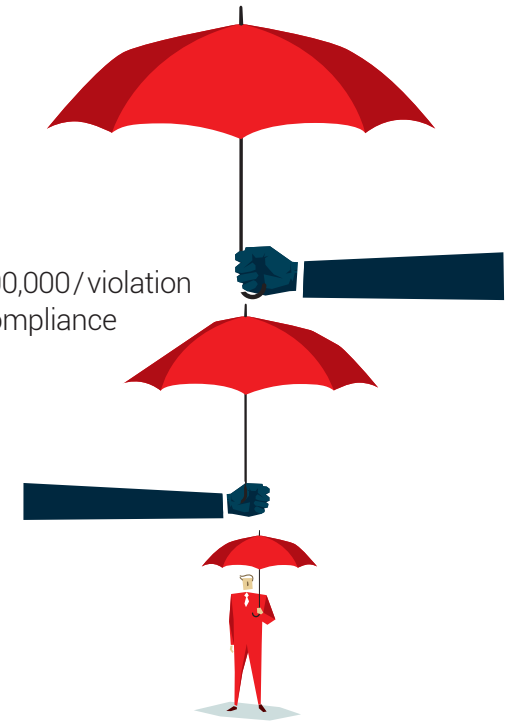
FTC Safeguards Rule

What Your Business Needs to Know



What is it?

A rule requiring financial institutions to take specific steps to protect customer information

Deadline

Must comply by 6/9/23

Penalties

Up to $100,000/violation of non-compliance

Who needs to comply with the Safeguards Rule?

An institution that is significantly engaged in financial activities, or significantly engaged in activities incidental to such financial activities, is a financial institution.

Examples include 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.

What does the Safeguards Rule require companies to do?

Develop, implement, and maintain an information security program with administrative, technical, and physical safeguards designed to protect customer information.

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.

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.

1 **Designate a Qualified Individual** to implement and supervise your company's information security program (can be a service provider).

2 **Conduct a written risk assessment.**

3 **Design and implement safeguards** to control the risks identified through your risk assessment. [Details]

4 **Regularly monitor and test the effectiveness of your safeguards** 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.

5 **Provide your people with security awareness training** and schedule regular refreshers.

6 **Monitor your service providers.** Select service providers with the skills and experience to maintain appropriate safeguards.

7 **Keep your information security program current.**

8 **Create a written incident response plan.**

9 **Require your Qualified Individual to report to your Board of Directors.** 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.

TPX