SAMPLE FINRA REQUEST

1. Please provide all of the firm's current procedures and policies established to protect client, trade, and confidential firm data. These may include policies and procedures as noted below and may include other processes in place at the firm. Examples of policies and procedures include Password Management, Vendor Management, Patch Management, Security Training, Penetration Testing, Data Classification and Encryption, Change Management, and Incident Response etc.

2. Please supply an organization chart (or similar document) that outlines the teams/departments that are involved in the protection of information (confidential firm data or client information) from cybersecurity incidents.

3. Please provide a listing of cybersecurity issues the firm has identified within the last 12 months. These issues could include but are not limited to: Unauthorized access to customer information, Customer account loss or take over, DDOS attacks causing outages, Lost or stolen hand-held devices, Malware infections, Phishing messages to employees or customers, System penetration by outsiders, Web Site defacement, Password sniffing, or others, etc.

4. Please describe any internal testing of the firm's cybersecurity programs during the past 12 months. Please provide a list of these tests and related findings. In addition, please provide a summary of the third party reviews of the firm's cybersecurity system.

5. Please provide a list of customer, trade, firm, or other confidential databases including the storage location, whether or not the data is encrypted at rest, how the data is backed up, and how compliance is achieved with SEC Reg 17a-3/4. Please include external systems and cloud storage locations.

6. Provide a list of any training provided by the firm to its employees or registered representatives in the past 12 months related to information security and risks and indicate the nature of the training method (e.g., in person, computer based learning, or email alerts). Please identify the dates, topics, and groups of participants for these training events and provide a copy of any written guidance or training materials provided.

7. Provide a list of the systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to confidential data including client, trading and confidential firm data and assets. Please include a brief description of their functions and whether the systems are proprietary, managed by a third party, or commercial off-the-shelf products.

8. Provide a list of all third-party vendors with access to the firm's network or data including a brief description of the service (or type of service) the vendor provides to the firm.

9. Please describe the process followed by the home office to communicate, oversee compliance, and audit the cybersecurity controls in the firm's branch offices.

10. Provide a copy of your firm's Business Continuity Plan (BCP), Disaster Recovery Plan (DRP), and as well as your firm's Incidence Response Plan (IRP).

11. Provide evidence of the most recent tests performed on the BCP, DR and IRP.

12. Provide an excerpt of the most recent annual report to senior management regarding risk assessments and unauthorized activities or intrusions and corrective action taken.\

13. Provide a copy of the Electronic Communications Systems and Devices Policy, Mobile Devices policy, Data Protection Policy and your Information Security Policy.