Examination Period

Information is requested for the period **January 1, 2013** through **April 30, 2014** (the "Examination Period") unless otherwise noted.

Organizing the Information to be Provided

Please provide the requested information and documentation in encrypted, electronic format, and group the items so that each item corresponds to an item number in the request list, naming each item with an identifiable title. If an item provided is responsive to more than one request, you may provide it only once and refer to it when responding to the other requested item numbers. If any of the items requested are not applicable, please indicate that in your response.

Identification of Risks/Cybersecurity Governance

1. For each of the following practices employed by the Firm related to the management of information security, please provide: the month and year in which the noted action was last taken; the frequency with which such practices are conducted; the group with responsibility for conducting the practice; and, if not conducted firm-wide, the areas that are included within the practice. Please also provide a copy of any relevant policies and procedures.

    a. Physical devices and systems within the Firm are inventoried.

    b. Software platforms and applications within the Firm are inventoried.

    c. Maps of network resources, connections, and data flows (including locations where client data is housed) are created or updated.

    d. Connections to the Firm's network from external sources are catalogued.

    e. Resources (hardware, data, and software) are prioritized for protection based on their sensitivity and business value.

    f. Logging capabilities and practices are assessed for adequacy, appropriate retention, and secure maintenance.

2. Please provide a copy of the Firm's written information security policy. If the Firm has a board of directors, please also provide copies of any relevant board minutes and any pertinent briefing documents provided to the Firm's board regarding cybersecurity risk issues, cybersecurity incident response planning, or any cybersecurity incident since January 1, 2013, if applicable.

3. Please indicate whether the Firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. If such assessments are conducted, please also:

a. Identify who (individual(s), business group(s), and title(s)) conducts them, and the month and year in which the most recent assessment completed.

b. Describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated. Alternatively, provide written reports from the review that discuss the findings and remediation efforts.

4. Please indicate whether the Firm conducts periodic risk assessments to identify physical security threats and vulnerabilities that may bear on cybersecurity. If such assessments are conducted:

   a. Identify who (business group/title) conducts them, and the month and year in which the most recent assessment completed.

   b. Describe any findings from the most recent risk assessment that were deemed to be potentially moderate or high risk and have not yet been fully remediated. Alternatively, provide written reports from the review that discuss the findings and remediation efforts.

5. If cybersecurity roles and responsibilities for the Firm's workforce and managers have been explicitly assigned and communicated, please provide written documentation of these roles and responsibilities. If no written documentation exists, please provide a brief description.

6. Please provide a copy of the Firm's written business continuity of operations plan that addresses mitigation of the effects of a cybersecurity incident and/or recovery from such an incident if one exists.

7. Please provide the name of the Firm's Chief Information Security Officer, or, if one does not exist, an equivalent position (name and title). If an individual does not serve in this capacity, address with whom or where the principal responsibility for overseeing cybersecurity reside within the Firm.

8. Please briefly identify the insurance carrier for the Firm that specifically covers losses and expenses attributable to cybersecurity incidents, if applicable. Also, please briefly describe the nature of the coverage and indicate whether the Firm has filed any claims, as well as the nature of the resolution of those claims.

Protection of Firm Networks and Information

9. Please identify any published cybersecurity risk management process standards that the Firm has used to model its information security architecture and processes (*i.e.*, those issued by the National Institute of Standards and Technology (NIST) or the International Organization for Standardization (ISO)).

10. Please indicate which of the following practices and controls regarding the protection of its networks and information are utilized by the Firm, and provide any relevant policies and procedures for each item.

a. The Firm provides written guidance and periodic training to employees concerning information security risks and responsibilities. If the Firm provides such guidance and/or training, please provide a copy of any related written materials (*e.g.*, presentations) and identify the dates, topics, and which groups of employees participated in each training event conducted since January 1, 2013.

b. The Firm maintains controls to prevent unauthorized escalation of user privileges and lateral movement among network resources. If so, please describe the controls, unless fully described within policies and procedures.

c. The Firm restricts users to those network resources necessary for their business functions. If so, please describe those controls, unless fully described within policies and procedures.

d. The Firm maintains an environment for testing and development of software and applications that is separate from its business environment.

e. The Firm maintains a baseline configuration of hardware and software, and users are prevented from altering that environment without authorization and an assessment of security implications.

f. The Firm has a process to manage IT assets through removal, transfers, and disposition.

g. The Firm has a process for ensuring regular system maintenance, including timely installation of software patches that address security vulnerabilities.

h. The Firm's information security policy and training address removable and mobile media.

i. The Firm maintains controls to secure removable and portable media against malware and data leakage. If so, please briefly describe these controls.

j. The Firm maintains protection against Distributed Denial of Service (DDoS) attacks for critical internet-facing IP addresses. If so, please describe the internet functions protected and who provides this protection.

k. The Firm maintains a written data destruction policy.

l. The Firm maintains a written cybersecurity incident response policy. If so, please provide a copy of the policy and indicate the year in which it was most recently updated. Please also indicate whether the Firm conducts tests or exercises to assess its incident response policy, and if so, when and by whom the last such test or assessment was conducted.

m. The Firm periodically tests the functionality of its backup system. If so, please provide the month and year in which the backup system was most recently tested.

11. Please indicate whether the Firm makes use of encryption. If so, also identify the categories of data, communications, and devices are encrypted and under what circumstances.

12. Please indicate whether the Firm conducts periodic audits of compliance with its information security policies. If so, identify who (individual(s), business group(s), and title(s)) conducts them, and the month and year in which the most recent audit was completed.

Risks Associated With Remote Access to Client Information and Funds Transfer Requests

13. Please indicate whether the Firm provides clients with on-line account access. If so, please provide the following information:

    a. The name of any third party or parties that manage the service.

    b. The functionality for clients on the platform (e.g., balance inquiries, address and contact information changes, beneficiary changes, transfers among the clients' accounts, withdrawals or other external transfers of funds).

    c. How clients are authenticated for on-line account access and transactions.

    d. Any software or other practice employed for detecting anomalous transaction requests that may be the result of compromised client account access.

    e. A description of any security measures used to protect client PINs stored on the sites.

    f. Any information given to clients about reducing cybersecurity risks in conducting transactions/business with the Firm.

14. Please provide a copy of the Firm's procedures for verifying the authenticity of email requests seeking to transfer client funds. If no written procedures exist, please describe the process.

15. Please provide a copy of any Firm policies for addressing responsibility for losses associated with attacks or intrusions impacting clients.

Risks Associated With Vendors and Other Third Parties

16. If the Firm conducts or requires cybersecurity risk assessments of vendors and business partners with access to the Firm's networks, client data, or other sensitive information, or due to the cybersecurity risk of the outsourced function, please describe who conducts this assessment, when it is required, and how it is conducted. If a questionnaire is used, please provide a copy. If assessments by independent entities are required, please describe any standards established for such assessments.

17. If the Firm regularly incorporates requirements relating to cybersecurity risk into its contracts with vendors and business partners, please describe these requirements and the circumstances in which they are incorporated and provide a sample copy.

18. Please provide a copy of policies and procedures and any training materials related to information security procedures and responsibilities for trainings conducted since January 2013 for vendors and business partners authorized to access its network.

19. If the Firm assesses the segregation of sensitive network resources from resources accessible to third parties, identify who (individual(s), business group(s), and title(s)) conducts them, and the month and year in which the most recent assessment completed.

20. If vendors, business partners, or other third parties may conduct remote maintenance of the Firm's networks and devices, describe any approval process, logging process, or controls to prevent unauthorized access, and provide a copy of any relevant policies and procedures.

Detection of Unauthorized Activity

21. For each of the following practices employed by the Firm to assist in detecting unauthorized activity on its networks and devices, please briefly explain how and identify who (individual(s), business group(s), and title(s)) carries the practice out.

    a. Identifying and assigning specific responsibilities, by job function, for detecting and reporting suspected unauthorized activity.

    b. Maintaining baseline information about expected events on the Firm's network.

    c. Aggregating and correlating event data from multiple sources.

    d. Establishing written incident alert thresholds.

    e. Monitoring the Firm's network environment to detect potential cybersecurity events.

    f. Monitoring the Firm's physical environment to detect potential cybersecurity events.

    g. Using software to detect malicious code on Firm networks and mobile devices.

    h. Monitoring the activity of third party service providers with access to the Firm's networks.

    i. Monitoring for the presence of unauthorized users, devices, connections, and software on the Firm's networks.

    j. Evaluating remotely-initiated requests for transfers of client assets to identify anomalous and potentially fraudulent requests.

k. Using data loss prevention software.

l. Conducting penetration tests and vulnerability scans. If so, please identify the month and year of the most recent penetration test and recent vulnerability scan, whether they were conducted by Firm employees or third parties, and describe any findings from the most recent risk test and/or assessment that were deemed to be potentially moderate or high risk but have not yet been addressed.

m. Testing the reliability of event detection processes. If so, please identify the month and year of the most recent test.

n. Using the analysis of events to improve the Firm's defensive measures and policies.

Other

22. Identify whether the Firm updated its written procedures to reflect the Identity Theft Red Flags Rules, which became effective in 2013. If the written procedures were not updated, explain why.

23. List the factors the Firm has identified as relevant best practices regarding cybersecurity for its business model.

24. **Since January 1, 2013**, identify whether the Firm experienced any of the types of events listed below. If so, please provide a brief summary for each category, identifying the number of such incidents (approximations are acceptable if precise numbers are not readily available) and describing their significance and any effects on the Firm, its clients, and its vendors or affiliates. If the response to any one item includes more than 10 incidents, the Firm may note the number of incidents and describe incidents that resulted in losses of more than $5,000, the unauthorized access to client information, or the unavailability of a Firm service for more than 10 minutes. The record or description should, at a minimum, include: the extent to which losses were incurred, client information accessed, and Firm services impacted; the date of the incident; the date the incident was discovered and the remediation for such incident.

    a. Malware was detected on one or more Firm devices. Please identify or describe the malware.

    b. The availability of a critical Firm web or network resource was impaired by a software or hardware malfunction. (Down time resulting from routine maintenance and equipment upgrades should not be included in this response.) Please identify the service affected, the nature and length of the impairment, and the cause.

    c. The Firm's network was breached by an unauthorized user. Please describe the nature, duration, and consequences of the breach, how the Firm learned of it, and how it was remediated.

d. The compromise of a client's or vendor's computer used to remotely access the Firm's network resulted in fraudulent activity, such as efforts to fraudulently transfer funds from a client account or the submission of fraudulent payment requests purportedly on behalf of a vendor.

e. The Firm received fraudulent emails, purportedly from clients, seeking to direct transfers of client funds or securities.

f. The Firm was the subject of an extortion attempt by an individual or group threatening to impair access to or damage the Firm's data, devices, network, or web services.

g. An employee or other authorized user of the Firm's network engaged in misconduct resulting in the misappropriation of funds, securities, sensitive client or Firm information, or damage to the Firm's network or data.

25. **Since January 1, 2013**, if not otherwise reported above, identify whether the Firm, either directly or as a result of an incident involving a vendor, experienced theft, loss, unauthorized exposure, or unauthorized use of or access to client information. Please respond affirmatively even if such an incident resulted from an accident or negligence, rather than deliberate wrongdoing. If so, please provide a brief summary of each incident or a record describing each incident.

26. For each event identified in response to Questions 24 and 25 above, please indicate whether it was reported to the following:

    a. Law enforcement (please identify the entity)

    b. FinCEN (through the filing of a Suspicious Activity Report)

    c. FINRA

    d. A state or federal regulatory agency (please identity the agency and explain the manner of reporting)

    e. An industry or public-private organization facilitating the exchange of information about cybersecurity incidents and risks

27. Identify what the Firm presently considers to be its three most serious cybersecurity risks, and why.

28. Please feel free to provide any other information you believe would be helpful to the SEC in evaluating the cybersecurity posture of the Firm or the securities industry.