WISPs and the FTC Safeguards Rule

IN THIS DOCUMENT

FTC Safeguards Rule: What Your Business Needs to Know

https://www.ftc.gov/business-guidance/resources/ftc-safeguards-rule-what-your-business-needs-know

As the name suggests, the purpose of the Federal Trade Commission's Standards for Safeguarding Customer Information – the Safeguards Rule, for short – is to ensure that entities covered by the Rule maintain safeguards to protect the security of customer information. The Safeguards Rule took effect in 2003, but after public comment, the FTC amended it in 2021 to make sure the Rule keeps pace with current technology. While preserving the flexibility of the original Safeguards Rule, the revised Rule provides more concrete guidance for businesses. It reflects core data security principles that all covered companies need to implement.

This publication serves as the small entity compliance guide under the Small Business Regulatory Enforcement Fairness Act. Your best source of information is the text of the Safeguards Rule itself. In reviewing your obligations under the Safeguards Rule, consider these key compliance questions.

Who's covered by the Safeguard Rule?

The Safeguards Rule applies to financial institutions subject to the FTC's jurisdiction and that aren't subject to the enforcement authority of another regulator under section 505 of the Gramm-Leach-Bliley Act, 15 U.S.C. § 6805. According to Section 314.1(b), an entity is a "financial institution" if it's engaged in an activity that is "financial in nature" or is "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)."

How do you know if your business is a financial institution subject to the Safeguards Rule? First, consider that the Rule defines "financial institution" in a way that's broader than how people may use that phrase in conversation. Furthermore, what matters are

the types of activities your business undertakes, not how you or others categorize your company.

To help you determine if your company is covered, Section 314.2(h) of the Rule lists 13 examples of the kinds of entities that *are* financial institutions under the Rule, including mortgage lenders, payday lenders, finance companies, mortgage brokers, account servicers, check cashers, wire transferors, collection agencies, credit counselors and other financial advisors, tax preparation firms, non-federally insured credit unions, and investment advisors that aren't required to register with the SEC. The 2021 amendments to the Safeguards Rule add a new example of a financial institution – finders. Those are companies that bring together buyers and sellers and then the parties themselves negotiate and consummate the transaction.

Section 314.2(h) of the Rule lists four examples of businesses that *aren't* a "financial institution." In addition, the FTC has exempted from certain provisions of the Rule financial institutions that "maintain customer information concerning fewer than five thousand consumers."

Here is another key consideration for your business. Even if your company wasn't covered by the original Rule, your business operations have probably undergone substantial transformation in the past two decades. As your operations evolve, consult the definition of financial institution periodically to see if your business could be covered now.

What does the Safeguards Rule require companies to do?

The Safeguards Rule requires covered financial institutions to develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information. The Rule defines customer information to mean "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." (The definition of "nonpublic personal information" in Section 314.2(l) further explains what is – and isn't – included.) The Rule covers information about your own customers and information about customers of other financial institutions that have provided that data to you.

Your information security program must be written and it must be appropriate to the size and complexity of your business, the nature and scope of your activities, and the sensitivity of the information at issue. The objectives of your company's program are:

- to ensure the security and confidentiality of customer information;
- to protect against anticipated threats or hazards to the security or integrity of that information; and
- to protect against unauthorized access to that information that could result in substantial harm or inconvenience to any customer.

PART 314—STANDARDS FOR SAFEGUARDING CUSTOMER INFORMATION

Authority:15 U.S.C. 6801(b), 6805(b)(2).

https://www.ecfr.gov/current/title-16/part-314#p-314.2(h)
16 CFR 314.2(h)

(1) ***Financial institution*** means 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.

(2) Examples of financial institutions are as follows:

(i) A **retailer that extends credit** by issuing its own credit card directly to consumers is a financial institution because extending credit is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act of 1956 (12 U.S.C. 1843(k)(4)(F)), and issuing that extension of credit through a proprietary credit card demonstrates that a retailer is significantly engaged in extending credit.

(ii) An **automobile dealership** that, as a usual part of its business, leases automobiles on a nonoperating basis for longer than 90 days is a financial institution with respect to its leasing business because leasing personal property on a nonoperating basis where the initial term of the lease is at least 90 days is a financial activity listed in 12 CFR 225.28(b)(3) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iii) A **personal property or real estate appraiser** is a financial institution because real and personal property appraisal is a financial activity listed in 12 CFR 225.28(b)(2)(i) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(iv) A **career counselor** that specializes in providing career counseling services to individuals currently employed by or recently displaced from a financial organization, individuals who are seeking employment with a financial organization, or individuals who are currently employed by or seeking placement with the finance, accounting or audit departments of any company is a financial institution because such career counseling activities are financial activities

listed in 12 CFR 225.28(b)(9)(iii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(v) A **business that prints and sells checks for consumers**, either as its sole business or as one of its product lines, is a financial institution because printing and selling checks is a financial activity that is listed in 12 CFR 225.28(b)(10)(ii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(vi) A **business that regularly wires money to and from consumers** is a financial institution because transferring money is a financial activity referenced in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A), and regularly providing that service demonstrates that the business is significantly engaged in that activity.

(vii) A **check cashing business** is a financial institution because cashing a check is exchanging money, which is a financial activity listed in section 4(k)(4)(A) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(A).

(viii) An **accountant or other tax preparation service that is in the business of completing income tax returns** is a financial institution because tax preparation services is a financial activity listed in 12 CFR 225.28(b)(6)(vi) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(ix) A **business that operates a travel agency in connection with financial services** is a financial institution because operating a travel agency in connection with financial services is a financial activity listed in 12 CFR 225.86(b)(2) and referenced in section 4(k)(4)(G) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(G).

(x) An **entity that provides real estate settlement services** is a financial institution because providing real estate settlement services is a financial activity listed in 12 CFR 225.28(b)(2)(viii) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xi) A **mortgage broker** is a financial institution because brokering loans is a financial activity listed in 12 CFR 225.28(b)(1) and referenced in section 4(k)(4)(F) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(F).

(xii) An **investment advisory company and a credit counseling service** are each financial institutions because providing financial and investment advisory services are financial activities referenced in section 4(k)(4)(C) of the Bank Holding Company Act, 12 U.S.C. 1843(k)(4)(C).

(xiii) 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** is a financial institution because acting as a finder is an activity that is financial in nature or incidental to a financial activity listed in 12 CFR 225.86(d)(1).

(GENERAL-23-09) Updates to the Gramm-Leach-Bliley Act Cybersecurity Requirements

https://fsapartners.ed.gov/knowledge-center/library/electronic-announcements/2023-02-09/updates-gramm-leach-bliley-act-cybersecurity-requirements

On December 9, 2021, the Federal Trade Commission (FTC) issued final regulations (Final Rule) to amend the Standards for Safeguarding Customer Information (Safeguards Rule), an important component of the Gramm-Leach-Bliley Act's (GLBA) requirements for protecting the privacy and personal information of consumers. The effective date for most of the changes to the Safeguards Rule is June 9, 2023. This Electronic Announcement provides a summary of the changes to the GLBA requirements resulting from the Final Rule, explains the impacts of the changes on postsecondary institutions, and describes changes to the Department of Education's (Department) enforcement of the GLBA requirements. Institutions should coordinate with their leadership and appropriate staff to implement the requirements in the Final Rule by June 9.

Background

Postsecondary institutions and third-party servicers must protect student financial aid information provided to them by the Department or otherwise obtained in support of the administration of the Federal student financial aid programs (Title IV programs) authorized under Title IV of the Higher Education Act of 1965, as amended (HEA). Each institution that participates in the Title IV programs has agreed in its Program Participation Agreement (PPA) to comply with the GLBA Safeguards Rule under 16 C.F.R. Part 314. Institutions and servicers also sign the Student Aid Internet Gateway (SAIG) Enrollment Agreement, which states that they will ensure that all Federal Student Aid applicant information is protected from access by, or disclosure to, unauthorized personnel, and that they are aware of and will comply with all of the requirements to protect and secure data obtained from the Department's systems for the purposes of administering the Title IV programs.

In Dear Colleague Letters GEN-15-18 and GEN-16-12, we reminded institutions about the longstanding requirements of GLBA and notified them of our intention to begin enforcing the legal requirements of GLBA through annual compliance audits. In Dear CPA Letter CPA-19-01, the Office of Inspector General (OIG) explained the audit procedures for auditors to determine whether institutions were complying with GLBA. On February 28, 2020, we issued an Electronic Announcement that explained the

Department's procedures for enforcing those requirements and the potential consequences for institutions or servicers that fail to comply. On December 18, 2020 we issued an Electronic Announcement encouraging institutions to review and adopt NIST 800–171 as a security standard to support continuing obligations under GLBA.

Updated GLBA Requirements

Below we provide additional information about the updated requirements and definitions in the GLBA Safeguards Rule. Note that while the following provides a summary of the requirements, your best source of information is the text of the Safeguards Rule itself and GLBA guidance provided by the FTC. The FTC also provides a great deal of general data security guidance on its website.

Definition of "Customer" for Purposes of GLBA Compliance

The regulations at 16 C.F.R. Part 314 use the terms "customer" and "customer information." For the purpose of an institution's or servicer's compliance with GLBA, customer information is information obtained as a result of providing a financial service to a student (past or present). Institutions or servicers provide a financial service when they, among other things, administer or aid in the administration of the Title IV programs; make institutional loans, including income share agreements; or certify or service a private education loan on behalf of a student.

Requirements in the GLBA Safeguards Rule

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, 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.

Enforcement Authority and Compliance Requirements

Under the Standards of Administrative Capability at 34 C.F.R. 668.16(c), an institution is required to have an adequate system of internal controls that provides reasonable assurance that the institution will achieve its objectives regarding reporting, operations, and compliance. Information security safeguards are fundamental to a system of internal controls and essential for preventing disruption to these core objectives as they guard the information systems that collect, maintain, process, and disseminate student information. Therefore, an institution that does not provide for the security of the information it needs to continue its operations would not be administratively capable.

The changes to the Safeguards Rule expand on the minimum information security requirements that should already be in place at participating institutions and their third-party servicers. The Department intends to work with all institutions to improve their information security posture, including those that may not have yet implemented the Safeguards Rule requirements.

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.

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.

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.

The Safeguards Rule and WISPs

- **Do you think you are required by law to have a WISP?**
- **Do you think you need a WISP even though you aren't required by law to have one?**

We create state-specific, company-specific WISPs for people who are required to have them as well as those who know that it is imperative that they have one no matter what.

CONTACT US