Overview

# New York Department of Financial Services (NYDFS) Cybersecurity Requirements

Dan Pepper and Elyssa Diamond, Norton Rose Fulbright US LLP.

Bloomberg Law

Read Professional Perspectives | Become a Contributor

Reproduced with permission. Published July 2023. Copyright © 2023 Bloomberg Industry Group, Inc. 800.372.1033. For further use, please contact permissions@bloombergindustry.com.

# New York Department of Financial Services (NYDFS) Cybersecurity Requirements

*Contributed by Dan Pepper and Elyssa Diamond, Norton Rose Fulbright US LLP.*

The New York Department of Financial Services (NYDFS) enforces its own cybersecurity requirements for financial service companies. They apply to any organization operating in New York State under authorization of the Banking Law, Insurance Law, or Financial Services Law. This includes credit unions, health insurers, banks, lenders, and life insurance companies, among others.

## Comparison to FTC Safeguards Rule

The NYDFS Cybersecurity Regulation, 23 NYCRR Part 500, builds on many of the same requirements outlined in the Safeguards Rule promulgated under the Gramm-Leach-Bliley Act of 1999 (GLBA) (*see* Overview - Gramm-Leach-Bliley Act (GLBA) Privacy & Data Security), including the following elements:

- Cybersecurity Program: NYDFS requires that covered entities set up a cybersecurity program supported by periodic risk assessments;
- Penetration Testing: NYDFS requires annual penetration testing, and adds the additional requirement of bi-annual vulnerability assessments; and
- Access Privilege: Like the Safeguards Rule, NYDFS requires that covered entities limit who can access the information systems that provide access to the covered nonpublic information.

As in the Safeguards Rule, NYDFS also requires the implementation of multifactor authentication, encryption of confidential information, a written incident response plan, and adequate staff training.

The NYDFS Cybersecurity Regulation also has additional safeguards not included in the Safeguard Rule, including:

- Cybersecurity Policies: NYDFS requires that covered entities develop and enforce written cybersecurity policies and procedures.
- CISO: Rather than a "qualified individual," NYDFS requires that covered entities appoint a Chief Information Security Officer to be responsible for, and to execute, the cybersecurity program.
- Audit Trail: Covered entities must maintain systems that are designed to reorganize financial transactions following a security breach and audit trails.
- Application Security: The cybersecurity program should include written procedures, guidelines, and standards designed to ensure secure development practices for apps designed in-house.

## Proposed Revisions

Additionally, the NYDFS is currently reviewing comments to a proposed amendment to the Cybersecurity Requirements. The proposal, which is likely to be accepted in 2023, would bring about a number of changes to the regulation, including the following:

- Class A Companies: Certain high grossing companies would be considered "Class A" companies and would be subject to addition security requirements.
- Policies: The written policies required by § 500.3 must be approved by the senior governing body of the company at least annually, and should be accompanied by procedures. The amendment also expands the scope of what the written policies and procedures should cover, including data retention, asset end of life management, incident notification, and vulnerability management.

 ©2023 Bloomberg Industry Group, Inc.

- Access Management: Section 500.7, which currently covers access privileges, is expanded to include access management. Some proposed requirements around access management are limiting the number of privileged accounts, reviewing all user access privileges at least annually, and terminating access following employee departures.
- Asset Management: Covered entities will be required to create a complete asset inventory, which should be used as a way of tracking key information about each asset such as the owner, location, and sensitivity.
- Business Continuity: Covered entities will be required to create a business continuity and disaster recovery plant to ensure the availability and functionality of the covered entity's services and protect personnel, assets, and nonpublic information in the case of an emergency.

Track NYDFS rulemaking and other activities related to the NYDFS Cybersecurity Regulation here.


©2023 Bloomberg Industry Group, Inc.