NetworkTitan

THE “SAFEGUARDS RULE”

A Compliance Guide

Information On The Gramm-Leach-Bliley Act (GLBA)

mike@networktitan.com
www.NetworkTitan.com

Disclaimer:

The Safeguards Rule references the Gramm-Leach-Bliley Act and the Bank Holding Company Act when defining who must comply with the Rule. It is important to review these texts, and the Rule itself, to determine your obligations.

Information contained in this Guide is simplified. It is not a legal document and Network Titan is not acting in a legal capacity to disseminate this information.

BACKGROUND

The Federal Trade Commission's (FTC) "Safeguards Rule" took effect in 2003 to ensure safeguards were taken and maintained by companies to protect customer information. The Safeguards Rule was amended in December 2021 to keep pace with cybersecurity trends and technologies. Today, the Rule as written, gives more concrete guidance to businesses, defining essential data security principles that demonstrate safeguards are in place and maintained that protect customer information.

The Safeguards Rule, section 501(b) of the Gramm-Leach-Bliley Act (GLBA), is one of three sections in the Act. The Act was signed into law by President Clinton in 1999 for the purpose of reforming and modernizing the banking industry. Its focus is on information security and mandates the protection of customer information collected by financial organizations.

Many businesses are familiar with the two other sections of the Act, the **Financial Privacy Rule** which regulates how private financial information is collected and disclosed (those consumer privacy notice forms that explain privacy policies and practices), and the third section of the Act, the **Pretexting Provisions** section which forbids access to private information under false pretenses – or simply put, forbids lying in order to get private financial information (social engineering, phishing). The Rules work together to give the Gramm-Leach-Bliley Act its strength in protecting customers' private, personal data.

This Guide mainly addresses the Safeguards Rule section of the Act although full GBLA Compliance extends into each section.

The Safeguards Rule

A QUICK LOOK AT THE IMPORTANT PROVISIONS OF THE RULE

Companies that fall under the provisions of the Gramm-Leach-Bliley-Act are required to comply with the following provisions of the Safeguards Rule.

- **Designate** a qualified person to oversee their information security program.
- Develop a **written risk assessment.**
- Limit and **monitor who can access** sensitive customer information.
- **Encrypt** all sensitive information.
- **Train** security personnel.
- **Develop an Incident Response Plan.**
- **Periodically assess** the security practices of service providers.
- **Implement Multi-Factor Authentication** for anyone accessing customer information.
- Know what you have and where you have it (**inventory of data, systems, devices, etc.**).
- **Review security** of in-house and third-party applications.
- **Dispose** of customer information securely.
- Anticipate and **evaluate changes** to your information systems.
- **Maintain a log** of authorized users' activity and detect unauthorized access.
- **Regularly monitor and test** the effectiveness of your safeguards (Vulnerability scanning and Penetration testing).
- **Train all staff** with access to consumer data on how to detect and avoid threats.
- Keep your information security program **current.**

WHAT IS THE GLBA SAFEGUARDS RULE?

The Safeguards Rule is one of three "rules" initiated by the FTC under the Gramm Leach Bliley Act (GLBA) and requires financial institutions under FTC jurisdiction to follow standards for developing, implementing and maintaining reasonable administrative, technical, and physical safeguards – that are appropriate to the size and complexity of the entity – to protect the security, confidentiality, and integrity of customer information. Companies covered by the Rule must take steps to ensure that their affiliates and service providers 'safeguard' customer information in their care.

Companies are required to develop a written information security program (or plan) that describes the methods used to protect their data.

WHO MUST COMPLY WITH THE SAFEGUARDS RULE?

The Safeguards Rule applies to all "financial institutions" over which the FTC has jurisdiction (pursuant to section 501(b) of the Gramm-Leach-Bliley Act). The FTC's definition of a financial institution is *very* broad. A short list of these entities includes mortgage lenders, tax preparation firms, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors.

EXAMPLES OF FINANCIALS INSTITUTIONS (Refer to 16 CFR 314.2(h)(1) for additional examples)

- A business that regularly wires money to and from consumers.
- An accountant or other tax preparation service that is in the business of completing income tax returns.
- Nonbank mortgage lenders, securities firms, and insurance companies.
- An entity that provides real estate settlement services.
- An entity that engages in debt collection.
- An automobile dealership that leases automobiles on a nonoperating basis for longer than 90 days.
- A company acting as a finder in bringing together one or more buyers and sellers of any product or service for transactions that the parties themselves negotiate and consummate.
- A personal property or real estate appraiser.

NONPUBLIC PERSONAL INFORMATION (NPI) DEFINED

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.

NPI is any customer data or information considered to be personal and not publicly available, like full legal names and social security numbers: 1) provided by a consumer to a financial institution 2) resulting from a transaction or service performed for the consumer or 3) otherwise obtained by the financial institution.

OBJECTIVES OF AN INFORMATION SECURITY PROGRAM

(1) Ensure the security and confidentiality of customer information.

(2) Protect against any anticipated threats or hazards to the security or integrity of such information.

(3) Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

REQUIRED ELEMENTS OF AN INFORMATION SECURITY PROGRAM FOR COMPLIANCE

A. **Designate a Qualified Individual** - Designate an employee or employees to coordinate an Information Security Program to ensure accountability and achieve adequate safeguards.

B. **Conduct Risk Assessments** - 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, and assess the sufficiency of any safeguards in place to control these risks. With special attention to (1) Employee training and management; (2) information systems, including network and software design, information processing, storage, transmission and disposal; and (3) detecting, preventing and responding to attacks, intrusions, or other systems failures.

C. **Design Safeguards Based on Risk Assessment Results** - Design and implement information safeguards to control the risks [identified] through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

D. **Select a Qualified IT Provider** - Take reasonable steps to select and retain appropriate [IT] service providers that maintain sufficient procedures to detect and respond to security breaches and maintain reasonable procedures to discover and respond to widely known security failures. Require its service providers by contract to implement and maintain such safeguards.

E. **Test Regularly and Adjust Accordingly** - Evaluate and adjust its information security program based on; the results of the testing and monitoring required by paragraph (C); any material changes to its operations or business arrangements; or any other circumstances that may have a material impact on its information security program.

FINES and PENALTIES

The Federal Trade Commission has the enforcement authority for the GLBA and the Safeguards Rule. Penalties for violating the GLBA are substantial. Fines can be up to $100,000 for each individual violation. Additionally, officers and directors of an organization can also face civil penalties of $10,000 per violation.

The Act also includes provisions for criminal enforcement. In these cases, statutory fines and up to five years in federal prison can be levied.

The Most Important Thing To Do Now For Compliance

Get the results of a Risk Assessment.

The results and documentation of your risk assessment must address in detail the 3 key sections, or Rules, of the GLBA. Keep this documentation on file and continually (at least 2 times per year) review and update all components. This documentation will be the baseline for any FTC audits you may find yourself in.

If done thoroughly and correctly, your firm will avoid any fines or penalties and be an excellent steward of all customer data in your care.

NetworkTitan Can Solve Your GLBA Compliance Needs

Our in-depth experience working with financial institutions makes us uniquely qualified to handle complex GLBA compliance requirements.

We utilize a step-by-step process that begins with a GLBA Review Consultation and progresses to a comprehensive Risk Assessment.

As gaps and insufficiencies related to compliance are identified, we provide detailed documentation and implement the necessary changes to remediate and repair your Information Security Program so your company is fully GLBA compliant.

Contact us today to discuss a path forward. Call 619-255-2621 or contact us online at https://www.networktitan.com/contact-us

SAFEGUARDS RULE DEFINITIONS (Refer to 16 C.F.R. § 314.2 for more definitions)

Consumer – 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.

Customer – a consumer who has a customer relationship with you.

Customer Information – 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.

Encryption – 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 the current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

Financial Institution - any institution the business of which is engaging in an activity that is financial in nature or incidental to such financial activities as described in section 4(k) of the Bank Holding Company Act of 1956, 12 U.S.C § 1843(k) An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

Incident Response Plan – A written protocol to respond to a "security event" which clearly describes the activation of internal processes to respond and recover.

Information Security Program – the administrative, technical or physical safeguards that a financial institution uses to access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle customer information. *See "What Are The Elements of an Information Security Program."*

Information System - A discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic information containing customer information or connected to a system containing customer information, as well as any specialized system such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental controls systems that contains customer information or that is connected to a system that contains customer information.

Multi-factor Authentication - 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.

NPI – Nonpublic Personal Information – Any personally identifiable financial information that a financial institution collects about an individual in connection with providing a financial product or service, unless that information is otherwise "publicly available."

Security Event – 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 – 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.

RESOURCES

The Final Rule - FTC 16 CFR Part 314 https://www.govinfo.gov/content/pkg/FR-2002-05-23/pdf/02-12952.pdf

FTC Safeguards Rule: What Your Business Needs to Know https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

Network Titan The "Safeguards Rule" A Compliance Guide

Contact us today to discuss a path forward. Online at https://www.networktitan.com/contact-us

Mike Hughes, President
Network Titan
9685 Via Excelencia, Ste. 110
San Diego CA 92126
www.NetworkTitan.com
619-255-2621 x101