GLB Amended Safeguard Rule Background:

The amended Safeguards Rule adds more specificity and prescription to the flexible, process-oriented approach of the original rule. GLB applies to financial institutions. The original GLB safeguard rule became effective May 23, 2003. The amended safeguard rule was applicable on December 9, 2021, and became initially effective January 10, 2022.

Requires financial institutions, including colleges and universities, to develop plans and policies to protect customer financial information (16 CFR Part 314). Includes: names, addresses, phone numbers, bank and credit card account numbers, income and credit histories, and SSN. GLB broadly defines in scope activities as: "making, acquiring, brokering, or servicing loans" and "collection agency services".

Higher education institutions are included because they participate in federal loan (& financial aid) activities. Although FTC rules consider them GLB financial institutions, they are deemed in compliance with the privacy provisions of GLB if they are in compliance with FERPA. However, higher education institutions are required to comply with GLB requirements related to the safeguarding of customer information (physical, technological, administrative).

For institutions that maintain customer data for less than 5,000 consumers, there is a "small business" exception to the following requirements in the Safeguards rule: a written risk assessment, a written incident response plan, an annual written report to the board, and penetration testing and vulnerability assessment requirements.

GLB loosely aligns with the New York Department of Financial Services Cybersecurity Regulation and the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law. This has been a goal of the FTC for some time and reflects years of public feedback.

Synopsis GLB Major New Requirements for Covered Financial Institutions Under the Safeguards Rule include:

- Adoption of a comprehensive, documented information security program focused on protecting customer data.
- Designating a "qualified individual"—in essence a Chief Information Security Officer (**CISO**)—to implement and oversee the organization's information security program. This person can be an employee or contractor/consultant.
- Regular written risk assessments, to include evaluation and assessment criteria, requirements for mitigating, accepting or transferring identified risks, and other specifics. The risk assessment and its findings are intended to be the foundation of the information security program, not just a check-the-box exercise.
- Written reports made by the "qualified individual" to the board/governing body at least once per year.
- Yearly **penetration tests** and twice-yearly **vulnerability assessments**, which must address concerns identified in the risk assessment.
- Documenting a comprehensive incident response plan.
- Encryption of customer data both at rest and in transit, or the implementation of effective compensating controls.

- Multifactor authentication (MFA) for systems that store or handle customer data, or the implementation of effective compensating controls.
- Authentication and access controls as needed to implement the "principle of least privilege" around accessing customer data.
- **Third-party risk management** to ensure that vendors can protect any customer data they handle, including mandating appropriate safeguards in contracts and periodically assessing vendor risk.
- Data retention and disposal controls to facilitate secure disposal of customer data within two years of the data of its last use, unless retention is required or needed for valid business reasons.
- Additional controls to support data classification, secure web development, IT change management, employee security awareness training, and more.

Examples of GLB financial activities:

- Appraisal services, Brokering and Servicing loans.
- Career counseling for individuals seeking employment in the financial services industry.
- Check cashing and issuing payday loans.
- Courier services.
- Debt collection.
- Financial, economic, and investment advisory services.
- Lending, exchanging, transferring, and investing money or securities for others.
- Mortgage lending.
- Nonbank lending.
- Real estate settlement services.
- Tax preparation services.

Safeguards Rule Examples:

Administrative Safeguards

Administrative Safeguards include developing and publishing policies, standards, procedures, and guidelines, and are generally within the direct control of a department, such as:

- Reference checks for potential employees.
- Confidentiality agreements that include standards for handling customer information.
- Training employees on basic steps they must take to protect customer information.
- Assure employees are knowledgeable about applicable policies and expectations.
- Limit access to customer information to employees who have a business need to see it.
- Impose disciplinary measures where appropriate.

Physical Safeguards

Physical Safeguards are also generally within a department's control and include:

- Locking rooms and file cabinets where customer information is kept.
- Using password activated screensavers.
- Using strong passwords.

- Changing passwords periodically and not writing them down.
- Referring calls or requests for customer information to staff trained to respond to such requests.
- Being alert to fraudulent attempts to obtain customer information and reporting these to management for referral to appropriate law enforcement agencies.
- Ensure the storage areas are protected against destructions or potential damage from physical hazards, like fire or floods.
- Store records in a secure area and limit access to authorized employees.
- Dispose of customer information appropriately:
    - Designate a trained staff member to supervise disposal of records containing customer personal information.
    - Shred or recycle customer information recorded on paper and store it in a secure area until the confidential recycling service picks it up.
    - Erase all data when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media that contains customer information.
    - Promptly dispose of outdates customer information according to record retention policies.

Technical Safeguards

Technical Safeguards include:

- Storing electronic customer information on a secure server that is accessible only with a password or has other security protections and is kept in a physically secure area.
- Avoiding storage of customer information on machines with an Internet connection.
- Maintaining secure backup media and securing archived data.
- Using anti-virus software that updates automatically.
- Obtaining and installing patches that resolve software vulnerabilities.
- Following written contingency plans to address breaches of safeguards.
- Maintaining up-to-date firewalls particularly if the institution uses broadband Internet access or allows staff to connect to the network from home.
- Providing central management of security tools and keep employees informed of security risks and breaches.