CSBS Nonbank Model Data Security Law Summary

The CSBS Nonbank Model Data Security Law Summary provides an overview of the model law by addressing the key questions listed below. Please continue reading or click the question link to jump directly to that section.

What is the CSBS Nonbank Model Data Security Law?

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

The model law is largely based on the FTC Safeguards Rule, including the amendments that went into effect on June 9, 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 also ensures a streamlined approach to data security regulations and facilitates a smoother implementation for financial institutions.

Why should state regulators consider adopting the CSBS Nonbank Model Data Security Law?

State regulators should consider adopting the model law due to the following benefits:

Regulatory Oversight:

Adopting the model data security law positions state regulators as proactive in addressing cyber threats. It aligns state regulators with federal standards, leveraging the FTC Safeguards Rule to reduce the regulatory burden for industry participants. By monitoring the implementation and adherence to the standards, state regulators strengthen their regulatory oversight, contributing to a safer financial environment for all stakeholders.

Consumer Protection:

The model law enhances the privacy and security of consumers' personal information, reducing the risk of identity theft and fraud. By adopting robust data security requirements, state regulators instill

consumer trust and confidence in regulated financial institutions. This promotes a more secure and reliable financial landscape to the benefit of consumers.

Collaboration with Other Regulators:

Adopting the data security law allows state regulators to align themselves directly with the FTC and other regulators dedicated to protecting consumer data. It enables state regulators to collaborate and share information with other regulators, promoting a coordinated approach to data security. This coordination promotes effective supervision and consistent standards among state and federal regulators.

What does the model legislation cover?

The CSBS Nonbank Model Data Security Law covers a range of aspects related to data security in nonbank financial institutions. Examples include:

Data Security Standards: The model law establishes comprehensive data security standards that nonbank financial institutions must adhere to. These standards are designed to protect sensitive information and mitigate cyber threats.

Elements of the Information Security Program: The model law establishes ten elements that are required by nonbank financial institutions to include in their information security program. The ten elements include:

1. Designate a Qualified Individual to implement and supervise the company's 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 your 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. Create a written business continuity and disaster recovery plan.

Notification of a Security Event: The model law includes an optional section that addresses the notification process for nonbank financial institutions after a security event. Under this provision, financial institutions must notify the Commissioner once a security event has taken place. The notification should be made within 72 hours of the determination and applies when the financial institution reasonably believes that the number of affected customers meets the threshold specified un the Law. As the proposed rule on notification requirements for the FTC Safeguards Rule is still pending, the model law allows each state regulator to establish their own customer threshold number, providing flexibility in determining the extent of the impact that triggers the notification obligation.

Why are there two versions of the model legislation?

The two versions of the model legislation, the full version, and the alternative language requiring compliance with the FTC Safeguards Rule, accommodate the different needs and circumstances of adopting state regulators.

The full version of the model legislation offers a comprehensive framework, addressing a wide range of data security standards and requirements, sometimes beyond what is covered by the FTC Safeguards Rule. This version provides state regulators with the flexibility to customize and adapt the law to their specific regulatory needs.

On the other hand, the alternative language approach streamlines the adoption process by aligning with the existing FTC Safeguards Rule. By requiring compliance with the FTC Safeguards Rule, state regulators can leverage the established federal standards, reducing the additional regulatory burden on industry participants who are already complying with the Safeguards Rule. This version is particularly beneficial for state regulators s looking for a quicker implementation or primarily seeking consistency with federal regulations.

Providing both versions allow state regulators to choose the approach that best suits their needs and specific requirements.

Who will the model law affect?

The model legislation will affect the nonbank financial institutions operating within the adopting state. State regulators can define the coverage in their state. Per the Coverage Section 2(b):

"Coverage. Persons or entities covered by this law are defined as "Financial Institutions" in Section 3. More specifically, covered financial institutions, persons or entities include, but are not limited to, mortgage lenders, ''pay day'' lenders, finance companies, mortgage brokers, money services businesses, check cashers, collection agencies, credit counselors, [list all appropriate entities]."

Are there any exceptions for nonbank financial institutions in the model law?

The exceptions to the model law are covered in Section 7. However, the model law does not specify the exact sections and leaves this up to each state to determine. Please note that in the FTC Safeguard Rule, Section 314.4(b)(1), (d)(2), (h), and (i) do not apply to financial institutions that maintain customer information concerning fewer than five thousand consumers. This equates to Section 5(b)(1), (d)(2), (h), and (i) in the model law.

My state is not yet ready to adopt the model law. Are there any recommended first steps?

If a state regulator is unable or not prepared to adopt either version of the model law, it is recommended to consider at least adopting the data breach notification section. Doing so provides the following benefits:

Regulatory Oversight: By mandating data breach notifications, state regulators can maintain regulatory oversight over nonbank financial institutions. It allows them to have a comprehensive understanding of the data security landscape, the frequency and severity of breaches, and the potential impact on consumers and the financial industry.

Consumer Protection and Awareness: By requiring nonbank financial institutions to report breaches, state regulators can ensure affected consumers are notified promptly, allowing them to take appropriate actions to protect their personal and financial information.

Advocacy for Resources: Adopting data breach notification requirements can serve to advocate for additional resources, even if the state regulator currently lacks the staffing to individually address every notification. The data obtained from notifications can be used to highlight the magnitude and impact of

security breaches, reinforcing the need for increased resources to strengthen supervision and response capabilities.

If the FTC Safeguards Rule already covers state regulators' needs and nonbank financial institutions must already comply, why do state regulators need their own law?

State regulators have varying authority and comfort enforcing the FTC Safeguards Rule. While a state could identify failures in compliance as a control weakness in an exam, it is questionable whether a state could enforce compliance with the rule directly. By adopting the model law, state regulators are provided with enforcement authority and the ability to address specific needs, like data breach notifications.