

# FTC Safeguards Rule



The purpose of the Safeguards Rule, is to protect the security of customer information. It reflects core data security principles that all covered companies need to implement.

## Who's covered by the FTC 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. Some examples of that are:



Retailer that extends credit



Automobile dealership



Personal property or real estate appraiser



Career counselor in financial org



Business that prints and sell checks



Business that wires money for consumers



Check cashing business



Accountant or tax preparation service



Travel agency with financial services



Real estate settlement services



Mortgage broker



Investment advisory company



Company acting as a finder for transactions

## What **Customer Information** needs to be protected?

"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."

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.

[www.turnkeysol.com](http://www.turnkeysol.com) / 225-751-4444



## What does the Safeguards Rule require companies to do?



Develop



Implement



Maintain



Administrative



Technical



Physical

Safeguards designed to protect customer information

## What are the requirements of “Information security program”?

9 elements that your company’s information security program must include:



Designate a Qualified Individual (QI) to implement and supervise an information security program. The QI maybe an MSSP.



Conduct a Risk Assessment.



Design and implement safeguards to control the risks identified through your risk assessment.



Regularly monitor and test the effectiveness of your safeguards.



Implement Security Awareness Training.



Monitor your service providers.



Keep your information security program current.



Create a written incident response plan.



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

