Attachment A – Document Request List

Governance and Risk Assessment

Provide in Advance

1. Provide a copy of firm policies and procedures addressing the protection of customer/client records and information, including those that are designed to secure customer/client documents and information; protect against anticipated threats to customer/client information; and protect against unauthorized access to customer/client accounts or information for the review period. *Please note that subsequent questions in this Request Letter may ask for policies and procedures that are covered by the documents produced in response to this question. For those questions, reference this question and specifically indicate where the information can be found within the documents produced.*

Provide in Advance

2. If the firm has a board of directors ("Board"), provide copies of all Board minutes and briefing material regarding cybersecurity-related risks, cybersecurity incident response planning, actual cybersecurity incidents, and cybersecurity-related matters involving vendors within the review period.

Provide in Advance

3. Identify the Chief Information Security Officer ("CISO") or equivalent position. If the role does not exist, explain where the principal responsibility for overseeing cybersecurity resides within the firm.

Provide in Advance

4. Provide organizational charts which illustrate the positions and departments responsible for cybersecurity-related matters and where these individuals and departments fit within the firm's organization or hierarchy. Please also identify and briefly describe the roles and responsibilities of the CISO or equivalent role and any additional supporting roles responsible for cybersecurity matters and identify lines of authority and reporting.

Make Available On-Site

5. If the firm conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences, please indicate the month and year in which the most recent risk assessment was completed and describe the scope of review.

Make Available On-Site

   a. Please identify any moderate or high risk findings and any remediation efforts undertaken in response to each finding.

Provide in Advance

6. Provide a copy of any firm policies related to penetration testing.

Make Available On-Site

   a. Please include a list of all penetration testing conducted by the firm or on behalf of the firm including a brief description of the tests and their frequency.

Make Available On-Site

   b. Please also provide a copy of the results of the most recent test, and briefly describe any significant findings and any remediation efforts undertaken in response to the results.

Provide in Advance

7. Provide a copy of any firm policies related to vulnerability scans.

Make Available On-Site

a. Please include a brief description of the types of scans and their frequency.

Make Available On-Site

b. Please also describe any significant findings and any remediation efforts undertaken in response to the results.

Provide in Advance

8. Provide a copy of firm policies and procedures for patch management, including procedures designed to ensure the prompt installation of critical patches. Also provide documentation (e.g., a sample log or report) evidencing patch maintenance tracking.

Access Rights and Controls

Make Available On-Site

9. Provide a copy of firm policies, procedures, and standards that are designed to ensure that unauthorized persons do not access firm network resources and devices or restrict user access according to job functions (e.g., access control policy, acceptable use policy, administrative management of systems, and corporate information security policy). Please clearly identify where each of the following topics is referenced:

Make Available On-Site

a. Establishing the access rights of each employee, including the employee's role or group membership.

Make Available On-Site

b. Updating access rights based on personnel or system changes (i.e., obtaining authorization to add, delete, or modify authorized user access to systems or applications); and

Make Available On-Site

c. Obtaining manager approval of changes to access rights or controls.

Provide in Advance

10. In reference to 9.a through 9.c, please also provide the following:

Provide in Advance

a. For establishing access rights: documentation evidencing the tracking of these access rights during the review period;

Provide in Advance

b. For updating access rights: (1) a list of the last ten employees to leave the firm during the review period and documentation evidencing their last date of employment and the date their access to the firm's systems was terminated and (2) a list of the last ten employees to be reassigned by the firm to a new group or function during the review period and documentation evidencing their date of reassignment and the date their access to the firm's systems was modified; and

Provide in Advance

c. For manager approval: sample documentation evidencing manager approval of access rights changes during the review period.

Make Available On-Site

11. Provide a list of the systems or applications for which the firm uses multi-factor authentication for employee and customer/client access.

Make Available On-Site

a. Please describe the multi-factor authentication components used and include any related documentation evidencing implementation.

Make Available On-Site

b. Please also describe any means or processes that allow users to bypass multi-factor authentication and provide a copy of related firm policies and procedures.

Make Available On-Site

c. Please also list the perimeter-facing systems or applications for which the

firm does not use multi-factor authentication.

Make Available On-Site

12. Provide a copy of firm policies, procedures, and standards related to login attempts, failures, lockouts, and unlocks or resets for each perimeter-facing system. Please indicate how these policies are enforced.

Make Available On-Site

13. Provide a list of all logs and reports that the firm uses to review perimeter-facing systems for failed log-in attempts, deactivation of access, dormant user accounts, and unauthorized log-in attempts during the review period. Please provide a description of each log or report and its frequency.

Provide in Advance

14. Provide a list of any instances during the review period where system users, including employees, customers, and vendors, received entitlements or access to firm data, systems, or reports in contravention of the firm's policies or practices and without authorization. Please include the date and a brief description of the instance and any remediation efforts undertaken in response.

Provide in Advance

15. Provide a copy of the firm procedures for notifying system users, including employees and customers/clients, of appropriate usage obligations when logging into the firm's system (e.g., log-on banners, warning messages, or acceptable use notifications). Please also provide related sample forms, screen shots, or documentation.

Provide in Advance

16. Provide a copy of firm policies, procedures, and standards regarding any devices used to access the firm's system externally (i.e., firm-issued and personal devices) including any written policies or procedures addressing the encryption of such devices and the firm's ability to remotely monitor, track, and deactivate remote devices.

Provide in Advance

17. Provide copies of the 25 most recent customer/client complaints received by the firm related to customer/client access. Please include a brief description of the resolution of the complaints and any remediation efforts undertaken in response.

Make Available On-Site

18. Provide a copy of firm policies, procedures, and standards related to verification of the authenticity of a customer/client request to transfer funds. If no such written policies, procedures, or standards exist, please describe the process the firm follows to verify the authenticity of fund transfer requests and describe the individuals and/or departments involved in the approval process.

Provide in Advance

19. If the firm conducts reviews of employee access rights and restrictions with respect to job-specific resources within the network, provide a list of reviews conducted during the review period and a brief description of each. If the firm maintains documentation related to these reviews, provide a copy of the most recent report for each type of review.

Provide in Advance

20. Provide the date of the last internal audit conducted by the firm that covered

access rights and controls, if any.

Make Available On-Site

a. Please describe the scope, process, and results of the audit, including any significant issues identified and any remediation efforts undertaken in response.

Data Loss Prevention

Provide in Advance

21. Provide a copy of firm policies and procedures related to enterprise data loss prevention.

Make Available On-Site

a. Provide a data map with owners identified as well as documentation evidencing the location of personally identifiable information ("PII").

Make Available On-Site

b. Provide a list of the systems, utilities, and tools used to prevent, detect, and monitor data loss as it relates to PII and access to customer/client accounts. 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.

Provide in Advance

22. Provide a copy of the firm policy relating to data classification. Please include a list of the types of data classification, the risk level (e.g., low, medium, or high) associated with each data classification, and a description of how the factors and risks are considered when determining whether data fits within each classification.

Make Available On-Site

23. Provide a copy of firm policies and procedures relating to monitoring exfiltration and unauthorized distribution of sensitive information outside of the firm through email, physical media, hard copy, web-based file transfer programs, or via other electronic means. If the firm maintains documentation of this monitoring, please include a copy of the most recent report.

Vendor Management

Provide in Advance

24. Provide a copy of firm policies, procedures, and standards relating to third-party vendors including, but not limited to, the following:

Provide in Advance

a. vetting and due diligence of vendors prior to selection;

Provide in Advance

b. vendor contracts, agreements, and the related approval process;

Provide in Advance

c. supervision, monitoring, tracking, and access control of vendors;

Provide in Advance

d. risk assessments conducted or required by the firm of vendors, including process and frequency; and

Provide in Advance

e. risk management and performance reports that vendors are required to provide the firm (e.g., internal and external audit reports and security reviews or certification reports).

Provide in Advance

If no written policies or procedures exist, please describe the firm's processes related to vendor selection, management, and oversight.

Make Available On-Site

25. 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.

Provide in Advance

a. Please provide a sample contract that illustrates the typical contractual terms related to accessing firm networks or data that are included in such vendor contracts.

Provide in Advance

26. Provide a list of all third-party vendors that facilitated the mitigation of cybersecurity risks by means related to access controls, data loss prevention, and management of PII during the review period and include a brief description of the services each vendor provided to the firm. Please also provide a sample contract that exemplifies the typical contractual terms included in vendor contracts involving cybersecurity-related services.

Provide in Advance

27. Provide a copy of any written contingency plans the firm has with its vendors in case of bankruptcy, the development of conflicts of interest, or other issues that might put the vendor out of business. If not documented, please describe any such contingency plans (e.g., software escrow).

Provide in Advance

28. Provide a sample of documentation or notification that the firm requires third-party vendors to provide prior to any significant changes to the third-party vendors' systems, components, or services that could potentially have security impacts to the firm and the firm's data containing PII.

Training

Provide in Advance

29. Provide a list of any training provided by the firm to its employees during the review period 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 participating employees for these training events and provide a copy of any written guidance or training materials provided.

Provide in Advance

30. Provide a list of any training provided by the firm to third-party vendors or business partners during the review period relating to information security.

Incident Response

Provide in Advance

31. 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 such a plan exists. If the firm maintains a separate written cybersecurity incident response policy, please provide a copy of the policy and indicate the date it was most recently updated.

Provide in Advance	32. Provide a copy of any firm policies for addressing responsibility for losses associated with attacks or intrusions impacting clients.
Provide in Advance	33. Describe the firm's process for conducting tests or exercises of its incident response plan, including the frequency of such testing, if applicable. If the firm prepares a report related to such testing, please provide a copy of the most recent report.
Make Available On-Site	34. Identify the 25 most recent system-generated alerts within the review period related to data loss of sensitive information or confidential customer/client records and information. Please identify whether those alerts became incidents requiring further action and, if so, briefly describe the incidents and any remediation efforts undertaken in response.
Provide in Advance	35. Provide a list of all incidents of unauthorized distributions of PII that occurred during the review period. Please provide a brief description of each incident, including the time of occurrence and time of discovery, and a description of any remediation efforts undertaken in response.
Provide in Advance	36. Provide a list of any successful unauthorized external incidents related to access controls that occurred during the review period. Please note when unauthorized access first occurred, when it was identified by the firm, and when it was corrected. Please also briefly describe escalation or remediation efforts undertaken in response.
Provide in Advance	37. Identify the amount of actual customer losses associated with cyber incidents, as well as:
Provide in Advance	a. the amount of customer losses reimbursed by the firm;
Provide in Advance	b. whether the firm had cybersecurity insurance coverage;
Provide in Advance	c. whether any insurance claims related to cyber events were filed; and
Provide in Advance	d. the amount of cyber-related losses recovered pursuant to the firm's cybersecurity insurance coverage.