FTC Safeguards Rule: What Your Business Needs to Know

Tags: Finance | Privacy and Security | Data Security | Gramm-Leach-Bliley Act

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. The FTC further amended the Rule in 2023 to require covered entities to report certain data breaches and security incidents. Those breach notification requirements took effect in May 2024.

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.

Table of Contents

Who's covered by the Safeguards 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.

What does a reasonable information security program look like?

Section 314.4 of the Safeguards Rule identifies nine elements that your company's information security program must include. Let's take those elements step by step.

a. ***Designate a Qualified Individual to implement and supervise your company's information security program.*** The Qualified Individual can be an employee of your company or can work for an affiliate or service provider. The person doesn't need a particular degree or title. What matters is real-world know-how suited to your circumstances. The Qualified Individual selected by a small business may have a background different from someone running a large corporation's complex system. If your company brings in a service provider to implement and supervise your program, the buck still stops with you. It's your company's responsibility to designate a senior employee to supervise that person. If the Qualified Individual works for an affiliate or service provider, that affiliate or service provider also must maintain an information security program that protects your business.

b. ***Conduct a risk assessment.*** You can't formulate an effective information security program until you know what information you have and where it's stored. After completing that inventory, conduct an assessment to determine foreseeable risks and threats – internal and external – to the security, confidentiality, and integrity of customer information. Among other things, your risk assessment must be written and must include criteria for evaluating those risks and threats. Think through how

customer information could be disclosed without authorization, misused, altered, or destroyed. The risks to information constantly morph and mutate, so the Safeguards Rule requires you to conduct periodic reassessments in light of changes to your operations or the emergence of new threats.

c. ***Design and implement safeguards to control the risks identified through your risk assessment.*** Among other things, in designing your information security program, the Safeguards Rule requires your company to:

1. **Implement and periodically review access controls.** Determine who has access to customer information and reconsider on a regular basis whether they still have a legitimate business need for it.

2. **Know what you have and where you have it.** A fundamental step to effective security is understanding your company's information ecosystem. Conduct a periodic inventory of data, noting where it's collected, stored, or transmitted. Keep an accurate list of all systems, devices, platforms, and personnel. Design your safeguards to respond with resilience.

3. **Encrypt customer information on your system and when it's in transit.** If it's not feasible to use encryption, secure it by using effective alternative controls approved by the Qualified Individual who supervises your information security program.

4. **Assess your apps.** If your company develops its own apps to store, access, or transmit customer information – or if you use third-party apps for those purposes – implement procedures for evaluating their security.

5. **Implement multi-factor authentication for anyone accessing customer information on your system.** For multi-factor authentication, the Rule requires at least two of these authentication factors: a knowledge factor (for example, a password); a possession factor (for example, a token), and an inherence factor (for example, biometric characteristics). The only exception would be if your Qualified Individual has approved in writing the use of another equivalent form of secure access controls.

6. **Dispose of customer information securely.** Securely dispose of customer information no later than two years after your most recent use of it to serve the customer. The only exceptions: if you have a legitimate business need or legal requirement to hold on to it or if targeted disposal isn't feasible because of the way the information is maintained.

7. **Anticipate and evaluate changes to your information system or network.** Changes to an information system or network can undermine existing security measures. For

example, if your company adds a new server, has that created a new security risk? Because your systems and networks change to accommodate new business processes, your safeguards can't be static. The Safeguards Rule requires financial institutions to build change management into their information security program.

8. **Maintain a log of authorized users' activity and keep an eye out for unauthorized access.** Implement procedures and controls to monitor when authorized users are accessing customer information on your system and to detect unauthorized access.

d. ***Regularly monitor and test the effectiveness of your safeguards.*** Test your procedures for detecting actual and attempted attacks. For information systems, testing can be accomplished through continuous monitoring of your system. If you don't implement that, you must conduct annual penetration testing, as well as vulnerability assessments, including system-wide scans every six months designed to test for publicly-known security vulnerabilities. In addition, test whenever there are material changes to your operations or business arrangements and whenever there are circumstances you know or have reason to know may have a material impact on your information security program.

e. ***Train your staff.*** A financial institution's information security program is only as effective as its least vigilant staff member. That said, employees trained to spot risks can multiply the program's impact. Provide your people with security awareness training and schedule regular refreshers. Insist on specialized training for employees, affiliates, or service providers with hands-on responsibility for carrying out your information security program and verify that they're keeping their ear to the ground for the latest word on emerging threats and countermeasures.

f. ***Monitor your service providers.*** Select service providers with the skills and experience to maintain appropriate safeguards. Your contracts must spell out your security expectations, build in ways to monitor your service provider's work, and provide for periodic reassessments of their suitability for the job.

g. ***Keep your information security program current.*** The only constant in information security is change – changes to your operations, changes based on what you learn during risk assessments, changes due to emerging threats, changes in personnel, and changes necessitated by other circumstances you know or have reason to know may have a material impact on your information security program. The best programs are flexible enough to accommodate periodic modifications.

h. ***Create a written incident response plan.*** Every business needs a "What if?" response and recovery plan in place in case it experiences what the Rule calls a security event – an episode resulting in unauthorized access to or misuse of information stored on your system or maintained in physical form. Section 314.4(h) of the Safeguards Rule specifies what your response plan must cover:

- The goals of your plan;
- The internal processes your company will activate in response to a security event;
- Clear roles, responsibilities, and levels of decision-making authority;
- Communications and information sharing both inside and outside your company;
- A process to fix any identified weaknesses in your systems and controls;
- Procedures for documenting and reporting security events and your company's response; and
- A *post mortem* of what happened and a revision of your incident response plan and information security program based on what you learned.

i. ***Require your Qualified Individual to report to your Board of Directors.*** Your Qualified Individual must report in writing regularly – and at least annually – to your Board of Directors or governing body. If your company doesn't have a Board or its equivalent, the report must go to a senior officer responsible for your information security program. What should the report address? First, it must include an overall assessment of your company's compliance with its information security program. In addition, it must cover specific topics related to the program – for example, risk assessment, risk management and control decisions, service provider arrangements, test results, security events and how management responded, and recommendations for changes in the information security program.

What are the Safeguards Rule breach notification requirements?

Section 314.4(j) of the Safeguards Rule requires financial institutions to notify the FTC as soon as possible – and no later than 30 days after discovery – of a "notification event." For purposes of the Rule, a "notification event" is a security breach involving the unauthorized acquisition of at least 500 consumers' unencrypted information. In this context, "unencrypted" information includes encrypted customer information when its encryption key was accessed by an unauthorized person. Additionally, under the Rule, unauthorized access to unencrypted customer information is considered

"unauthorized acquisition" of that information unless reliable evidence shows that there has not been, or could not reasonably have been, unauthorized acquisition of the information in question.

Financial institutions that determine that they've experienced a notification event must report the event using the FTC's online reporting form. When submitting a breach report using the form, there are a few things you should keep in mind:

- The form requires just basic, high-level information about the notification event – the company name, the start and end date of the notification event, the number of customers affected (or potentially affected), the types of customer information involved, and a brief summary of what happened. If FTC staff needs more information, they will contact you to request it.
- If you do not yet know some of the information the form requests (for example, how many consumers were affected or what kind of unencrypted customer information was accessed), just report what you know, and submit a new updated report when you have more details.
- Your report may be made public. For example, your report might be included in a public listing of breach notifications or in response to a Freedom of Information Act request.
- If the police are investigating the breach and they've asked you not to make information about it public yet, you should check the "Law Enforcement Delay Requested" box on the form.

The FTC has more information about the Safeguards Rule and general guidance on data security.

GLOSSARY

Here are some definitions from the Safeguards Rule. Consult 16 C.F.R. § 314.2 for more definitions.

Authorized user means any employee, contractor, agent, customer, or other person that is authorized to access any of your information systems or data.

Customer information means 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 means 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 current cryptographic standards and accompanied by appropriate safeguards for cryptographic key material.

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.

Information security program means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle customer information.

Information system means 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 means 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.

Nonpublic personal information means: (i) Personally identifiable financial information; and (ii) 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.

Penetration testing means a test methodology in which assessors attempt to circumvent or defeat the security features of an information system by attempting penetration of databases or controls from outside or inside your information systems.

Security event means 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 means 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 that is subject to this part.

December 2024