to the security or integrity of such records.
- Protect against unauthorized access to, or use of, such records or information that could result in substantial harm or inconvenience to any student.

Under the Safeguard Rule, institutions are required to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The information security program must address the following nine (9) elements:

1. Designate a Qualified Individual to oversee the institution's information security program.

   Suppose the institution utilizes a service provider to implement and supervise the information security program. In that case, the institution is still responsible for compliance and must designate a senior employee to supervise that Qualified Individual. If the Qualified Individual works for an affiliate or service provider, that affiliate or service provider also must maintain an information security program.

2. For institutions maintaining information on over 5,000 students, the Qualified Individual must report to the Board of Directors or governing body in writing regularly, at least annually, and include an overall assessment of the institution's compliance with its information security program. In addition, the report must cover specific topics related to the program (i.e., risk assessment, risk management and control decisions, service provider arrangements, test results, security events and response, and recommendations for program changes).

3. Develop and conduct a written risk assessment.

   This assessment starts with a complete data inventory, followed by an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information. The risk assessment must be written and include criteria for evaluating identified risks and threats. Consider how customer information could be disclosed without authorization, misused, altered, or destroyed. The Safeguards Rule requires institutions to conduct periodic reassessments that account for changes in operations or the emergence of new threats.

4. Design and implement safeguards to control the risks identified through your risk assessment. At a minimum, these safeguards must include:

   - Implement and periodically review access control standards. Determine who has access to customer information and regularly reconsider whether they still have a legitimate business need or educational interest for each data component.

- Implement and maintain a data inventory. The data inventory consists of all systems, devices, platforms, and personnel that access/store data. The data inventory should include where data is collected, stored, and/or transmitted. The corresponding safeguards should be designed to respond with resilience.
- Encrypt customer information at rest and in transit. If it's not feasible to use encryption, secure it using effective alternative controls approved by the Qualified Individual who supervises your information security program.
- Implement procedures for evaluating the security of applications that store, access, or transmit customer information. Procedures should include criteria for in-house developed applications and applications hosted by or purchased through a vendor.
- Implement multi-factor authentication for anyone accessing customer information on your system.
- Dispose of customer information securely. Securely dispose of customer information no later than two years after your most recent use of it to serve the customer. The only exceptions are (a) if you have a legitimate business need or legal requirement to hold on to it or (b) if targeted disposal isn't feasible because of how the information is maintained.
- Anticipate and evaluate changes to your information systems and network. The Safeguards Rule requires institutions to build change management into their information security program.
- Maintain a log of authorized users' activity and monitor for unauthorized access. Implement procedures and controls to monitor when authorized users access customer information on your system and detect unauthorized access.

5. Regularly monitor and test the effectiveness of your safeguards. Test your procedures for detecting actual and attempted attacks. For information systems, testing can be accomplished through continuous monitoring of your system. At a minimum, the institution must conduct annual penetration testing and vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities. In addition, you must test whenever there are material changes to your operations or business arrangements and when circumstances you know, or have reason to know, may have a material impact on your information security program.

6. Implement policies/procedures around the administration of your information security program. Policies/procedures must provide regular security awareness training for all staff who access customer information. Conduct specialized training for employees, affiliates, or service providers with hands-on responsibility for executing your information security program. Ensure security staff are monitoring for emerging threats and effective countermeasures.

7. Monitor service providers. Contracts must specify your security expectations and ensure the provider maintains appropriate safeguards. Contracts must also include a process allowing the institution to monitor the provider's work and provide periodic reassessments of their suitability for the service.

8. Keep your information security program current to account for changes to your operations and personnel, identified risks, emerging threats, and other circumstances that may have a material impact on your information security program.

9. For institutions maintaining information on over 5,000 students, create a written incident response plan designed to respond to and recover from a security event.

   Your response plan must include the following:

   - The goals of your plan;
   - The internal processes your company will activate in response to a security event;
   - Clear roles, responsibilities, and levels of decision-making authority;

- Communications and information sharing both inside and outside your company;
- A process to fix any identified weaknesses in your systems and controls;
- Procedures for documenting and reporting security events and your company's response; and
- A *post-mortem* of what happened and a revision of your incident response plan and information security program based on what you learned.

The Pretexting Rule

The Privacy Protection for Customer Information "Pretexting" Provision, 15 USC § 6821, was designed to counter identity theft. Pretexting is a social engineering technique where the attacker tries to trick an unsuspecting staff (through some form of pretext) into handing over non-public personal information. To comply, the institution must adhere to the following:

- Have policies, procedures, and controls in place to prevent the unauthorized disclosure of customer financial information and to deter and detect unauthorized disclosure or access.
- Periodic risk assessment of covered accounts, including (1) methods used to open accounts; (2) methods used to access accounts; and (3) previous experiences with identity theft.
- Establish a written Identity Theft Prevention Program to detect, prevent, and mitigate identity theft. The program must identify, detect, and respond to Red Flags as defined by the "Red Flags Rule."
- Continued administration of identity theft prevention program that includes approval from and involvement of the board of directors (or appropriate committee), staff training, and oversight of service providers.
    - see Appendix A to Part 681 for additional guidance

Definitions

Consumer means an individual who obtains or has obtained a financial product or service from you that is to be used primarily for personal, family, or household purposes or that individual's legal representative.

- An individual who applies to you for credit for personal, family, or household purposes is a consumer of a financial service, regardless of whether the credit is extended.
- (ii) An individual who provides nonpublic personal information to you in order to obtain a determination about whether he or she may qualify for a loan to be used primarily for personal, family, or household purposes is a consumer of a financial service, regardless of whether the loan is extended.
- (iii) An individual who provides nonpublic personal information to you in connection with obtaining or seeking to obtain financial, investment, or economic advisory services is a consumer, regardless of whether you establish a continuing advisory relationship.

Customer Information means any record containing nonpublic personal information about a customer of a financial institution, whether in paper, electronic, or other form, that is handled or maintained by or on behalf of you or your affiliates.

Customer means a person that has a covered account with a financial institution or creditor.

Encryption means the transformation of data into a form that results in a low probability of assigning meaning without the use of a protective process or key, consistent with current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

Information Security Program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Multi-factor Authentication means authentication through verification of at least two of the following types of authentication factors: (1) Knowledge factors, such as a password; (2) Possession factors, such as a token; or (3) Inherence factors, such as biometric characteristics.

Nonpublic Personal Information means (i) Personally identifiable financial information; and (ii) 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.

Security Event means an event resulting in unauthorized access to, or disruption or misuse of, an information system, information stored on such information system, or customer information held in physical form.

Service Provider (provider) means 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.

References

Appendix A to Part 681. (2023, June 15). Retrieved June 18, 2023, from National Archives Code of Federal Regulations: ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681/appendix-Appendix%20A%20to%20Part%20681

Cornell Law School. (n.d.). *15 U.S. Code § 6825 - Agency guidance*. Retrieved May 2023, from https://www.law.cornell.edu/uscode/text/15/6825

Federal Student Aid. (2020, February 28). Enforcement of Cybersecurity Requirements under the Gramm-Leach-Bliley Act. Retrieved May 2023, from https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2020-02-28/enforcement-cybersecurity-requirements-under-gramm-leach-bliley-act

Federal Student Aid. (2023, 02 09). Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements. *Electronic Announcement ID: General-23-09*. Retrieved May 2023, from https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements

Federal Trade Commission. (2022, November 15). *Compliance deadline for certain revised FTC Safeguards Rule provisions extended to June 2023*. Retrieved May 2023, from Federal Trade Commission: https://www.ftc.gov/business-guidance/blog/2022/11/compliance-deadline-certain-revised-ftc-safeguards-rule-provisions-extended-june-2023

Federal Trade Commission. (2022, May). FTC Safeguards Rule: What Your Business Needs to Know. Retrieved May 2023, from https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Federal Trade Commission. (2022, July). *How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act*, FTC - Privacy Rule. Retrieved May 2023, from https://www.ftc.gov/business-guidance/resources/how-comply-privacy-consumer-financial-information-rule-gramm-leach-bliley-act

Federal Trade Commission. (2023, May). *Gramm-Leach-Bliley Act*. Retrieved from https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

Federal Trade Commission. (2021, December 21). *Standards for Safeguarding Customer Information*. Retrieved May 2023, from Federal Register: https://www.federalregister.gov/documents/2021/12/09/2021-25736/standards-for-safeguarding-customer-information

NIST. (2020, February 02). *SP 800-171 Rev. 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. Retrieved May 2023, from https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Title 16 / Chapter I / Subchapter F / Part 681 / § 681.1. (2023, June 5). Retrieved June 18, 2023, from National Archives Code of Federal Regulations: https://www.ecfr.gov/current/title-16/chapter-I/subchapter-F/part-681/section-681.1#p-681.1(c)

United States Department of Education Office of Inspector General. (2019, October 30). CPA-19-01 Amendment to September 2016 Audit Guide, Guide for Audits ofProprietary Schools. Retrieved May 2023, from https://oig.ed.gov/sites/default/files/document/2023-03/title_iv_dear_cpa_19-01.pdf