November 15, 2022

NYDFS Proposes Updated Cybersecurity Regulation

On November 9, 2022, New York Superintendent of Financial Services Adrienne A. Harris announced that the New York State Department of Financial Services ("NYDFS") proposed updates to the cybersecurity regulations codified in 23 NYCRR 500 ("Part 500"). The proposed amendments reflect NYDFS' prioritization of ensuring robust cybersecurity measures by NYDFS-regulated entities in the financial sector. If finalized, the proposed updates would significantly increase the obligations of NYDFS-regulated entities to report cybersecurity events and to protect consumer data, requiring greater investment in cybersecurity infrastructure and heightening the risk of regulatory enforcement. The proposed rulemaking is more stringent than the cybersecurity framework promulgated by the National Institute of Standards and Technology ("NIST") in its incident reporting and cyber defense requirements. Moreover, the stricter requirements, if finalized, would become subject to the obligation NYDFS imposes on senior officials to attest to their organizations' compliance with Part 500. The proposed updates would apply to any financial entity regulated by NYDFS, including banks, insurance companies, money services businesses, and virtual currency companies.

The requirements set out in the proposed regulations would substantially increase the enforcement risks faced by NYDFS-regulated entities. 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 in the proposed regulations 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.

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 entering into effect on a rolling basis thereafter. Part 500 applies 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, the Insurance Law or the Financial Services Law."[1] The NYDFS has the authority to enforce violations of Part 500, and has brought six enforcement actions, resulting in sizable penalties, over the past two years.[2] These actions were brought against entities representing diverse parts of the financial sector, including insurance companies, mortgage brokers, and cryptocurrency firms.[3]

1 23 NYCRR 500.1(c)

2 *See, e.g.,* Paul Weiss, Client Alert, *NYDFS Fines First Unum and Paul Revere Insurance Companies $1.8 Million for Violations Arising out of Data Breaches,* (May 20, 2021), available at https://www.paulweiss.com/practices/litigation/cybersecurity-data-protection/publications/nydfs-fines-first-unum-and-paul-revere-insurance-companies-18-million-for-violations-arising-out-of-data-breaches?id=40125.

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

Among other requirements, Part 500 requires Covered Entities to: adopt a written cybersecurity policy;[4] conduct periodic risk assessments to adapt to novel cybersecurity threats;[5] and maintain a cybersecurity program to identify and defend against threats, detect and respond to cybersecurity events, and fulfill reporting obligations.[6]

After Part 500 came into effect, various regulatory bodies in the financial sector and other areas, 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 Proposed Updated Regulations

The changes proposed by the updated regulations reflect an effort to impose heightened data protection requirements in light of the increasing seriousness and number of cybersecurity threats:

- **Definition of "Class A" companies subject to heightened requirements:**
  - Under new Section 500.1(c), a Covered Entity is categorized as a Class A company if it has either (1) employed more than 2,000 people averaged over the last two fiscal years, with over $20 million in gross annual revenue or (2) has made 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 an annual, independent audit of its cybersecurity programs;[7]
    - 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;[8] 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.[9]
- **Enhanced governance requirements for CISOs and Boards:**
  - The proposed regulations set out new requirements on the Chief Information Security Officer ("CISO") of Covered Entities, including requiring that CISOs:
    - Be vested with "adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain a cybersecurity program";[10]

4 23 NYCRR 500.3(k)

5 23 NYCRR 500.9(a)

6 23 NYCRR 500.2

7 Section 500.2(c)

8 Section 500.7(b)

9 Section 500.14(b)

10 Section 500.4(a)

- "[T]imely report to the senior governing body regarding material cybersecurity issues, such as updates to the covered entity's risk assessment or major cybersecurity events;"[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 and direction to executives regarding the organization's approach to cybersecurity risk management[13] and the creation, implementation and maintenance of the cybersecurity program.[14]
- Providing expertise and knowledge, or obtaining advice from persons with such expertise and knowledge, in to ensure effective oversight of the organization's management of cybersecurity risks."[15]

▪ **Additional mandatory cybersecurity defense mechanisms:**

– The proposed regulations also would require 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, as well as the documentation and escalation of "material issues" found during testing;[18] and
- Limiting user access to nonpublic information "to [only that information] necessary to perform the user's job"[19] and restricting the use of privileged accounts to only when required, with annual reviews of all privileged users.[20]

▪ **Enhanced monitoring, planning, and reporting requirements:**

– The proposed rulemaking would require covered entities to implementing enhanced cybersecurity monitoring through:

11 Section 500.4(c)

12 Section 500.17(b)(2)

13 Section 500.4(d)(1)

14 Section 500.4(d)(2)

15 Section 500.4(d)(3)

16 Section 500.5(a)(1)

17 Section 500.5(a)(2)

18 Section 500.5(c)-(d)

19 Section 500.7(a)

20 Section 500.7(a)

- Mandatory written policies to ensure a complete, accurate and documented data asset inventory;[21] and
- Setting up a means to track key information for each asset, including the owner, location, classification, and recovery time requirements.[22]

– Covered Entities would also be required to step up cybersecurity planning efforts, including by drafting key policies to adopt "proactive measures to investigate and mitigate disruptive events and ensure operational resilience," such as incident response plans and specified business continuity/disaster recovery plans.[23]

– The proposed regulations also expand the reporting obligations for Covered Entities by:

- Broadening the notification requirements for cybersecurity events to include "any information requested regarding the investigation of the cybersecurity event" within 90 days of a Covered Entity providing notice of event;[24] and
- Requiring notification within 72 hours for cybersecurity events impacting a third-party service provider.[25]

Implications for Companies in the Financial Sector

The NYDFS's proposed amendments, if finalized, would have significant implications for Covered Entities operating in the financial sector:

- **Heightened investments in cyber defense efforts.** Covered Entities would likely need to increase corporate investment in consumer data privacy. Specifically, Covered Entities would be required to design and implement more rigorous programs that incorporate planning, testing, surveillance, and training.

- **Increased likelihood of NYDFS enforcement actions.** Covered Entities would face more stringent requirements for managing cybersecurity risks and responding to cybersecurity threats. Both the proposed rulemaking 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 efforts to strengthen the cyber integrity of financial companies could lead to enforcement actions related to this area of focus for the NYDFS.

- **Potential for similar regulations in other jurisdictions.** NYDFS has historically been an early mover in enacting cybersecurity legislation. Given the degree to which 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 similar provisions to those introduced in the proposed amendments to Part 500. As a result, companies in the financial sector and other regulated industries should track regulatory developments closely in order to prepare for similar regulations to be enacted in other settings

Conclusion

The proposed rulemaking by the NYDFS, if finalized, would 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 consider how they would strengthen cybersecurity infrastructure to meet the new NYDFS requirements, if enacted. In the longer term,

---

21 Section 500.13(a)

22 Section 500.13(a)

23 Section 500.16(a)

24 Section 500.17(a)(2)

25 Section 500.17(a)(3)

companies that deal with consumer data in other jurisdictions and industries should consider the proposed rulemaking 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:

H. Christopher "Chris" Boehning
+1-212-373-3061
cboehning@paulweiss.com

John P. Carlin
+1-202-223-6115
jcarlin@paulweiss.com

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

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

Roberto J. Gonzalez
+1-202-550-4105
rgonzalez@paulweiss.com

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

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

David Kessler
+1-212-373-3614
dkessler@paulweiss.com

Associates Neil Chitrao and Cole A. Rabinowitz contributed to this Client Memorandum.