Director and Officer Checklist:

Complying with the global reach of the New York DFS Cybersecurity Regulation

The New York State Department of Financial Services (NYDFS) issued Cybersecurity Requirements for Financial Services Companies (the "Cybersecurity Regulation") effective March 1, 2017. The regulation imposes tight compliance deadlines, which begin on August 28, 2017, on institutions operating under New York's banking, financial services or insurance laws.

Perhaps least understood outside of New York is the regulation's potential reach, which extends well beyond New York and, indeed, well beyond the United States. Absent careful consideration and planning, global, national and regional institutions that have as little as a single corporate affiliate (or a single individual agent or representative) operating under New York's supervision may find their entire cybersecurity program under New York's watchful eye, regardless of whether the cybersecurity program is housed in New York or controlled by the New York entity. Consider, for example, a parent company outside New York that operates a single corporate network on behalf of each of its subsidiaries. Under the new regulation, all of the parent company's documentation and information that is relevant to the New York entity's cybersecurity program must be made available to NYDFS upon request.

What follows is a useful checklist to help officers and directors adequately monitor and oversee their company's Cybersecurity Regulation compliance efforts.

My organization understands whether it must comply with the Cybersecurity Regulation

We have determined which, if any, of our companies and individual representatives/agents is subject to New York's Cybersecurity Regulation ("Covered Entities").

If there are one or more Covered Entities, we have determined whether they will need to rely upon any resources (networks, policies or personnel) of a corporate affiliate to fulfill their compliance obligations and, if so, we understand how any shared corporate resources will be subject to New York's review.

My organization understands who is responsible for ensuring compliance with the Cybersecurity Regulation

- ☐ We have designated a qualified individual (such as a CISO) to oversee and implement the Covered Entity's cybersecurity program and enforce its policies.
- ☐ We understand the requirement to sign an annual certification of full compliance.
- ☐ We have designated one or more qualified Senior Officers, or the entire Board of Directors, to sign the annual certification, and have informed them of their responsibility.
- ☐ We are maintaining the records, schedules and data to support our annual certification of compliance, and will maintain those records for the required period of five years to be made available upon New York's request.
- ☐ The Board of Directors (or equivalent governing body) of each Covered Entity will receive a written report, no less than annually, about the Covered Entity's cybersecurity program and material cybersecurity risks.

☐ **My organization understands its cybersecurity risk management requirements**

- ☐ We have identified the most significant internal and external risks to the security or integrity of our data and systems.
- ☐ We have a written risk assessment that takes into account the adequacy of existing controls in the context of identified risks, and describes plans to address any gaps.
- ☐ We have a roadmap for implementing each of the 17 substantive sections of the Cybersecurity Regulation that complies with the specific requirements of each substantive section, and takes into account:
  - their varying due dates,
  - how much lead time is anticipated for their completion,
  - the resources that will be required, and
  - how we measure success.
- ☐ We are providing cybersecurity awareness training to our personnel, incorporating guidance on the specific risks identified in our risk assessment.
- ☐ We are encrypting nonpublic information while it is in transit over external networks and while it is at rest, unless we have determined and documented that it is "infeasible" to do so and have implemented effective, alternative compensating controls.
- ☐ We have a written incident response plan that addresses the internal process for responding to a security incident and identifies the internal stakeholders and external third parties that compose the incident response team.
- ☐ We understand all of the circumstances that require us to notify New York about a cybersecurity event, and we are prepared to do so within 72 hours of determining such an event has occurred.

☐ **My organization understands its responsibility for the security of third-party service providers**

- We have implemented written policies and procedures that address the adequacy of security-of-information systems containing nonpublic information that is accessed or held by third-party service providers.

☐ **My organization is prepared to demonstrate its compliance**

- ☐ We have adopted and implemented industry-recognized guidance, frameworks or best practices to address each of the 14 cybersecurity policy areas outlined in the Cybersecurity Regulation.
- ☐ We have documented the implementation of the specific access controls New York requires, including access privileges, application security, multi-factor authentication, network monitoring and encryption.
- ☐ We have documented our requirements for either mitigating or accepting identified cybersecurity risks, and our decisions are consistent with our risk profile and regulatory requirements.
- ☐ We have identified and documented remedial efforts that are planned and underway to address areas, systems or processes that require material improvement, updating or redesign.