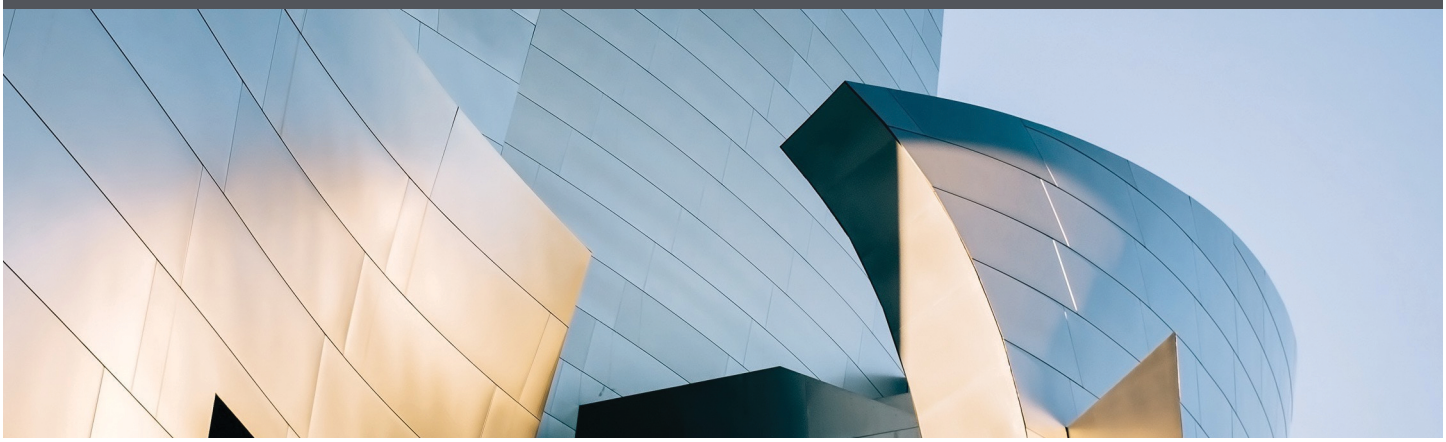
BLANKROME

Financial Institutions Litigation and Regulatory Compliance ("FILARC")



DECEMBER 27, 2022 • NO. 6

NYDFS' Proposed Amendment to Part 500 Includes Important Changes to Cybersecurity Regulations

The New York Department of Financial Services ("NYDFS") released its proposed second amendment to its Cybersecurity Requirements for Financial Services Companies ("Part 500"), which includes heightened cybersecurity requirements for some companies, new security event reporting requirements, and mandated multi-factor authentication for remote access to systems. ***The 60-day public comment period for the proposed amendment ends on January 9, 2023.*** *Covered entities should thoroughly review the proposed amendment and consider submitting comments by the deadline. The newly proposed amendment follows up on the NYDFS' pre-proposal outreach from earlier this year.*

Foremost among the proposed changes is the creation of a separate category of regulated entity known as "Class A Companies." Previously, Part 500 regulations have applied uniformly to all non-exempt entities operating under New York banking, insurance, or financial services law licenses, registrations, or authorizations. The proposed amendments include a heightened set of requirements for Class A Companies, which are defined as entities with at least $20 million in gross annual revenue in each of the last two fiscal years from New York business operations and either: (1) greater than 2,000 employees (including employees of affiliates) averaged over the last two fiscal years, wherever located; or (2) greater than $1 billion in gross annual revenue (including revenue from affiliates) in each of the last two fiscal years from all business operations, wherever located.

Among the heightened requirements specifically applicable to Class A Companies are the following:

1) Performing, at minimum, ***annual independent audits*** of their cybersecurity systems;

2) Blocking weak or commonly used ***passwords*** for all accounts that use company systems (or implementing a similar system with compensating controls);

3) Hiring external experts to conduct a ***cybersecurity risk assessment*** at least once every three years;

4) Implementing an ***endpoint detection and response solution*** to monitor anomalous cybersecurity-related activity including lateral movement; and

5) Implementing a ***centralized system*** for security event logging and alerting.

Additional proposed changes found in the amendment include annual penetration testing obligations and requirements related to implementing monitoring processes to ensure prompt notification of new security vulnerabilities, maintaining written policies and procedures for vulnerability management and conducting automated vulnerability scans, and reviewing and updating risk assessments annually.

Significantly, covered entities will need to utilize multi-factor authentication for all those with remote access to either the entity's information systems or third-party applications, including but not limited to those that are cloud based, from which nonpublic information is available. So-called "Privileged Accounts" (accounts that perform security-relevant functions that ordinary users are not authorized to perform or that can affect material changes to the technical or business operations of the covered entity) will also need to use multi-factor authentication.

Finally, the proposed amendment also defines three new security events that must be reported to the NYDFS within 72 hours:

1) Unauthorized access to Privileged Accounts;

2) Deployment of ransomware within a material part of a covered entity's systems, and

3) Any cybersecurity event affecting a third-party service provider that also affects the covered entity.

After the final amendments are released, they will become effective upon publication of the Notice of Adoption in the New York State Register, but covered entities will have a transition period ranging between 30 days and two years to come into compliance with most of the updated provisions.

If you have any questions regarding the proposed amendments to Part 500 or would like to submit a comment by the January 9, 2023, deadline, please contact Scott D. Samlin, Daniel V. Funaro, or any member of Blank Rome's Financial Institutions and Regulatory Compliance ("FILARC") team.

Scott D. Samlin
212.885.5208 | scott.samlin@blankrome.com

Daniel V. Funaro
202.420.2777 | daniel.funaro@blankrome.com