NEW YORK STATE
DEPARTMENT *of*
FINANCIAL SERVICES

Cyber Security:

1. Please provide a copy of the firm's cyber security program that is based on the firm's risk assessment, including supporting documentation, such as policies, procedures, and processes relating to the following, including an index showing which policy, procedure, and process maps to each of the following:

   (a) information security;

   (b) data governance and classification, including data retention and disposal;

   (c) asset inventory and device management;

   (d) access controls, including physical control, and identity management;

   (e) business continuity and disaster recovery planning and resources;

   (f) systems operations and availability concerns;

   (g) systems and network security;

   (h) systems and network monitoring;

   (i) systems and application development and quality assurance;

   (j) physical security and environmental controls;

   (k) customer data privacy;

   (l) vendor and third party service provider management, including any security policies and procedures;

   (m) risk assessment;

   (n) incident response; and

   (o) data encryption if available.

2. Please detail the involvement of the board of directors, an appropriate committee of the board, an equivalent governing body, or the senior management, in the development or approval of the cyber security program of the firm, including an organizational chart detailing the organizational hierarchy, as well as the individuals involved, and their titles, positions, and roles.

3. Please describe how the risk assessment assesses the likelihood and potential damage of identified threats, taking into account, the sensitivity of information that may be impacted.

4. Please describe how the risk assessment takes into account the sufficiency of policies and procedures and other arrangements in place to control identified risks.

5. How frequently does the firm update its risk assessment? Please provide a copy of any policy and procedure relating to the types of events or circumstances that would trigger an update to the risk assessment, such as the development of new products or services, new geographies of operation, or evolving threats. Please provide information as to the total number of updates made to the firm's risk assessment during the past calendar year.

6. Please provide a list of any review of the firm's cybersecurity program, including any self-evaluation or gap analysis conducted with respect to the program, any report prepared by a third-party consultant engaged to review the program, or internal audit report or any other documentation regarding any internal audit examination of the program.

7. Please provide a complete copy of the risk assessment of the firm that forms the basis of the firm's cyber security program, including any summary or analysis used to report the result of such assessment to the firm's senior management, board of directors, an appropriate committee of the board, or an equivalent governing body.

8. Please identify whether or not the firm is claiming any exemption from any part of 23 NYCRR 500, and if so, the exemption claimed and documents sufficient to show the analysis of the firm's entitlement to that exemption.

9. Please provide an organizational chart identifying the firm's cybersecurity personnel, including the reporting structure within the firm and job responsibilities.

    - To the extent that the firm has a Chief Information Officer and Chief Information Security Officer ("CISO"), please provide the resume of such individuals.

    - To the extent that the firm has met its CISO requirement using an affiliate or third party service provider, please indicate the senior member(s) of the firm's personnel responsible for direction and oversight of the outsourced function.

10. Please provide a copy of any agreement or arrangement with a third-party service provider for outsourcing the firm's cyber security program and/or risk assessment.

11. Please provide a copy of all reports or presentations regarding the firm's cybersecurity controls submitted to its board of directors, an appropriate committee of the board, an equivalent governing body, or the senior management of the firm responsible for the firm's cybersecurity program. Please state the frequency of such submissions.

12. To the extent that the firm has identified areas, systems or processes that require material improvement, updating or redesign, please produce the schedule identifying such items and the remedial efforts underway to address such areas, systems or processes.

13. Please provide a copy of the most recent cybersecurity training conducted by the firm, including training materials and attendance logs of the training, and a schedule of its training planned for the coming calendar year.

14. To the extent not already provided to the Department, please provide a list of all cybersecurity events or incidents reported to any regulatory, governmental or enforcement agency in any jurisdiction in the past calendar year, including the date, description, the agency, jurisdiction, and a summary of any action or steps taken in response to any such event or incident.

15. Please make available minutes of any cybersecurity management or IT steering committee meetings during which cybersecurity is discussed.