Gramm-Leach-Bliley Act (GLBA):

By: Lucas Higgs

ChatGPT Overview:

The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act of 1999, is a United States federal law that governs the financial industry. It was signed into law on November 12, 1999, by President Bill Clinton.

The GLBA's primary purpose is to deregulate the financial industry by removing barriers between banking, securities, and insurance companies. It effectively repealed parts of the Glass-Steagall Act of 1933, which had established a separation between commercial banks, investment banks, and insurance companies.

The GLBA has several key provisions:

1. Privacy Requirements: It requires financial institutions to inform consumers about their information-sharing practices and give them the option to opt-out of sharing their personal information with non-affiliated third parties. It also mandates the development and implementation of information security programs to protect customer data.

2. Safeguards Rule: It requires financial institutions to develop and implement comprehensive written information security programs to protect customer data from unauthorized access or use.

3. Pretexting Prohibition: It prohibits the practice of obtaining customer information under false pretenses, such as impersonating the customer or using deceptive methods to obtain personal data.

4. Financial Privacy Rule: It sets limits on the disclosure of non-public personal information by financial institutions and requires them to provide privacy notices to customers.

The GLBA applies to a wide range of financial institutions, including banks, credit unions, insurance companies, securities firms, and other financial service providers.

Overall, the GLBA aims to balance the need for financial industry deregulation with the protection of consumer privacy and information security. It seeks to promote competition and innovation in the financial sector while ensuring that customers' personal information is handled responsibly and securely.

**What is it?:** (Kranz, 2021)

* The Gramm-Leach-Bliley Act (GLB Act or GLBA), also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways financial institutions deal with the private information of individuals. The Act consists of three sections:
  + **The Financial Privacy Rule,** which regulates the collection and disclosure of private financial information;
  + the **Safeguards Rule**, which stipulates that financial institutions must implement security programs to protect such information; and the
  + **Pretexting provisions**, which prohibit the practice of pretexting or accessing private information using false pretenses.
    - The Act also requires financial institutions to give customers written privacy policy notices that explain their information-sharing practices.
* The GLBA repealed large portions of the Glass-Steagall Banking Act of 1933 and the Bank Holding Company Act of 1956. It amended the rules to permit banks, brokerage houses and insurance firms to merge.
* This created a new structural framework whereby a bank holding company could acquire full-service investment banks and insurance companies, while allowing the latter types of firms to form holding companies to acquire banks. As a consequence of GLBA, the U.S. Federal Reserve was granted expanded supervisory power to regulate these new types of financial structures.

**Purpose:** (Kranz, 2021)

* The standards established by GLBA complement data security requirements imposed by the Federal Deposit Insurance Corporation (FDIC). The purpose of the GLB Act is to ensure that financial institutions and their affiliates safeguard the confidentiality of personally identifiable information (PII) gathered from customer records in paper, electronic or other forms. The law requires affected companies to comply with strict data security guidelines. (Kranz, 2021)
* According to the law, financial institutions have an obligation to respect their customers' privacy and securely protect their sensitive personal information against unauthorized access. (Kranz, 2021)
* GLBA compliance requires that companies develop privacy practices and policies that detail how they collect, sell, share and otherwise reuse consumer information. Consumers also must be given the option to decide which information, if any, a company is permitted to disclose or retain for future use. (Kranz, 2021)
* A related requirement governs data storage and security as part of a comprehensive written information security policy. This objective addresses protections against "any anticipated threats or hazards" to data that could result in "substantial harm or inconvenience" to consumers. (Kranz, 2021)
* GLBA's PII guidelines apply to any non-public personal information, which is defined as information a customer may provide to facilitate a transaction or which is otherwise obtained by the institution. (Kranz, 2021)

**Data covered by GLBA:** (Kranz, 2021)

* GLBA compliance is intended to decrease the likelihood an organization will have a data breach and face the resulting fallout, including significant financial and legal penalties and damage to its reputation. GLBA has become a top priority for chief information security officers and other IT professionals charged with managing corporate data. (Kranz, 2021)
* Best practices have emerged, including internal risk assessments, periodic testing of internal controls and ensuring third-party compliance by business partners and service providers. Practical advantages of the law's requirements include an increased ability to identify critical data, eliminate data errors, locate dark data, improve consolidation and enhance data classification. (Kranz, 2021)
* Data that falls under the GLBA:
  + addresses;
  + bank account and financial data;
  + biometric and related data;
  + birth dates;
  + car dealers;
  + credit history (including property records or purchasing history);
  + education level and academic performance;
  + employment data;
  + inferences drawn from other data;
  + internet and other electronic information;
  + geolocation data;
  + names;
  + personal income;
  + Social Security data; and
  + tax information.

**Organizations regulated by GLBA:**(Kranz, 2021)

* The passage of GLBA coincided with the emergence of internet technologies for transacting business, which in turn generated reams of new data and new ways of accessing data. The law broadened the definition of companies classified as financial institutions.
* GLBA regulates any institution significantly engaged in financial activities. Even organizations that do not disclose non-public personal information are required by GLBA to develop a policy to protect information against potential future threats.
* In addition to banks, brokerage firms and insurers, GLBA applies to companies that process loans or otherwise assume credit risk. Any organization that falls within the scope of GLBA must comply with its provisions, although individual states have the power to enact more stringent privacy regulations, as is the case in California and Virginia.
* Professions and businesses subject to GLBA's provisions include:
  + accountants
  + ATM operators
  + car rental companies
  + courier services
  + credit reporting companies
  + credit unions
  + debt collectors
  + financial advisory firms
  + hedge funds
  + non-bank mortgage lenders
  + payday lenders
  + property appraisers
  + real estate firms
  + retailers
  + stockbrokers
  + tax preparers
  + universities

**How GLBA compliance works:**

* Financial Privacy Rule
* Safeguard Rules
* Pretexting Rules

**Pretexting Rule:**

* This rule aims to prevent employees or business partners from collecting customer information under false pretenses, such as social engineering techniques. Although GLBA does not have specific requirements regarding pretexting, prevention usually entails building employee training to avoid pretexting scenarios in the written information security document. (Kranz, 2021)

**Financial Privacy Rule:**

* This rule, often referred to as the *Privacy Rule*, places requirements on how organizations may collect and disclose private financial data. An organization must give "clear and conspicuous notice" of its privacy policy at the start of a customer relationship. Subsequently, customers must get an annual notice for the duration of the relationship unless the organization meets certain criteria. (Kranz, 2021)
* The Privacy Rule outlines which data will be collected, how it will be used and shared, who has access to it, and the policies and procedures used to protect it. As required by the Fair Credit Reporting Act, customers are to be notified of the privacy policy annually, including the right to opt out of sharing information with unaffiliated third-party entities. If a customer agrees to share information, the organization must abide by the provisions of the original privacy notice. (Kranz, 2021)

**Safeguard Rules: (Federal Student Aid)**

The objectives of the GLBA standards for safeguarding information are to –

* Ensure the security and confidentiality of student information;
* Protect against any anticipated threats or hazards to the security or integrity of such information; and
* 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)).

To achieve the GLBA objectives, institutions and servicers are required to develop, implement, and maintain a written, comprehensive information security program. The FTC’s regulations require that the information security program contains administrative, technical, and physical safeguards that are appropriate to the size and complexity of the institution or servicer, the nature and scope of their activities, and the sensitivity of any student information.

An institution’s or servicer’s written information security program must include the following nine elements included in the FTC’s regulations:

Element 1: Designates a qualified individual responsible for overseeing and implementing the institution’s or servicer’s information security program and enforcing the information security program (16 C.F.R. 314.4(a)).

Element 2: Provides for the information security program to be based on a risk assessment that identifies reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information (as the term customer information applies to the institution or servicer) that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assesses the sufficiency of any safeguards in place to control these risks (16 C.F.R. 314.4(b)).

Element 3: Provides for the design and implementation of safeguards to control the risks the institution or servicer identifies through its risk assessment (16 C.F.R. 314.4(c)). At a minimum, the written information security program must address the implementation of the minimum safeguards identified in 16 C.F.R. 314.4(c)(1) through (8).

Element 4: Provides for the institution or servicer to regularly test or otherwise monitor the effectiveness of the safeguards it has implemented (16 C.F.R. 314.4(d)).

Element 5: Provides for the implementation of policies and procedures to ensure that personnel are able to enact the information security program (16 C.F.R. 314.4(e)).

Element 6: Addresses how the institution or servicer will oversee its information system service providers (16 C.F.R. 314.4(f)).

Element 7: Provides for the evaluation and adjustment of its information security program in light of the results of the required testing and monitoring; any material changes to its operations or business arrangements; the results of the required risk assessments; or any other circumstances that it knows or has reason to know may have a material impact the information security program (16 C.F.R. 314.4(g)).

Element 8: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the establishment of an incident response plan (16 C.F.R. 314.4(h)).

Element 9: For an institution or servicer maintaining student information on 5,000 or more consumers, addresses the requirement for its Qualified Individual to report regularly and at least annually to those with control over the institution on the institution’s information security program (16 C.F.R. 314.4(i)).

Institutions or servicers that maintain student information for fewer than 5,000 consumers are only required to address the first seven elements.

While all elements of the Safeguards Rule are vital to protecting the security of customer information, an institution or servicer may significantly reduce the risk of a security breach, and the resulting harm and inconvenience to its customers, by encrypting customer information while it is in transit outside its systems or stored on its system and by implementing multi-factor authentication for anyone accessing customer information on its systems.

In April of 2022, the FTC issued a new publication entitled [FTC Safeguards Rule: What Your Business Needs to Know](https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know), which is meant to act as a “compliance guide” to ensure that entities covered by the Safeguards Rule maintain safeguards to protect the security of customer information. The publication provides valuable information such as describing what a reasonable security program should look like and goes over each of the nine required elements in greater detail.

**Safeguard Rule:** (Kranz, 2021)

* As the name implies, steps to ensure information security are the key focus of GLBA's Safeguard Rule. The Federal Trade Commission ([FTC](https://searchcompliance.techtarget.com/definition/FTC-Federal-Trade-Commission)) issued this rule in 2002 and continues to enforce it.
* **The rule instructs organizations to implement administrative, physical and technical protections as safeguards against cyber attacks, email spoofing, phishing schemes and similar cybersecurity risks.**
* The rule also requires an organization to designate at least one person to be accountable for all aspects of the information security plan, including development and regular testing. Data encryption and key management are recommended as best practices, but they are not FTC requirements under the Safeguard Rule.

### **NIST 800-171 Standards:**

* The Department will issue guidance on NIST 800-171 compliance in a future Electronic Announcement, but again encourages institutions to begin incorporating the information security controls required under NIST 800-171 into the written information security program required under GLBA as soon as possible. Please note that compliance with the GLBA requirements is not the same as compliance with NIST 800-171. The current information security requirements that institutions must meet are the GLBA Safeguards Rule requirements at 16 C.F.R. Part 314. (Federal Student Aid)

### **Enforcement Process When Noncompliance with GLBA has been Identified:**

* The changes to the Safeguards Rule are effective June 9, 2023. Any GLBA findings identified through a compliance audit, or any other means, after the effective date will be resolved by the Department during the evaluation of the institution’s or servicer’s information security safeguards required under GLBA as part of the Department’s final determination of an institution’s administrative capability. GLBA related findings will have the same effect on an institution’s participation in the Title IV programs as any other determination of non-compliance. (Federal Student Aid)
* In cases where no data breaches have occurred and the institution’s or servicer’s security systems have not been compromised, if the Department determines that an institution or servicer is not in compliance with all of the Safeguards Rule requirements, the institution or servicer will need to develop and/or revise its information security program and provide the Department with a Corrective Action Plan (CAP) with timeframes for coming into compliance with the Safeguards Rule. Repeated non-compliance by an institution or a servicer may result in an administrative action taken by the Department, which could impact the institution’s or servicer’s participation in the Title IV programs. (Federal Student Aid)

**Who Enforces this:**

* State and federal banking agencies have varying degrees of authority to enforce GLBA provisions. The FTC can take action in federal district courts against organizations that fail to comply with the Privacy Rule. Section 5 of GLBA grants the FTC the authority to audit privacy policies to ensure they are developed and applied fairly. (Kranz, 2021)
* Enforcement of the Safeguard Rule remains with the FTC, although the Dodd-Frank Act in 2010 transferred new rulemaking authority to the Consumer Financial Protection Bureau (CFPB). Other federal agencies that play a role in GLBA enforcement include the Federal Reserve Board, the FDIC, the Office of Thrift Supervision and the Office of the Comptroller of the Currency. The responsibility for regulating insurance providers falls to individual states. (Kranz, 2021)

**Penalties and Cases:** (Kranz, 2021)

* Failure to comply with GLBA can have severe financial and personal consequences for executives and employees. A financial institution faces a fine up to $100,000 for each violation. Its officers and directors can be fined up to $10,000, imprisoned for five years or both. Companies also face increased exposure and a loss of customer confidence.
* Heightened awareness of security risks is among the benefits companies may derive from GLBA compliance, especially as hackers develop more sophisticated tools to breach computer systems. Aside from enhanced brand reputation, a company can gain new insights from existing data and improve its data management capabilities.
* Recent GLBA cases brought by the FTC include:
  + **Ascension Data and Analytics.** In 2020, the Arlington, Texas, company agreed to an undisclosed financial settlement after a vendor, OpticsML, was found to have stored customer financial information in plain text in insecure cloud storage.
  + **PayPal.** The online [payment processor](https://www.techtarget.com/whatis/definition/payment-processor) agreed to pay $175,000 to the state of Texas in 2018 to settle GLBA and Federal Trade Act violations that compromised data security and privacy of customers using its Venmo peer-to-peer application.
  + **TaxSlayer.** Hackers were able to access nearly 9,000 of the Augusta, Ga., online tax preparer's customer records for several months in 2015. The FTC said it failed to implement a comprehensive security program, including providing a privacy notice to customers, as required under GLBA. Under the settlement with the FTC, the company is prohibited from violating the GLBA's Privacy Rule and the Safeguards Rule for 20 years and is required to have a third party assess its compliance every two years for 10 years.

### **GLBA and GDPR:**

* GLBA and Europe's General Data Protection Regulation (GDPR) have different goals, but both define data security and consumer privacy. Whereas GLBA sets data privacy rules for financial institutions, GDPR encompasses any organization that processes an individual's personal data in the course of transacting business. (Kranz, 2021)
* Like GLBA, GDPR encourages companies to be more transparent in how they capture and handle sensitive information. That includes individuals' personal data and any metadata that may be used to identify or characterize them. (Kranz, 2021)

**How this relates to TKH:**

* The Gramm-Leach-Bliley Act (GLBA), also known as the Financial Services Modernization Act, primarily applies to financial institutions and their handling of consumer financial information. As a result, its direct impact on non-profit organizations may be limited, as they typically do not fall under the definition of financial institutions.
* However, it's important to note that non-profit organizations may still collect and handle personal information from their donors, supporters, and beneficiaries. In such cases, they may have obligations under other data protection laws, such as the General Data Protection Regulation (GDPR) in the European Union or other applicable local regulations.
* While the GLBA itself may not directly apply to non-profit organizations, they should still take measures to protect the privacy and security of the personal information they handle. This includes implementing appropriate data protection practices, maintaining confidentiality, obtaining consent where required, and ensuring compliance with applicable data protection laws.
* It's advisable for non-profit organizations to consult legal professionals or experts in their jurisdiction to understand the specific requirements and regulations that apply to their operations and the handling of personal information.

**Resources:**

* Federal Student Aid, anonymous. (n.d.). *(general-23-09) updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements*. Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements | Knowledge Center. <https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements>
  + (Federal Student Aid)
* Kranz, G. (2021, June 17). *What is the Gramm-Leach-Bliley Act?*. CIO. <https://www.techtarget.com/searchcio/definition/Gramm-Leach-Bliley-Act>
  + (Kranz, 2021)