Insights, News & Events

NEW CYBER RULES IN EFFECT AS OF MAY 1 FOR NY FINANCIAL FIRMS: 3 KEY COMPLIANCE PRIORITIES

Insights
May 14, 2025

New cybersecurity requirements just kicked in for thousands of financial firms operating in New York, and companies need to make sure they have taken action to comply. As of May 1, the latest amendments to the New York Department of Financial Services (NYDFS) Cybersecurity Regulation impose stricter technical standards across three major areas: vulnerability scanning, access controls, and threat monitoring. These rules apply to all Covered Entities under the regulation, including insurers and their service providers – and they scale based on company size. With more requirements set to take effect in November, now's the time to assess your systems, update your controls, and ensure your policies meet the state's evolving expectations. Here are the three key compliance priorities you should focus on.

Quick Background on New Cyber Rules

- Compliance with the NYDFS Cybersecurity Regulation is mandatory for all financial services providers operating under the oversight of the NYDFS, including most enterprises engaged in the insurance industry, as well as for Service Providers (see 500.1(s) for the full definition) to those entities.
- In November 2023, the Cybersecurity Regulation (23 NYCRR Part 500) was amended, introducing multiple new requirements that had various effective dates. The most recent amendments came into effect on May 1, and imposed additional technical requirements for Covered Entities (see § 500.1(e) for the full definition).

Related People

Kate Dedenbach, CIPP/US
Of Counsel
248.901.0301

Daniel Pepper, CIPP/US
Partner
303.218.3661

- These requirements are tailored to reflect the size and complexity of entities within New York State's financial services sector. This includes:
  - Large (Class A) Companies, defined under 23 NYCRR 500.1(d) as those with over 2,000 employees or more than $1 billion in gross annual revenue;
  - Small (Exempt) Companies, as described in 23 NYCRR 500.19, which meet certain thresholds for exemption such as fewer than 20 employees or less than $7.5 million in gross annual revenue or less than $15 million in year-end total assets; and
  - Non-Class A, Non-Exempt (Standard) Companies, which fall outside the definitions of Class A or Exempt Companies and are subject to the full scope of the regulation.

The Amendments Primarily Focus on 3 Key Areas

Here are the three key compliance areas you need to know about.

1. Vulnerability Scanning

Under the amended Section 500.5(a), all Covered Entities are required to:

- Conduct automated vulnerability scanning and perform manual scans for any systems not otherwise covered by an automated scanning.

The cadence for reporting and remediating any vulnerabilities identified by the scans should be determined by the Covered Entity's risk assessment and after any material system changes. Manual review is required for unscannable systems.

2. Access Controls

Pursuant to the amended Section 500.7(a), all Covered Entities are required to implement the following access control measures:

- Limit user access privileges to information systems containing nonpublic information to only those necessary for users to perform the user's job, and their access privileged must be reviewed periodically;

Xuan Zhou, CIPP/US, CIPM, CIPP/E

Associate

858.597.9632

Service Focus

Consumer Privacy Team

Privacy and Cyber

Industry Focus

Financial Services

Related Offices

New York

- Minimize the number of privileged accounts and limit the access functions of those accounts to only what is necessary to perform the user's job;
- Restrict the use of privileged accounts so they are only used when performing functions requiring the use of such access;
- Conduct access reviews at least annually to assess all user privileges, and promptly remove or disable accounts and access that are no longer necessary;
- Disable or securely configure all protocols that permit remote control of devices; and
- Promptly terminate user access following an employee's departure or role change that no longer justifies existing access rights.

In addition, Class A Companies must also comply with the requirements of amended Section 500.7 (c) by implementing the following controls:

- A privileged access management (PAM) solution to secure and manage privileged accounts;
- Monitoring of privileges access; and
- An automated method of blocking commonly used passwords for all accounts on information systems owned or controlled by the Class A Company, and wherever feasible, for all other accounts. If the company determines that blocking commonly used passwords is infeasible, then the entity's CISO may instead approve in writing at least annually the infeasibility and authorize the use of reasonably equivalent or more secure compensating controls.

3. Monitoring and Logging

Under the amended Section 500.14(a), Covered Entities are required to implement risk-based controls designed to protect against malicious code, including monitoring and filtering web traffic and the blocking of malicious email content.

In addition, Class A Companies must also implement the following security measures pursuant to amended Section 500.14(b):

- Endpoint Detection and Response (EDR) tools to monitor anomalous activity; and
- Centralized Logging and Security Event Alerting to support timely threat detection and response.

Alternatively, with the CISO's written approval, Class A Companies may implement reasonably equivalent or more secure compensating controls.

Final Portions of Amendments Effective on November 1, 2025

On November 1, 2025, the final portions of the Second Amendment will take effect. These additional requirements focus on the implementation of multi-factor authentication (MFA) for all covered entities regardless of size. They will also mandate a comprehensive data asset inventory that tracks key information for each data asset, including owner, location, classification or sensitivity, expiration date, and recovery time objectives.

Conclusion

These recent amendments to the NYDFS Cybersecurity Regulation represent the continued evolution of the NYDFS's approach to regulate financial services entities and their responsibility to protect customer information from ever-increasing cyber threats. As the regulatory landscape continues to change to address emerging risks, Covered Entities must prioritize compliance to meet legal obligations and to strengthen operational resilience.

If you have any questions about your organization's compliance obligations with the recent amendments, contact your Fisher Phillips attorney, the authors of this Insight, or any member of Fisher Phillips' Data Protection and Cybersecurity Team for guidance. Make sure you are subscribed to the Fisher Phillips Insight system to receive the latest developments straight to your inbox.