From: Campbell H. Wallace, Esq. Pastel Rosen & Wallace, LLP.

Date: 11/3/2023

Re: NY finalizes major changes to its cyber security regulation.

Executive summary

On November 1, 2023, New York State's Department of Financial Services issued final regulations regarding cybersecurity for financial services companies. They also posted links to upcoming training sessions starting on November 15, 2023. This final regulation adopted many of the changes proposed in the July 2023 draft amendment, which drew on those first proposed in a November 2022 draft but also adopted a limited number of changes suggested by commenters. The preamble to the adopted regulation highlights the department's approach of requiring regulated entities to deploy reasonable, risk-based measures to protect themselves and their customers from foreseeable cybersecurity threats. Major changes from current regulation and imposed in this version are:

- the recognition of the greater complexity of larger entities, and their inclusion in the newly-created category of "Class A" entities with corresponding additional responsibilities;
- enhanced requirements around periodic system testing, record keeping and maintenance of written incident and recovery plans;
- mandating specific technical approaches such as blocking common passwords and the use of multifactor authentication in certain instances
- directing companies to use recognized industry standards.

When does this take effect?

The regulation is effective November 1, but employs a series of "transitional periods" to phase in compliance obligations. These periods are 30 days (December 1, 2023); 180 days (April 29, 2024), 1 year (November 1, 2024); 18 months (May 1, 2025) and two years (November 1, 2025).

The different classes of businesses recognized in the regulation have different compliance schedules. The Department of Financial Services has released a series of visual flowcharts identifying the timelines for these businesses.

One of the most important changes from current law is the creation of the "Class A company" designation with the attendant obligations. A necessary first compliance step is determining whether you are a Class A company. Class A Companies are described in the analysis of 500.1 below.

The flowchart for class A companies is here

The flowchart for small businesses is here

The flowchart for other covered entities is here

What do you need to know right now?

As noted above, the final regulation adopts many of the changes first proposed in June, but other notable changes are made.

The specific requirements of the final regulation are explained and given further context below:

The procedural history of the regulation is that on November 9, 2022, the Department of Financial Services issued a proposed Second Amendment to DFS's Cybersecurity Regulation, (23 NYCRR Part 500) in the New York State Register. As a result of comments received during the 60-day comment period, which ended on January 9, 2023, a revised proposed Second Amendment was published in the New York State Register on June 28, 2023 along with ninety-two pages of review and analysis of the comments submitted to the November proposal. On November 1, 2023, the final regulation was issued, this time accompanied by a 38 page assessment of public comments.

The final adopted regulation makes incorporated some proposed changes from industry but is substantively similar to the June draft.

While the final regulation significantly revises the existing Part 500, the regulation retains the general structure with which both large and small insurers are familiar. The regulation adds some new requirements – it spells out the need for certain policies to be adopted and formally documented in writing, imposes some additional specific security measures such as automated system scans, password and access management practices, and multifactor authentication, and adds an asset management policy. Many compliance requirements such as penetration testing, and even the role of the CISO are written in contemplation of being delivered in whole or in part by third parties.

Individuals and agent and broker entities should note the Department's proposed adoption of an exemption for inactive insurance agents and agents who meet specific criteria.

Specifically, they are responsible for:

- Annual independent audit of their cybersecurity programs
- Creation and implementation of a privileged access activity management solution with an automated system of blocking commonly used passwords on their accounts
- Implementation of an endpoint detection and response solution, and centralized logging and security event alerting.

Below are selected highlights of changes from the prior regulation, the requirements of the adopted regulation, and brief commentary about the prior proposed changes that led to the new regulation.

Section 500.1 - Definitions

One of the most important changes from current law is the creation of the "Class A company" designation with the attendant obligations. A necessary first compliance step is determining whether you are a Class A company. A Class A company is one, as defined in 500.1(d), with:

with at least $20,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and the business operations in this State of the covered entity's affiliates and:

(1) over 2,000 employees averaged over the last two fiscal years, including employees of both the covered entity and all of its affiliates no matter where located; or

(2) over $1,000,000,000 in gross annual revenue in each of the last two fiscal years from all business operations of the covered entity and all of its affiliates no matter where located.

Class A Companies have additional security obligations. Specifically, they are responsible for:

- Annual independent audit of their cybersecurity programs
- Creation and implementation of a privileged access activity management solution with an automated system of blocking commonly used passwords on their accounts
- Implementation of an endpoint detection and response solution, and centralized logging and security event alerting.

Section 500.1 of the adopted regulation creates a new definition for a Chief Information Security Officer (CISO)

This definition simplifies and clarifies references to a person who bears these responsibilities and creates a uniform reference throughout the regulation. It does not notably amend or expand the duties of this role.

A Chief Information Security Officer is: *"…a qualified individual responsible for overseeing and implementing the covered entity's cybersecurity program and enforcing its cybersecurity policy, who has adequate authority to ensure cybersecurity risks are appropriately managed, including the ability to direct sufficient resources to implement and maintain an effective cybersecurity program*."

The Department earlier explained its reasoning supporting this new definition as: "T*he new category of Class A companies is intended to capture certain larger entities and it is not by itself indicative of these entities' risk exposure. Larger entities by their nature have more systems and those systems are typically more complicated, and these larger entities would benefit from the additional controls and tools required for Class A companies. Larger entities may also have a greater amount of non-public information and a breach at a Class A company could have a greater impact."*

The Department earlier addressed the question of whether an affiliate can qualify as its own Class A Company in the July 2023 comments: *"Whether a covered entity is considered to be Class A depends on its gross annual revenue and number of employees as well as the gross annual revenue and number of employees of its affiliates, <u>but the affiliates cannot become Class A companies themselves unless they are also covered entities</u>…"*

The final draft keeps the definition of "Independent Audit" which allows "**internal** or external auditors," a change which is relevant to the requirements proposed in 500.2.

500.1 also includes an amended definition of "Senior governing body" which means *"the board of directors (or an appropriate committee thereof) or equivalent governing body or, if neither of those exist, the senior officer or officers of the covered entity responsible for the covered entity's cybersecurity program. For any cybersecurity program or part of a cybersecurity program adopted from an affiliate under section 500.2(d) of this Part, the senior governing body may be that of the affiliate."* The introduction of the term "Senior governing body" simplifies and clarifies ongoing references to the organization's leadership including but not limited to the board of directors and committees thereof, and doesn't materially change the specific obligations contemplated.

The adopted regulation also adds a new definition of "cybersecurity incident" using language previously embedded in 500.17(a). This definition was added in acknowledgement of the Department's understanding of typical industry usage.

Section 500.2 – Cybersecurity Program

This section clarifies that the cybersecurity program protect the entity's systems, *and* the nonpublic information they store. This section includes the notable requirement that Class A companies conduct an independent audit at least annually. The proposed requirement to conduct an audit annually was amended and the adopted draft requires that Class A companies design and conduct independent audits of its cybersecurity program based on its risk assessment.

Section 500.3 - Cybersecurity Policy

After proposed changes, the adopted regulation retains the current language allowing a senior officer to approve the written policies. This had been the subject of proposed amendments to only allow approval by the entity's directors or committee.

Sections 500.4 Cybersecurity governance

The final regulation mirrors earlier proposals adds a new 500.4(c) and (d) which together requires a CISO's timely reports to the senior governing body or senior officers and require such bodies to have "sufficient understanding of cybersecurity-related matters" and requires the senior governing body to exercise oversight of the cybersecurity risk management and sets certain standards therefor.

Notably, 500.4 (d) was amended to clarify that the senior governing body's duty is to confirm that the covered entity's management has allocated sufficient resources to implement and maintain an effective cybersecurity program. The newly-defined senior governing body must (1) exercise effective oversight of the covered entity's cybersecurity risk management; ***(2) have sufficient understanding of cybersecurity-related matters to exercise such oversight, which may include the use of advisors;*** (emphasis added) and (3) require the covered entity's executive management or its designees to develop, implement and maintain the covered entity's cybersecurity program.

Section 500.5 Vulnerability Management

This section was renamed and is reworked significantly from the prior regulation and focuses on a risk based system intended to not just scan systems, but inform the entity of identified vulnerabilities. A notable departure from the prior regulation is the requirement that covered entities use automated and manual scans of information systems.

Section 500.7 Access privileges and management

Section 500.7 prescribes detailed access privilege management obligations on entities. It mandates specific protocols for who may access regulated systems and how. The adopted regulation is notable in the degree of technical specificity imposed by the regulation. Importantly, Section 500.7 imposes special obligations on Class A companies to monitor privilege access activity and use an *"an automated method of blocking commonly used passwords for all accounts on information systems…"* but allows an exemption for certain situation where this is infeasible. This requirement was amended in various drafts,

but the adopted regulation imposes it on *"information systems owned or controlled by a Class A company"*

Section 500.8 Application Security

Section 500.8(b) requires an annual cybersecurity risk assessment review. This change from the existing regulation was first proposed in early drafts and is maintained in the final adopted version.

Section 500.9 Risk Assessment

Language in prior drafts' subdivision 500.9(c) was moved to 500.9(a) The new 500.9 (a) reflects the original regulation's language with the added changes and states "(a) Each covered entity shall conduct a periodic risk assessment of the covered entity's information systems sufficient to inform the design of the cybersecurity program as required by this Part. Such risk assessment shall be reviewed and updated as reasonably necessary, but at a minimum annually, and whenever a change in the business or technology causes a material change to the covered entity's cyber risk. The covered entity's risk assessment shall allow for revision of controls to respond to technological developments and evolving threats and shall consider the particular risks of the covered entity's business operations related to cybersecurity, nonpublic information collected or stored, information systems utilized and the availability and effectiveness of controls to protect nonpublic information and information systems."

Notably an earlier draft's requirement that Class A companies shall use external experts to conduct a risk assessment at least once every three years was removed.

Section 500.11 Third party service provider policy.

The adopted regulation mostly mirrors the prior regulation, with the removal of the prior regulation's part (c) which offered exemptions to agents or employees of another covered entity. That exemption is now contained in part 500.19.

Section 500.12 Multi-Factor Authentication

This section updates the prior regulation by more explicitly prescribing the use of multifactor authentication (MFA) in named circumstances unless the entity qualifies for a limited exemption. The circumstances in which MFA must be used are: 1) remote access to the covered entity's information systems; (2) remote access to third party applications, including but not limited to those that are cloud based, from which nonpublic information is accessible; and (3) all privileged accounts other than service accounts that prohibit interactive login.

In response to various comments, the Department reiterated its position on multifactor authentication, stating *"The Department generally attempts to avoid mandating the use of specific techniques or technologies. One exception is multi-factor authentication ("MFA"), which evidence suggests is the best way to avoid breaches and is currently inexpensive and easy to implement."* Comment responses indicate the seriousness with which the Department views MFA implementation; the Department states: "*Section 500.12(a) requires MFA to be used for any individual accessing any information systems of a covered entity, regardless of location, type of user, and type of information contained on the information system being accessed, with few exceptions."*

Section 500.13 Asset management and data retention requirements

The final adopted version section 500.13 includes adopting an asset management requirement as directed by written policies and procedures and describes minimum standards for tracking key information.

Section 500.14 Monitoring and Training.

Section 500.14 (a)(2) was revised to require **risk-based** controls. This change was driven in part by commenters expressing concern with excessively prescriptive requirements and that risk-based measures are more appropriate.

Importantly, this section now requires Class A companies to implement, unless the CISO has approved in writing the use of reasonably equivalent or more secure compensating controls: *1) an endpoint detection and response solution to monitor anomalous activity, including but not limited to lateral movement; and*

(2) a solution that centralizes logging and security event alerting

Section 500.15 Encryption of nonpublic information.

The newly-adopted Section 500.15 restates part of the prior 500.15's requirements and adds language requiring a written policy regarding implementation of a written policy requiring encryption of nonpublic data at rest and in transit over external networks.

Section 500.16 Incident response and business continuity management

Section 500.16 is renamed to highlight its focus on business continuity.

The adopted regulation clarifies specific measures to be included in the written incident response plans and includes backups, plan updates, and the preparation of a root cause analysis.

The new Section 500.16(a)(2) requires business continuity and disaster recovery plans and gives prescriptive guidance on what must be in an entity's business continuity and disaster recovery (BCDR) and how it must be implemented. Such plan must identify documents, relevant personnel and action plans to protect nonpublic information and facilitate recovery of critical data and operation of information systems. It also requires a no-less-frequently than annual test of the BCDR plans and functionality with critical staff.

Section 500.17 Notices to Superintendent

Section 500.17 (a)(1), which deals with cybersecurity event notification, was reworked to require that the Department to be notified of certain cybersecurity-related events and require the annual submission of a periodic statement of compliance or non-compliance, due by April 15. The regulation now mandates notification in a form prescribed on the Department's website. This section further clarifies the specific events that trigger such reporting, including the deployment of ransomware and unauthorized access to a privileged account. The adopted regulation makes clear that the reporting obligation is tied to the covered entity having knowledge of the reportable event and requires that the compliance certification be based on data and documentation sufficient to demonstrate such compliance, or in the case of non-compliance, the areas of noncompliance and a remediation timeline.

A notable change from the prior regulation is the specific focus on extortion payments. Entities must give the Superintendent notice in the prescribed form, within 24 hours of the payment. Further notice is due within 30 days detailing the reasons payment was necessary, a description of alternatives to payment considered, all diligence performed to find alternatives to payment, and all diligence performed to ensure compliance with applicable rules and regulations including those of the Office of Foreign Assets Control.

The adopted 500.17(a)(2) requires that covered entities promptly provide any information requested regarding the cybersecurity event.

The final 500.17(b)(1)(i)(a) and (b)(1)(ii)(b) have adopted "materially" as a qualifier for compliance certification.

500.19 Exemptions

Section 500.19(a) amends the list of limited exemptions and adds that: "(b) An employee, agent, wholly-owned subsidiary, representative or designee of a covered entity, who is itself a covered entity, is exempt from this Part and need not develop its own cybersecurity program to the extent that the employee, agent, wholly-owned subsidiary, representative or designee is covered by the cybersecurity program of the covered entity."

The Department received comments seeking clarification regarding the exemption contained in 500.19(a)(1) designed for smaller entities with comparatively fewer resources than larger organizations. In its summary of responses to comment the Department of Financial Services stated that "The Department is considering providing additional guidance with respect to this limited exemption."

Additionally, the final adopted regulation adjusts the exemption threshold in current 500.19(a)(2) from $5,000,000 to $7,500,000

500.19 Part (e) which essentially exempts inactive insurance brokers, is clarified to refer to selling "any policy" versus earlier draft language which referred to selling "any insurance or annuity."

Part 500.19(g) adds recognized reciprocal jurisdiction reinsurers and inactive individual insurance agents to its exemptions.

Part 500.19(h) was amended to allow 180 days for an entity that ceases to qualify for an exemption to come into compliance. The current regulation calculates dates of determination of noncompliance and compliance obligations on an entity fiscal year basis.

500.20 Enforcement

The adopted Part 500.20 is significantly revised from the prior part 500.20 and adds language clarifying the Department's scope of authority for enforcement, specifically noting that a single prohibited act or failure to act constitutes a violation. The adopted regulation notes such acts include (1) the failure to secure or prevent unauthorized access to an individual's or an entity's nonpublic information due to noncompliance with any section of this Part; or (2) the material failure to comply for any 24-hour period with any section of this Part.

Importantly, this adopted regulation also contains a new part (c) which establishes a partial list of specific factors the department **shall** consider in assessing any violations of Part 500. These provisions lay out a consistent framework for offending entities and the Department to evaluate the context and seriousness of the violation, mitigating efforts and cooperation.

Section 500.22

This section of the regulation lays out the compliance deadlines as explained at the top of this document.

Regulated entities should keep in mind that annual certifications required under section 500.17 are due April 15.