The Asset Management Industry
SERVING INDIVIDUAL INVESTORS
INVESTMENT COMPANY INSTITUTE

MEMO# 30599

February 24, 2017

New York Adopts Cybersecurity Regulation Effective March 1st

[30599] February 24, 2017 TO: ICI Members
Chief Information Security Officer Advisory Committee
Privacy Issues Working Group
Technology Committee
SUBJECTS:

Compliance
Privacy

RE: New York Adopts Cybersecurity Regulation Effective March 1st

The New York Department of Financial Services ("DFS") has announced its adoption of a new cybersecurity regulation that Governor Cuomo touts as a "first-in-the-nation."[1] This new regulation, which is briefly summarized below, takes effect March 1, 2017. Section 500.22 of the regulation provides a transitional period of between 6 months and 2 years (depending on the provision) to comply with the new requirements.

Importantly, the DFS's regulation only applies to those firms that are subject to the DFS's regulation, which does not include mutual funds.[2] Generally speaking, the DFS only regulates banks, insurance companies, and finance companies.[3] As noted below under Section 500.19, Exemptions, insurance companies appear to have been largely exempted from the new regulation.

Summary of the New Regulation

The DFS's new regulation, Cybersecurity Requirements for Financial Services Companies, consists of the following 22 sections:

Section 500.00, Introduction. This section expresses the view that cybersecurity programs are a priority for New York State.

Section 500.01, Definitions. This section defines the variety of terms used in the regulation. Note that "cybersecurity event" is defined broadly to mean *any* act or attempt, successful or unsuccessful, to access, disrupt, or misuse an information system or information on a system.

Section 500.02, Cybersecurity Program. This section requires each person subject to the rule to maintain a cybersecurity program that is designed to protect the confidentiality,

integrity, and availability of such person's information system. This section list the "core cybersecurity functions" of the program.

Section 500.03, Cybersecurity Policy. This section requires each person subject to the regulation to implement and maintain a cyber security policy that is approved by a senior officer or the board. The policy must be based on a risk assessment and must include the 14 elements listed in this section "to the extent applicable" to the person's operations.

Section 500.04, Chief Information Security Officer. This section requires each entity to designate a CISO and defines such person's responsibilities. These responsibilities include, among other things, providing an annual written report to the firms' board of directors on the firm's cyber health.

Section 500.05, Penetration Testing and Vulnerability Assessments. This section requires an entity's cyber program to include monitoring and testing consistent with the entity's risk assessment. Such monitoring and testing must include continuous monitoring or periodic penetration testing and vulnerability assessments.

Section 500.06, Audit Trail. This section requires firms to maintain records required by the regulation for at least three years.

Section 500.07, Access Privileges. This section requires entities to limit user access privileges to information systems that provide access to nonpublic information and to periodically review such privileges.

Section 500.08, Application Security. This section requires entities to create and, thereafter, review, assess, and update, written procedures governing the use of secure development practices for in-house developed applications used by the firm.

Section 500.09, Risk Assessments. This section requires each firm to conduct a periodic risk assessment of its information systems and describes the components of such assessments.

Section 500.10, Cybersecurity Personnel and Intelligence. This section requires firms to have qualified cybersecurity personnel and to ensure such persons' training/skills are current.

Section 500.11, Third Party Service Provider Securities Policy. This section governs the interaction between firms and their service providers with respect to cyber issues.

Section 500.12, Multi-Factor Authentication. This section requires individuals accessing a firm's internal networks from an external network to use multi-factor authentication unless the firm's CISO has approved in writing the use of "reasonably equivalent or more secure access controls."

Section 500.13, Limitations on Data Retention. This section requires firms to have written policies and procedures governing data destruction when data no longer needs to be maintained.

Section 500.14, Training and Monitoring. This section requires each entity's cybersecurity program to monitor the activity of authorized system users and to provide "regular" cybersecurity training for all personnel.

500.15, Encryption of Nonpublic Information. This section requires entities to make sure that nonpublic information in transit or at rest is secured through either encryption or a compensation control approved by the CISO.

Section 500.16, Incident Response Plan. This section requires each entity to establish a written incident response plan for any cybersecurity event "materially affecting the confidentiality, integrity, or availability" of the entity's information systems or its continued business operations.

Section 500.17, Notices to Superintendent. This section requires each entity to report to the Superintendent: (1) within 72 hours following a cybersecurity event that is required to be reported to a governmental entity or that has a reasonable likelihood of materially harming a material part of the entity's normal operations; and (2) annually. The annual report must be filed by February 15th and must be in compliance with Appendix A to the regulation.

Section 500.18, Confidentiality. This section provides that the information provided to the Superintendent under the regulation shall be exempt from public disclosure.

Section 500.19, Exemptions. This section provides the following exemptions:

- A "limited exemption," which only exempts entities from the requirements of Sections 500.04, 500.05, 500.06, 500.08, 500.10, 500.12, 500.14 - 500.16. This limited exemption is available to entities with: (1) fewer than 10 employees located in New York who are responsible for the entity's business; (2) less than $5 million in gross annual revenue from New York business operations in each of the last three years; or (3) less than $10 million in year-end total assets of the entity and its affiliates.
- An exemption for entities that do not directly or indirectly operate, maintain, utilize, or control any information system or that do not control, own, access, generate, receive, or possess nonpublic information. Such entities are exempt from the requirements of Sections 500.02—500.08, 500.10, 500.12, and 500.14-500.16.
- An entity "under Article 70 of the Insurance Law that does not and is not required to directly or indirectly control, own, access, generate, receive, or possess Nonpublic Information other than information relating to its corporate parent company (or Affiliates)." Such entities are exempt from the requirements of Sections 500.02—500.08, 500.10, 500.12, and 500.14-500.16.[4]
- Persons subject to Insurance Law Section 1110 or 5904 and any accredited reinsurer or certified reinsurer that has been accredited or certified pursuant to 11 NYCRR 125.[5]

Section 500.20, Enforcement. This section affirms that the regulation will be enforced by the Superintendent.

Section 500.21, Effective Date. This section affirms (1) that the regulation will be effective March 1, 2017; and (2) the first Notice to the Superintendent required by Section 500.17 must be filed by February 15, 2018.

500.22, Transitional Periods. This section provides that, notwithstanding the effectiveness of the regulation on March 1, 2017, entities will have at least 180 days to comply with the new requirements. In addition, entities will have:

- One year to comply with the requirements of Sections 500.04(b), 500.05, 500.09, 500.12, and 500.14(b);[6]

- Eighteen months to comply with the requirements of Section 500.06, 500.08, and 500.13-500.15;[7] and
- Two years to comply with the requirements of Section 500.11, relating to the security policies of third-party service providers.

Section 500.23, Severability. This is a standard severability clause stating that, if any part of the regulation is judged invalid, such judgment shall not impact the validity of the remainder of the regulation.

The regulation also includes two appendices. Appendix A is the form for the annual certification to the Superintendent under Section 500.17 regarding the entity's compliance with the regulation. Appendix B is the form used to report that the entity is claiming one of the exemptions available under Section 500.19 that requires the filing of a notice with the Superintendent.

Tamara K. Salmon
Associate General Counsel

endnotes

[1] The new regulation is available at: http://www.dfs.ny.gov/legal/regulations/adoptions/rf23-nycrr-500_cybersecurity.pdf. The Governor's announcement of its adoption is available at: http://www.dfs.ny.gov/about/press/pr1702161.htm.

[2] Because the regulation would not impact our members' mutual fund business, the Institute did not comment directly on the proposed regulation when it was twice published for comment during 2016. However, the Institute actively participated in preparing comment letters submitted by the National Business Coalition on E-Commerce and Privacy. [The Institute is an original member of the Coalition.] Both of the letters filed by the Coalition strongly criticized the substance of the proposal and the DFS's failure to (1) evidence the need for the regulation and (2) conduct *any* analysis of the regulation's costs and benefits. With respect to (1), the only evidence the DFS provided to justify the need for the regulation was a report finding that nearly all institutions – almost 90% -- reported having an information security framework in place that includes what are considered to be the key pillars of such programs: (1) a written information security policy, (2) security awareness education and employee training, (3) risk management of cyber-risk, inclusive of key risks and trends, (4) information security audits, and (5) incident monitoring and reporting." This report expressly concludes that "information security programs at medium and large institutions *tend to be particularly well developed, with 89% and 98%, respectively, having implemented all five pillars.*" Notwithstanding these findings, the DFS used the report to justify adoption of the regulation.

[3] The Office of New York's Attorney General regulates the securities industry pursuant to New York's Martin Act. Such authority, however, is limited pursuant to the preemption contained in the National Securities Markets Improvement Act of 1996. For more information about the DFS's authority, see its website at: http://www.dfs.ny.gov/about/dfs_about.htm.

[4] Entities claiming an exemption under the first three bullets must file with DFS a Notice of Exemption within 30 days of the entity determining it is exempt. This notice must be in the form set forth in Appendix B of the regulation.

[5] The two exemptions provided under the Insurance Law were new to the final draft of the regulation – they were not in the proposed regulation when it was twice published for comment.

[6] These sections govern: designation of a CISO; penetration testing and vulnerability assessments; risk assessments; multi-factor authentication; and training and monitoring.

[7] These sections govern: the audit trail; application security; limitations on data retention; training and monitoring; and encryption of nonpublic information.
