Gramm-Leach Bliley Act

FTC Safeguards and Privacy Rules

by Ray Hutchins and Mitch Tanenbaum

2/9/2023

AI Statement: This document was written by a human being ***and not AI***. While we may use AI for aspects of our research, we find that AI is (thus far) incapable of writing a document of this kind.

Contents

Introduction

The U.S. Congress created the Federal Trade Commission (FTC) in 1915 to promote a free market economy. While the FTC shares joint responsibility with the Department of Justice for U.S. competition policy and antitrust law enforcement, the FTC is the principle regulatory force at the federal level to protect U.S. consumers from unfair and deceptive business practices.

As part of their mission, the FTC is responsible for enforcing the Gramm-Leach-Bliley Act (GLBA) which was initially signed into law in 1999. Two components this law are the FTC Safeguards Rule and the FTC Privacy Rule.

rh@cybercecurity.com
303-887-5864

Safeguards Rule History

The FTC Safeguards Rule was issued in 2000 as part of the Gramm-Leach-Bliley Act (GLBA) and became effective on May 23, 2003. It is still in effect.

The Safeguards Rule applies to financial institutions, including banks, credit unions, and mortgage companies, *that are subject to the jurisdiction of the FTC*. (See Exemptions below).

NOTE: The FTC expanded the definition of financial institutions to include money "finders":

a. Companies that bring together buyers and sellers
b. Companies that support the conveying of ownership interest
c. Finders ***often*** collect and maintain sensitive customer data

The rule requires such financial institutions to implement *appropriate and reasonable* security measures to protect customers' non-public personal information, such as Social Security numbers, account numbers, and credit histories.

The FTC approved changes to the Safeguards Rule in October 2021. These included more specific criteria for what safeguards financial institutions must implement as part of their information security programs. This document provides the reader with the latest such guidance from the FTC.

Safeguards Rule Security Requirements

The following is a summary of the Safeguards Rule security requirements. While these requirements are specific to the Safeguard rule, they are typical for any professional security program. Please contact us if you have any questions or would like additional information.

1. Single, qualified authority. Designate a SINGLE person who is responsible for overseeing and implementing the information security program. This person must be qualified, a term the rules do not yet define.
2. Risk assessments. Annual WRITTEN risk assessments must be performed and documented. Such assessments must identify control deficiencies and document how these risks will be mitigated or accepted, i.e., a Plan of Action with Milestones (PoAM).
3. Access controls. The institution must implement access controls based on least privilege.
4. System inventories. Conduct, document and maintain data and systems inventories. This includes cloud data and data "puddles."
5. Encryption. All customer information transmitted over external networks and stored locally must be encrypted.

rh@cybercecurity.com
303-887-5864

6. Multi-factor authentication (MFA). Implement MFA or another method with equivalent protection for any individual accessing customer information.
7. Intrusion detection. Implement intrusion detection – continuous monitoring and logging of intrusions.
8. Penetration testing and vulnerability scanning. If the institution doesn't have continuous monitoring in place, then annual pen testing and vulnerability scans must be performed. This should include social engineering testing (email? Text? Voice?)
9. Incident response (IR). Create, train and maintain a WRITTEN incident response program. The IR program needs to address security events materially affecting the confidentiality, integrity ***or*** availability of customer information in the financial institution's control. The IR Program must address seven key areas:
    a. The goals of the program
    b. Internal processes for responding to a security event
    c. Definition of included roles and decision making authority
    d. Internal and external communications and information sharing
    e. Identification of requirements for remediating any identified weaknesses
    f. Documentation and reporting of the security event
    g. Evaluation and revision of the plan on an ongoing basis

10. Change management. Implement formal change management processes.
11. Data retention. Implement formal processes around the retention and disposal of customer information.
12. Vendor management. Periodically assess the security practices of service providers and utilize service providers who take security seriously. Oversight of service providers must be performed on an ongoing basis.
13. Awareness training. Training for all staff has to be designed and performed based on the annual risk assessment and changes in practices. Training compliance must be documented.
14. Secure software development. Implement a Secure Software Development Lifecycle (SSDL) process.
15. Annual Reporting. The qualified individual described in item 1 above must issue a written annual report to the institution's governing body (Board of Directors or senior management team if not board) that describes the overall status of the security program and any material matters, and recommendations for changes. Please contact us for more information.

Safeguard Rules Exemptions

The Federal Trade Commission (FTC) Safeguards Rule, which requires financial institutions to implement appropriate security measures to protect customers' non-public personal information, applies to financial institutions that are subject to the jurisdiction of the FTC.

However, there are some financial institutions that are exempt from the Safeguards Rule, including:

rh@cybercecurity.com
303-887-5864

1. Certain small businesses: Financial institutions with less than $5 million in total assets or who maintain* information on less than 5,000 people (unless they are affiliates of larger financial institutions) may be exempt. In such instances the following requirements may not apply:

    a. No written risk assessment
    b. No continuous monitoring or annual pen tests
    c. No written incident response plan
    d. No annual board reporting

    *Note: The threshold is **maintaining** data, so that includes loan applications, closed loans, denied loans and servicing of loans.

2. Certain government agencies: Federal, state, and local government agencies are exempt from the Safeguards Rule.
3. Non-profit organizations: Non-profit organizations are exempt from the Safeguards Rule, unless they engage in financial activities that make them subject to the rule.

It is important to note that while these financial institutions may be exempt from the Safeguards Rule, they may still be subject to other privacy and security requirements under state or federal law. Please contact us for more information on exemptions to the FTC Safeguard Rule.

Privacy Rule History

The Federal Trade Commission (FTC) Privacy Rule has its roots in the Children's Online Privacy Protection Act (COPPA) of 1998. COPPA required website operators to obtain parental consent before collecting personal information from children under the age of 13. In response to the growing concern over online privacy, the FTC issued the Privacy Rule as part of the Children's Online Privacy Protection Rule (COPPA) in 2000.

Privacy Rule Security Requirements

The Privacy Rule which applies to all website operators that collect personal information from consumers requires such website operators to provide clear and concise notice to consumers about their information collection practices and give consumers the option to choose whether their personal information is shared with third parties,

The Privacy Rule has five main compliance requirements:

1. Notice: Companies must provide clear and concise notice to consumers about their information collection practices.
2. Choice: Companies must give consumers the option to choose whether their personal information is shared with third parties.
3. Access: Consumers must be able to access their personal information that is collected and maintained by companies.
4. Security: Companies must take reasonable steps to secure the personal information they collect from consumers.

rh@cybercecurity.com
303-887-5864

5. Enforcement: The FTC is responsible for enforcing the Privacy Rule and may take action against companies that violate the rule.

Safeguard Privacy Rule Exemptions

There are some entities that are exempt from the Privacy Rule, including:

1. Certain government agencies: Federal, state, and local government agencies.
2. Certain financial institutions: Financial institutions that are subject to the jurisdiction of other federal agencies, such as the Office of the Comptroller of the Currency and the Federal Reserve System.
3. Certain common carriers: Common carriers, such as telephone companies, are exempt from the Privacy Rule with respect to information collected in the ordinary course of business.

It is important to note that while these entities may be exempt from the Privacy Rule, they may still be subject to other privacy and security requirements under state or federal law.

Safeguards and Privacy Rules Enforcement

The FTC has taken enforcement actions to enforce the provisions of the GLBA, including the Safeguards and Privacy Rules, which requires financial institutions to implement appropriate security measures to protect customers' non-public personal information.

Such enforcement actions include:

1. Civil penalties: The FTC can impose civil penalties on financial institutions that violate the Safeguards Rule. These penalties can be substantial, and the FTC has imposed penalties in the millions of dollars against financial institutions that have violated the rule.
2. Injunctions: The FTC can seek injunctions to prevent financial institutions from continuing to engage in practices that violate the Safeguards Rule.
3. Settlements: The FTC has also entered into settlements with financial institutions to resolve violations of the Safeguards Rule. These settlements often require the financial institution to implement improved security measures and to pay a monetary penalty.

The FTC has also worked with other federal agencies, such as the Consumer Financial Protection Bureau (CFPB), to enforce the provisions of the GLBA and the Safeguards and Privacy Rules.

rh@cybercecurity.com
303-887-5864

Want more info? Would you like to meet our lead vCISO? Please watch the video on this page: https://www.turnkeycybersecurityandprivacysolutions.com

Or contact Mitch directly at:

Mitch Tanenbaum
720-890-1663
mitch@turnkeycybersecurityandprivacysolutions.com

Did you find this research paper of value? Here are some of our other research papers.

1. IT Infrastructure Monitoring Issues-Making the Best Choice for Your Company
2. Secrets of Hiring and Firing vCISOs
3. CMMC Compliance-The New Enclave Approach
4. The "NEW" CMMC 2.0 (AKA 800-171): Not the Right Way to Fix the DIB Security Crisis
5. When Management Fails: How the IT Folks Can Protect Their Jobs After a Breach
6. Monitoring Your IT Systems-The Best Tools That Meet Compliance Requirements and Which are Affordable for SMEs

rh@cybercecurity.com
303-887-5864