November 8, 2023

# NYDFS Finalizes Updates to Part 500 Cybersecurity Regulation

On November 1, 2023, New York Superintendent of Financial Services Adrienne A. Harris announced that the New York State Department of Financial Services ("NYDFS") had finalized updates to the cybersecurity regulations codified in 23 NYCRR 500 ("Part 500").[1] The now final regulations reflect NYDFS's effort to ensure that NYDFS-regulated entities implement robust cybersecurity policies and procedures. They increase the obligations of NYDFS-regulated entities to report cybersecurity events and to protect consumer data, and will require such entities to make larger investments in cybersecurity infrastructure.

The requirements of Part 500 are more stringent than the cybersecurity framework promulgated by the National Institute of Standards and Technology ("NIST") in their incident reporting and cyber defense requirements, and the new regulations heighten the risk that covered entities will face regulatory enforcement. They will require that senior executives of covered entities take more of a role in ensuring that their organizations take appropriate cybersecurity measures, including by requiring senior officials to attest to their organizations' compliance with the increased requirements of Part 500. The new regulations apply (with limited exceptions) to entities regulated by NYDFS, including banks, insurance companies, money services businesses, and virtual currency companies.

Given NYDFS's role as a first-mover in imposing data privacy and cybersecurity requirements in the financial sector, and the various proposals under consideration by other regulators in the space, the new requirements may also be adopted by other state or federal actors and crystallized into guidance and best practices that expand beyond New York and the financial sector.

In general, the updates will be effective 180 days after their adoption, or on April 29, 2024, although the new requirements regarding reporting cyber events are effective one month after adoption, or on December 1, 2023, and certain other requirements go into effect one year, 18 months, and two years after adoption.

## Background

Part 500 requires covered NYDFS-regulated entities to implement specific security safeguards to better protect consumer data. Certain provisions of Part 500 became effective in 2017, with other provisions becoming effective on a rolling basis thereafter. Part 500 applies, with limited exceptions,[2] to Covered Entities, defined as registered entities "operating under or required to operate under a license, registration, charter, certificate, permit, accreditation or similar authorization under the Banking Law,

[1] New York Department of Financial Services. "Press Release: Governor Hochul Announces Updates to New York's Nation-Leading Cybersecurity Regulations as Part of Sweeping Effort to Protect Businesses and Consumers from Cyber Threats." (Nov. 1, 2023), available at https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202311011.

[2] Certain entities and persons are exempted from the NYDFS Part 500 requirements, in whole or in part. *See* 23 NYCRR 500.19(a)–(g). They include certain small businesses, 23 NYCRR 500.19(a), entities covered by another NYDFS regulated businesses cybersecurity policy, 23 NYCRR 500.19(b), entities that do not control an Information System or process non-public information, 23 NYCRR 500.19(c), certain captive insurance companies, 23 NYCRR 500.19(d), certain inactive insurance brokers, 23 NYCRR 500.19(e), and certain other entities such as charitable gift societies, non-New York risk retention groups, certain inactive insurance agents and loan originators, and reinsurers. 23 NYCRR 500.19(g). Entities with exemptions under NYCRR 500.19(a)-(e) are required to file a Notice of Exemption with NYDFS in order to be entitled to the exemption. NYCRR 500.19(f).

the Insurance Law or the Financial Services Law."[3] NYDFS has the authority to enforce violations of Part 500, and has brought thirteen enforcement actions, with some resulting in sizable penalties, over the past three years. These actions were brought against a range of entities in the financial sector, including insurance companies, mortgage brokers, and cryptocurrency firms.[4]

Among other requirements, Part 500 requires Covered Entities to: adopt a written cybersecurity policy;[5] conduct periodic risk assessments to adapt to novel cybersecurity threats;[6] and maintain a cybersecurity program to identify and defend against threats, detect and respond to cybersecurity events, and fulfill reporting obligations.[7] After Part 500 came into effect, other regulatory bodies in the financial sector, including the U.S. Securities and Exchange Commission ("SEC") and National Association of Insurance Commissioners ("NAIC"), adopted similar requirements, establishing the Part 500 framework as a model of cybersecurity regulation.

## Summary of the Updates to Part 500

The updated regulations impose the following heightened data protection requirements on financial entities regulated by NYDFS:

- New Definition of "Class A" companies subject to heightened requirements:
  - Under new Section 500.1(d), a Covered Entity is categorized as a Class A company if it has either (1) employed more than 2,000 people on average over the last two fiscal years, and has over $20 million in gross annual revenue, or (2) has over $1 billion in gross annual revenue in each of the last two fiscal years.
  - Under the proposed amendments, a Class A company is required to:
    - Conduct independent audits of their cybersecurity programs based on their risk assessments;[8]
    - Implement access controls, including monitoring privileged access activity, such as through the use of privileged access management solutions, and impose password complexity requirements on employees;[9] and
    - Conduct risk assessments at least once every three years, implement security measures such as endpoint detection and response systems, and use a centralized solution for system logging and security event alerts.[10]

3 23 NYCRR 500.1(e). The updated regulation clarifies that registered entities are covered "regardless of whether the covered entity is also regulated by other government agencies."

4 *See* New York State Dep't Fin. Servs., *Cybersecurity Resource Center*, available at https://dfs.ny.gov/industry_guidance/cybersecurity.

5 23 NYCRR 500.3

6 23 NYCRR 500.9(a)

7 23 NYCRR 500.2

8 Section 500.2(c)

9 Section 500.7(c)

10 Section 500.14(b)

- Enhanced governance requirements for CISOs and Boards:
  - The new regulations set out new requirements for the Chief Information Security Officer ("CISO") of Covered Entities, including that CISOs:
    - "[T]imely report to the senior governing body or senior officer(s) on material cybersecurity issues, such as significant cybersecurity events and significant changes to the covered entity's cybersecurity program;"[11] and
    - Co-sign, along with the highest-ranking executive of the company, a certification of compliance with the updated cyber regulations.[12]
  - The amendments also impose new duties on boards of directors of Covered Entities, including:
    - Providing oversight to executives regarding the organization's approach to cybersecurity risk management[13] and the creation, implementation and maintenance of the cybersecurity program;[14] and
    - Providing expertise and knowledge, or obtaining advice from persons with such expertise and knowledge, to ensure effective oversight of the organization's management of cybersecurity risks.[15]
- Additional mandatory cybersecurity defense mechanisms:
  - The updated regulations also require regulated entities to employ enhanced cybersecurity testing and surveillance strategies, including:
    - Expanding the existing penetration testing requirement to include assessments "from both inside and outside the information systems' boundaries by a qualified internal or external independent party at least annually";[16]
    - Requiring Covered Entities to conduct "automated scans of information systems," supplemented by "a manual review of systems not covered by such scans," to identify vulnerabilities;[17]
    - Requiring the timely remediation and prioritization of vulnerabilities based on the risk they pose to the Covered Entity;[18]

11 Section 500.4(c)

12 Section 500.17(b)(2)

13 Section 500.4(d)

14 Section 500.4(d)(2)

15 Section 500.4(d)(1); *see also* Section 500.10(a)(2)

16 Section 500.5(a)(1)

17 Section 500.5(a)(2)

18 Section 500.5(c)

- Limiting user access to nonpublic information "to [only that information] necessary to perform the user's job,"[19] restricting the use of privileged accounts to only when required, with annual reviews of all privileged users,[20] and promptly terminating access following user departures;[21]
- Providing annual cybersecurity awareness training regarding social engineering attacks for all personnel in accordance with the Covered Entity's risk assessment;[22]
- Requiring a written password policy that meets industry standards, if passwords are used for authentication;[23] and
- Requiring multi-factor authentication ("MFA") for any individual accessing any information systems of a Covered Entity, except for certain small companies.[24]

- Enhanced monitoring and planning requirements:
  - The updated regulation requires covered entities to implement enhanced cybersecurity monitoring through:
    - Mandatory written policies to ensure a complete, accurate and documented data asset inventory;[25] and
    - A method to track key information for each asset, including the owner, location, classification, and recovery time requirements.[26]
  - Covered Entities are required to allocate sufficient resources to manage cyber risks.[27]
  - Covered Entities are also required to enhance cybersecurity planning efforts, including by adopting "proactive measures to investigate and mitigate disruptive events and ensure operational resilience," such as incident response plans and specified business continuity/disaster recovery plans,[28] and by providing related training to all employees responsible for implementing such plans.[29]
- Enhanced obligations to report cybersecurity events:
  - The proposed regulations retain the definition of the types of cybersecurity events that require reporting to DFS by Covered Entities ("cybersecurity events that have a reasonable likelihood of materially harming any material part of the

19 Section 500.7(a)(1)

20 Section 500.7(a)(3)

21 Section 500.7(a)(4)

22 Section 500.14(a)(3); *see also* New York Department of Financial Services. "Press Release" (Nov. 1, 2023).

23 Section 500.7(b)

24 Section 500.12

25 Section 500.13(a)

26 Section 500.13(a)(1)

27 Section 500.4(d)

28 Section 500.16(a)

29 Section 500.16(c)

normal operation(s) of the covered entity," or for which notice is required by another regulator), but they expand both the scope of events that need to be reported, and the scope of the information that must be provided with those reports, including:

- Requiring notification within 72 hours for cybersecurity events not just at the Covered Entity, but also its affiliates, or third-party service providers;[30] and

- Requiring the Covered entity to provide "any information requested regarding the investigation of the cybersecurity event" within 90 days of a Covered Entity providing notice of the event.[31]

## The Updated Regulations Reflect Industry Comments

As part of its rulemaking process, NYDFS solicited and considered comments from industry participants and other interested parties, and in some cases modified the final rule to accommodate expressed concerns.

For example, the original proposed amendments would have required class A companies to conduct an annual, comprehensive cybersecurity audit. The final regulation adopts a risk-based approach, requiring that class A companies design and conduct independent audits of their cybersecurity programs based on their risk assessment.[32] Similarly, the proposed amendments would have required Covered Entities to provide their CISO with authority to direct sufficient resources to implement an effective cybersecurity program. In response to a comment that CISOs do not typically make such resource allocations, NYDFS revised the regulation to require that the management of Covered Entities allocate sufficient resources to manage cyber risks.[33] And in response to a comment that requiring Covered Entities to report any cybersecurity event where an unauthorized user has obtained access to a privileged account would lead to overreporting, NYDFS eliminated this proposed specific requirement, to only require reporting of such events where reporting is required by the other reporting requirements in the regulation.[34]

## Implications for Companies in the Financial Sector

The NYDFS's updated regulations have significant implications for Covered Entities operating in the financial sector:

- Heightened investments in cyber defense efforts. Covered Entities will need to increase corporate investment in cybersecurity. Specifically, Covered Entities are required to design and implement compliant programs that incorporate planning, testing, surveillance and training.

- Increased likelihood of NYDFS enforcement actions. Covered Entities will face more stringent requirements for managing cybersecurity risks and responding to cybersecurity threats. Both the regulations and the administrative priorities announced by NYDFS emphasize addressing corporate cyber vulnerabilities and taking steps to prevent and respond to cybersecurity events. Failure to respond promptly to the NYDFS's requirements could lead to enforcement actions by the NYDFS.

Potential for similar regulations in other jurisdictions. NYDFS has historically been an early mover in enacting cybersecurity legislation. Many of the provisions of the original Part 500 text were adopted in other regulations, including those promulgated by SEC and NAIC; it is likely that regulators in other jurisdictions and industries will adopt provisions similar to those introduced

30 Section 500.17(a)(1).

31 Section 500.17(a)(2).

32 *See* Section 500.2(c).

33 *See* Section 500.4(d).

34 *See* Section 500.17(a)(iii).

in the proposed amendments to Part 500. As a result, companies in the financial sector and other regulated industries, including those not regulated by NYDFS, should track regulatory developments closely in order to prepare for similar regulations in other settings.

## Conclusion

The updates to Part 500 materially change the regulatory landscape for NYDFS-regulated financial entities. In the short term, companies in the financial sector operating in New York should take steps to strengthen cybersecurity infrastructure to meet the new NYDFS requirements. In the longer term, companies that deal with consumer data in other jurisdictions and industries should consider NYDFS's updated regulations as a bellwether for potential subsequent updates to applicable cybersecurity regulations.

* * *

This memorandum is not intended to provide legal advice, and no legal or business decision should be based on its content. Questions concerning issues addressed in this memorandum should be directed to:

**Jessica S. Carey**
+1-212-373-3566
jcarey@paulweiss.com

**John P. Carlin**
+1-202-223-7372
jcarlin@paulweiss.com

**Yahonnes Cleary**
+1-212-373-3462
ycleary@paulweiss.com

**Roberto Finzi**
+1-212-373-3311
rfinzi@paulweiss.com

**Michael E. Gertzman**
+1-212-373-3281
mgertzman@paulweiss.com

**Roberto J. Gonzalez**
+1-202-223-7316
rgonzalez@paulweiss.com

**Jeannie S. Rhee**
+1-202-223-7466
jrhee@paulweiss.com

**Peter Carey**
+1-202-223-7485
pcarey@paulweiss.com

**Steven C. Herzog**
+1-212-373-3317
sherzog@paulweiss.com