CSBS Nonbank Model Data Security Law

July 25, 2023
|
Download PDF

Data security is paramount to protect nonbank financial institutions and their customers. The CSBS Nonbank Model Data Security Law leverages the FTC Safeguards Rule to establish a robust framework for nonbank financial institutions to mitigate cyber threats, prevent data breaches, and uphold the integrity of the financial system. State regulators are prioritizing data security by adopting the model law and requiring institutions to take the appropriate actions to protect their business and their customers against evolving risks, thereby fostering a secure and resilient state financial system.

Nonbank Model Data Security Law
A Comprehensive Framework for Safeguarding Sensitive Information at Nonbank Financial Institutions
/sites/default/files/2023-07/Data%20Security_0.jpeg
Adoption Resources

Jump to Section: Overview | Key Provisions | Model Law Language | Adoption Resources | More Info

Overview

The Nonbank Model Data Security Law is model statutory language that establishes comprehensive standards for data security in financial institutions. It provides a robust framework to protect sensitive information and mitigate cyber threats across the industry.

The model law is largely based on the FTC Safeguards Rule, including the amendments effective from June 2023 and amendments announced in October 2023. By leveraging the existing applicability of the Safeguards Rule to state covered nonbanks, adopting the model law imposes minimal additional compliance burden. This alignment ensures a streamlined approach to data security regulations and facilitates smoother implementation for financial institutions.

In addition to the full model law, there is alternative language available which requires nonbank financial institutions to conform to the FTC Safeguards Rule. This is a streamlined legislative or rule approach for states looking to implement comparable standards.

By adopting the Nonbank Model Data Security Law, state regulators require financial institutions to meet and exceed data security standards, promoting a secure environment for customer information and reinforcing trust in the industry.

Current Model Data Security Enactments

- State Enacted Model Data Security Enactments

Key Provisions

Following is an overview of the essential provisions of the model law, outlining the standards it establishes for data security in nonbank financial institutions. These key provisions provide insights into the framework designed to protect sensitive information, mitigate cyber threats, and foster a secure financial ecosystem.

Section 3 | Definitions

This section creates consistency and uniform interpretation of key terms to promote uniform implementation of the Model Data Security Law by state regulators.

Section 4 | Standards for Safeguarding Customer Information

This section requires entities to “develop, implement, and maintain a comprehensive Information Security Program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any Customer Information at issue.”

Section 5 | Elements

This section lists the elements that must be found in the nonbank financial institution’s information security program, including:

1. Designate a Qualified Individual to implement and supervise the information security program.
2. Conduct a risk assessment.
3. Design and implement safeguards to control the risks identified through the risk assessment.
4. Regularly monitor and test the effectiveness of the safeguards.
5. Train staff.
6. Monitor service providers.
7. Keep the information security program current.
8. Create a written incident response plan.
9. Require the Qualified Individual to report to your Board of Directors.
10. Notify the commissioner about notification events.
11. Create a written business continuity and disaster recovery plan.

Language of the Model Law

- CSBS Model Data Security Law – February 2024
  - Includes updated notification event language.
- CSBS Model Data Security Law – July 2022
  - Includes original notification event language.
- CSBS Model Data Security Law Alternative Language
- CSBS Model Data Security Law Guidance

Resources for Adopting the Law

- CSBS Model Data Security Law Summary
- Using the CSBS Nonbank Model Data Security Law
- Overview of the Two Versions of the Model Data Security Law
- CSBS Model Data Security Law Compliance Checklist
- FTC Safeguards Rule Compliance Checklist
- Notifications Requirements – Bank vs Nonbank

Additional Information

- FTC Safeguards Rule
- FTC Safeguards Rule Business Guidance
- Final Rule Requiring Financial Institutions to Report Notification Events to the FTC

CSBS Staff Contact: Mike Bray, MBray@csbs.org, 202-559-1953

Related Posts