Cooley

# Rhode Island Enacts New Financial Institutions Cybersecurity Law With Immediate Effect

July 30, 2025

As the Consumer Financial Protection Bureau (CFPB) and Federal Trade Commission (FTC) scale back rulemaking and enforcement, states are advancing more prescriptive cybersecurity standards for financial institutions, including many that align with the approach and standards set by the New York Department of Financial Services (NYDFS). On July 2, 2025, Rhode Island became the latest state to impose new robust cybersecurity requirements on financial institutions. The new Rhode Island law is effective immediately.

## NYDFS Part 500 precedent

NYDFS has long maintained one of the nation's most prescriptive cybersecurity frameworks through its 23 NYCRR Part 500 Cybersecurity Rules (Part 500). Part 500 imposes technical and administrative cybersecurity requirements on covered entities, which include banks, lenders, insurers, cryptocurrency companies and other financial services providers.

NYDFS amended Part 500 in late 2023, with many of the additional enhanced cybersecurity controls taking effect in May 2025. Those updates to Part 500 include obligations to conduct automated vulnerability scans, maintain stricter access controls, and implement endpoint detection and response tools.

## Rhode Island's Senate Bill 603

The Rhode Island Legislature passed Rhode Island Senate Bill 603 in June 2025, and the governor signed the law on July 2, 2025.

Senate Bill 603 closely tracks NYDFS' Part 500 requirements, requiring nonbank financial institutions licensed by the state's Department of Business Regulation to develop written information security programs and a written incident response plan, perform risk assessments, and implement technical and administrative controls, such as multifactor authentication, access restrictions, and encryption of data at rest and in transit. Financial institutions also must conduct yearly penetration testing and twice-yearly vulnerability scans.

Senate Bill 603 also imposes an express timeline for breach notifications similar to NYDFS' Part 500, with one key change. Financial institutions must notify the director of the Department of Business Regulation **within three business days** of determining a security event has occurred, whereas NYDFS requires notice within 72 hours (regardless of whether the notice period includes nonbusiness days). Given the prevalence of cybersecurity events on weekends and holidays, Rhode Island's law provides financial institutions some welcome leeway relative to the NYDFS requirement.

## Rhode Island deviates from Part 500

Senate Bill 603 differs from Part 500 in how it defines security incidents.

The law defines a "security event" as an event "resulting in unauthorized access to, or disruption or misuse of, an information system or information stored on such information system, or customer information held in physical form … ." A "security event" requires notification when one of the following criteria has been met:

i. The security event requires notice to be provided to any governmental body, self-regulatory agency or any other supervisory body pursuant to any state or federal law.
ii. The security event has a reasonable likelihood of materially harming any consumer residing in Rhode

Island.

iii. The security event materially impacts the normal operations of the company.

These criteria are similar to those in Part 500, although Part 500 does not include a "material harm" to the consumer threshold.

Separately, the law also includes a definition for a "notification event" (defined as the "acquisition of unencrypted customer information without the authorization of the individual to which the information pertains"). However, Senate Bill 603 ultimately does not use the term "notification event" as the trigger for providing notice to the Department of Business Regulation, potentially causing confusion over which definition should prevail when assessing whether to notify the Department of Business Regulation.

Senate Bill 603's use of "security event" rather than "notification event" in the section requiring notice to the regulator creates some ambiguity regarding the circumstances under which a financial institution must notify the regulator. For example, a financial institution may experience an incident that meets the definition of both "security event" and "notification event" but not the criteria for notifying the Department of Business Regulation.

Senate Bill 603 also contains specific limits on the duration of retention for data, requiring covered financial institutions to destroy customer information within a specified time frame unless an exception applies, which may require changes to the data governance programs of licensed entities. Under the law, customer information must be destroyed no later than two years after the information is last used in connection with the provision of a product or service to the customer, unless retention of the information is required by other applicable law or is necessary for the company's business operations or for other legitimate business purposes. Notably, many licensees are subject to federal and state law record retention requirements that extend beyond two years.

Finally, Senate Bill 603 does not require companies to annually certify compliance with the state regulator, a requirement of Part 500.

# State-level trending to the NYDFS cybersecurity model

Historically, the CFPB and FTC have taken a more central role in taking enforcement actions against financial institutions for alleged insufficient cybersecurity practices. However, as the CFPB and FTC have shifted their enforcement priorities in the new administration, a growing number of states have recently passed laws that impose new cybersecurity requirements for financial services providers, indicating a trend in state regulation that is only just beginning.

North Dakota House Bill 1127 passed in April 2025, and the law takes effect on August 1, 2025. Among other things, the law requires that financial institutions maintain written incident response plans, update data retention policies and provide notice to the state's Department of Financial Institutions within 45 days after discovering certain security incidents affecting 500 or more consumers, regardless of state residency. This timeline for providing notice of a security incident is a substantial deviation from Part 500, which, as noted above, requires notice to NYDFS within 72 hours of discovering certain breaches.

Unlike NYDFS Part 500, House Bill 1127 explicitly exempts banks, industrial loan companies, savings and loan associations, and credit unions. Certain provisions of House Bill 1127 also do not apply to entities that process personal data pertaining to fewer than 5,000 consumers.

House Bill 1127 also deviates from Part 500 in that it does not require certification of compliance with the law to the state's Department of Financial Institutions.

Nevada Senate Bill 44 passed in May 2025 and takes effect on January 1, 2026. The bill requires licensed financial institutions in the state to comply with the FTC's Safeguards Rule and requires notification to the Commissioner of Mortgage Lending or the Commissioner of Financial Institutions within 30 days of a "notification event" impacting 500 or more customers. Functionally, Nevada's Senate Bill 44 does not create new obligations on financial institutions, but does allow the state to take enforcement actions against companies for noncompliance with the FTC's Safeguards Rule.

# What's next?

States remain the primary source of forward momentum in financial services cybersecurity, and the trend toward more granular and proactive state-level oversight is only growing. Financial institutions should closely monitor these developments and assess whether their existing cybersecurity programs and incident response plans satisfy this evolving web of obligations. These institutions also should take careful note of the differences across applicable regulations, particularly as related to security incident reporting obligations and record retention.

*Cooley summer associate Nate Low also contributed to this alert.*

This content is provided for general informational purposes only, and your access or use of the content does not create an attorney-client relationship between you or your organization and Cooley LLP, Cooley (UK) LLP, or any other affiliated practice or entity (collectively referred to as "Cooley"). By accessing this content, you agree that the information provided does not constitute legal or other professional advice. This content is not a substitute for obtaining legal advice from a qualified attorney licensed in your jurisdiction, and you should not act or refrain from acting based on this content. This content may be changed without notice. It is not guaranteed to be complete, correct or up to date, and it may not reflect the most current legal developments. Prior results do not guarantee a similar outcome. Do not send any confidential information to Cooley, as we do not have any duty to keep any information you provide to us confidential. When advising companies, our attorney-client relationship is with the company, not with any individual. This content may have been generated with the assistance of artificial intelligence (AI) in accordance with our AI Principles, may be considered Attorney Advertising and is subject to our legal notices.

# Key Contacts



| | |
|---|---|
| Michael Egan<br>Washington, DC | megan@cooley.com<br>+1 202 776 2249 |
| Kate Goodman<br>Chicago | kgoodman@cooley.com<br>+1 312 881 6685 |
| Mari Dugas<br>New York | mdugas@cooley.com<br>+1 202 740 0747 |



This information is a general description of the law; it is not intended to provide specific legal advice nor is it intended to create an attorney-client relationship with Cooley LLP. Before taking any action on this information you should seek professional counsel.

Copyright © 2023 Cooley LLP, 3175 Hanover Street, Palo Alto, CA 94304; Cooley (UK) LLP, 22 Bishopsgate, London, UK EC2N 4BQ. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Cooley LLP as the author. All other rights reserved.