Category	Request	Gaps Identified?	Responsible Party	Summary of Updates Needed
Annual Review of Cybersecurity and Safeguarding Policies and Procedures	Any reports and documentation generated during the Examination Period to evidence any reviews or testing of the Adviser's compliance with its cybersecurity and safeguarding policies and procedures, or the effectiveness of such policies and procedures, performed pursuant to Rule 206(4)-7 of the Advisers Act.			
Compliance Exceptions	A record of any non-compliance with the Adviser's cybersecurity or safeguarding policies and procedures during the Examination Period and any action taken as a result of such non-compliance, including but not limited to non-compliance with policies on access rights. Please include the date and a brief description of the instance and any remediation efforts undertaken in response.			
Compliance Policies and Procedures	All written compliance and operational policies and procedures, and the code of ethics in effect during the Examination Period. If any material amendment was made to these policies and procedures during the Examination Period that relate to cybersecurity or safeguarding client NPI, please describe the amendment and when it became effective.			
Cybersecurity Oversight	Organizational charts that illustrate the positions and departments responsible for cybersecurity-related matters and where these individuals and departments fit within the Adviser's organization or hierarchy. Identify the Chief Information Security Officer or equivalent position. If the role does not exist, explain where the principal responsibility for overseeing cybersecurity resides within the Adviser.			
Electronic Signatures	Please provide all electronic/digital client signature procedures, controls, any annual compliance review and testing.			
Governance and Risk Management	Provide a list and description of any automated systems or tools used to carry out compliance-related oversight functions and/or reporting obligations.			

Governance and Risk Management	Provide a copy of Registrant's privacy notice provided to clients during the Review Period and any supporting documentation evidencing the delivery of such notice to clients.			
Governance and Risk Management	Provide a record of any non-compliance by any employee, contractor/vendor, or other third party with the Registrant's policies and procedures as it relates to all applicable federal securities laws or cybersecurity policies and procedures during the Review Period and any action taken because of such non-compliance.			
Governance and Risk Management	Provide policies and procedures addressing the administrative, technical, and physical safeguards for the protection of customer/client records and information (including those that are designed to secure customer/client information, protect against anticipated threats to customer/client information, and protect against unauthorized access to customer/client accounts or information and address the storage and transmission of client non-public information ("NPI")).			
Governance and Risk Management	For Registrant's branch offices, provide: a. Policies, procedures, and guidance provided to branch offices covering information technology, cybersecurity, and client data governance; b. A list of the subject areas and frequency of branch office reviews;c. Reports from any branch office reviews performed within the Review Period; d. Any corrective actions taken in response to the branch office reviews within the Review Period.			
Governance and Risk Management	Provide a list identifying the name, function, purpose, and address of all corporate offices, data centers, cloud provider data centers that process or store customers' data, internet points of presence, and co-location services.			
Governance and Risk Management	Provide the Registrant's policies and procedures regarding risk assessment, management and operational risk.			
Governance and Risk Management	Provide Documentation of any risk assessments related to technology/cybersecurity risks, controls, threats, vulnerabilities, and potential business consequences of cybersecurity threats or vulnerabilities, and any technology risk			

	assessment schedule/plan and Risk Control Self-Assessment ("RCSA").			
Governance and Risk Management	Provide network diagrams that describe systems and data flows within the firm's network (if any), including any depictions of covered major networks, any specific IP addressing schemes, and the general network topology (including network connections, interdependencies, and access granted to third parties or managed service providers ("MSPs")). There is no need to create documentation solely to satisfy this request.			
Off-Channel Communication	Controls and surveillance for "off-channel communications" (ex. messaging services used, "apps", personal device use, etc.), and of which that under securities law and may be required to be recorded.			
Electronic Communications	Please explain the steps taken by the Adviser to monitor, review, and retain electronic Communications related to the Adviser's business. Electronic Communications include, but are not limited to, email, text messages, messaging apps, instant messages, Bloomberg messaging, and private messaging on social media sites. Please address the following: (1) whether Supervised Persons are permitted to use personal devices for firm business or are permitted to use any form of electronic Communication other than Adviser email accounts for business purposes; (2) if so, what steps the Adviser takes to approve the use of such personal devices or additional means of electronic Communications; and (3) what steps the Adviser takes to ensure that Supervised Persons only use approved means of electronic Communications to conduct firm-related business. Please also explain the Adviser's policies on use of Dropbox, Google Drive, and other forms of cloud storage by Supervised Persons.			

Access Rights and Controls	For each Registrant system, provide a list that identifies the authentication method(s) and the configuration of the authentication method, including: a. User ID and Password authentication;b. Multi-factor authentication; c. Single Sign-On authentication; d. Certificate-based authentication; and/or e. Biometric authentication.			
Access Rights and Controls	For each user granted access to the Registrant's network or any system used by the Registrant during the Review Period, provide evidence of the authorization of user access.			
Access Rights and Controls	Provide a copy of any policies and procedures that address the following with respect to user access to the Registrant's network and any systems: a. User account provisioning; b. User account de-provisioning; c. User account authorization; d. User account re-certifications; e. User account monitoring; f. User accounts provisioned to vendors; and g. The granting and handling of any exceptions to the Registrant's policies and procedures.			
Access Rights and Controls	Provide a copy of any policies and procedures that address the Registrant's review of user access.			
Updates to Access Rights	A list of the last ten changes to or terminations of access rights applied to Supervised Persons or Vendor representatives, including: a. Name of the Supervised Person or Vendor and its representative; b. The date the Supervised Person's or Vendor representative's access was changed; c. How the access rights were changed (e.g. terminated, expanded to include…, reduced to exclude…); d. Reason for the change; and			

	e. If applicable, the date the Supervised Person's or Vendor representative's role was changed or terminated with the firm.			
Vulnerability Management	Provide a list of any remediation performed during the Review Period on systems and applications, including installed patches, service packs, hot fixes, and other software updates to correct information system flaws.			
Service Providers	Provide the names and location of all service providers/vendors/outside contractors and the services they perform (both affiliated and unaffiliated providers) including information regarding due diligence processes by Registrant to evaluate and monitor (including terms and conditions, privacy, confidentiality, cybersecurity, potential conflicts, and designation of responsibilities) thereafter the services provided, data integrity testing, and date of most recent due diligence for each vendor. *Please identify as affiliated or unaffiliated (i.e. identify whether the service provider is affiliated with the Adviser or any officer, director, portfolio manager/adviser, or trader), and note the date of execution of the agreement and termination date (if applicable). Please be prepared to provide copies of most recent executed agreements.			
Cybersecurity	Please list any network providers, cybersecurity vendors, or cybersecurity consultants and date engaged. a. Cyber vendor due diligence: the selection, assessment, and suitability of a vendor based on the data and services the vendor will provide; b. Indicate if Registrant is contemplating changing network			

	providers, cybersecurity vendors, or cybersecurity consultants. If so, what are the reasons?			
Cybersecurity Procedures	Please provide procedures describing how Registrant manages cybersecurity preparedness in the following areas: (1) governance and risk management; (2) access rights and controls; (3) data loss prevention; (4) vendor management; (5) training; and (6) incident response.			
Cybersecurity Measures:	Please describe all cybersecurity measures implemented and tested by Registrant (including but not limited to, risk assessments, penetration testing, account takeover, vulnerability scans, incident response plans, etc.) and persons responsible for testing, and frequency of testing. Inclusive ofall branch offices, home offices, as needed/ad hoc office suites, and/or other satellite locations. A. Please provide any notification procedures, and as may be related to all parties who may be impacted by breaches; B. Please list and detail all hacks and cyber intrusions, including but not limited to any events that result in identity theft, fraud, or economic loss, and any subsequentnotifications; C. Any vendor cybersecurity due diligence- any vendor attestations and/or the results of cybersecurity testing.			

Areas of Cybersecurity and Safeguarding of NPI Addressed by the Adviser.	Please indicate, yes or no, whether the Adviser's policies and procedures address each of the areas listed below, and reference relevant sections of the Adviser's policies and procedures. For each of these areas that you indicate is not addressed in the Adviser's policies and procedures, indicate whether the area is not applicable or low-risk, and provide the basis for this determination; or whether you have plans to develop policies and procedures in the area, and the timeline for such plans.a. Regulation S-ID (if applicable) for addressing the risk of client identity theft;b. Training on cybersecurity and safeguarding of client NPI for Supervised Persons;c. Penetration testing and vulnerability scans;d. System and software patch management;e. Verification of the authenticity of a client request to transfer funds;f. Data loss prevention, including, monitoring of removable storage devices, and personal devices used by Supervised Persons for business purposes;g. Monitoring exfiltration and unauthorized distribution of client NPI outside of the Adviser through email, physical media, hard copy, web-based file transfer programs, or via other electronic means;h. Password requirements for Supervised Persons, including complexity, and changefrequency;i. Electronic transmission of client NPI to or from the Adviser or its Supervised Persons;j. Management of network and information access rights to 1) prevent unauthorized persons from accessing network resources and devices, 2) control access to information based on the need for the information to carry out role or job functions, and 3) timely revise access rights in the event of changes in employment status or job functions;k. Standards related to login attempts, failures, lockouts, and unlocks or resets;l. Standards regarding any remote devices (i.e., Adviser-issued and personal devices) used to access the Adviser's system externally, including any encryption of such devices and the Adviser's ability to remotely monitor, track, and deactivate these devices;m. Detection and mitigating responses to cybersecurity incidents, including actions that will			

	be taken to prevent further harm, address the vulnerability that led to the incident, communicate the incident to affected clients, and address and determine responsibility for any associated losses impacting clients, and any testing that will be conducted of this incident response plan; andn. Oversight and due diligence on the cybersecurity policies and procedures of serviceproviders that are given, or have access to, client NPI through the Adviser.			

Cybersecurity Breaches	Information on any actual or suspected breaches of the firm's data that led to, or may have led to loss, exfiltration, or unauthorized access to client NPI, including for each incident:a. Date of occurrence;b. Date the Adviser identified or was notified of the incident;c. Type of incident (i.e. ransomware, business email compromise, loss of device, Vendor,unauthorized distribution of client information, etc.);d. Brief description of incident;e. Whether the incident involved loss of client information;f. Whether the incident involved loss of client funds;g. Whether any impacted clients were notified of the incident;h. Status of incident (resolved or unresolved);i. Description of any remediation efforts taken;j. Description of any remediation efforts in process; andk. If the incident involved loss of client funds,i. The amount of actual client lossesii. The amount of client losses reimbursed by the Adviser;iii. Whether the Adviser had cybersecurity insurance coverage;iv. Whether any insurance claims related to cyber events were filed; andv. The amount of cyber-related losses recovered pursuant to the Adviser's cybersecurityinsurance coverage.			
Notice of Breaches	A copy of any communications (e.g., e-mails, letters, etc.) from the Adviser to clients/investors or other stakeholders concerning any suspected/actual breaches.			
Vendor Management	Provide a copy of any policies and procedures that address the selection, onboarding, governing, monitoring, tracking, supervision, and off-boarding of vendors, including both outsourcing and subcontracting agreements.			
Vendor Management	Provide a copy of any policies and procedures for assessing vendor information security (e.g., SOC 2 and SSAE 18).			
Vendor Management	For each vendor with access to customer records and information, provide a copy of the executed service level			

	agreement, operational level agreement, and/or master services agreement.			
Vendor Management	Provide evidence of any initial or ongoing risk assessment, monitoring, and due diligence performed to determine compliance with any agreement between the vendor and the Registrant.			
Vendor Management	Provide a list of events where the Registrant identified that a vendor did not fulfill the terms of the agreements with the Registrant. Provide a brief description of each event.			
Vendor Management	Please provide a list of vendors, including, but not limited to, information technology consultants, cloud-computing providers, managed service providers, and compliance consultants.			
Vendor Management	Firm practices and controls related to vendor management, including: (1) due diligence regarding vendor selection, monitoring and oversight of vendors, and contract terms; (2) assessing how vendor relationships are considered as part of the firm's ongoing risk assessment process, including how the firm determines the appropriate level of due diligence to conduct on a vendor; and (3) assessing how the firm ensures vendors protect client Non-Public Information that vendors may access or store.a. If Registrant changed vendors during the exam period, or is contemplating changing any vendors please provide reason(s) why.			
Vendors	A list of all Vendors a) with access to the Adviser's network, systems, or data, and/or b) that are a web or cloud based service provider or a cybersecurity-related Vendor. For each Vendor listed, please include a brief description of the service (or type of service) the Vendor provides to the Adviser, whether the Adviser has access to client NPI, and whether the Adviser has an executed contract in place with the Vendor that addresses the Vendor's cybersecurity and safeguarding practices.			

AI Disclosures and Marketing	All disclosure and marketing documents to clients where the use of AI by the Adviser is stated or referred to specifically in the disclosure. Include all audio and video marketing in which the Adviser's use of AI is mentioned.			
AI: Description of AI Models and Techniques	A written description of all distinct artificial intelligence based artificial intelligence models and artificial intelligence techniques developed and implemented by the Registrant to manage client portfolios or make investment decisions and transactions since inception.			
AI: List of Algorithmic Trading Signals and Associated Models	List and description of all algorithmic trading signals generated by AI models during the Examination Period. For each signal, please list input data sources along with their vendor or, if generated in-house, method of acquisition as well as primary data inputs.			
AI: Data Sources	List of all data sources utilized by artificial intelligence systems including: a. item name; b. description; c. source; d. manner of acquisition; and e. related trading or other strategy.			
AI: Data Source Providers	List of contracted data source providers utilized by Registrant during the examination period, list of the “in-house” alternative data sources, and description of how each are obtained and maintained (e.g. web scraping).			
AI: Compliance Policies and Procedures	All written compliance and operational policies and procedures concerning the supervision of all artificial intelligence systems utilized by the Registrant. If any material amendment was made to these policies and procedures during the Examination Period, please describe the amendment and when it became effective.			
AI: Conflict of Interest Policies	Documents outlining how potential conflicts of interest related to AI outputs are managed.			

AI: Contingency Plans	Documents detailing contingency plans in case of AI system failures or inaccuracies.			
AI: Client Profile Documents	Sample client profile documents used by the AI system to understand each client's risk tolerance and investment objectives.			
AI: Data Security	Documentation on data security measures when using AI.			
AI: Performance Evaluation Reports	Reports on the AI models' performance over time and under various market conditions.			
AI: Incident Reports	Reports on any incidents where AI use raised any regulatory, ethical, or legal issues.			
AI: Compliance Training	Written guidance the Adviser provided to its Employees regarding the compliance program and documents evidencing Employee compliance training during the Examination Period specifically addressing AI.			
Data Loss Prevention	Provide a copy of Registrant's policies and procedures relating to data classification. Please include a list of the types of data classification, including classification of non-public client/customer information, the risk level (e.g., low, medium, or high) associated with each data classification, and a description of how risks are considered when determining security controls addressing each data classification.			
Data Loss Prevention	Provide the Registrant's policies and procedures addressing data encryption "in motion" both internally and externally and data "at rest" on all and servers including both on-premise and off-premise.			
Data Loss Prevention	Provide a list of the systems, utilities, and tools used to prevent, detect, and monitor data loss, including supporting documentation that describes their functions, managed by a third party, or commercial off-the-shelf products. For each of the systems, please provide the types of information monitored and the configuration for identifying the information.			

Data Loss Prevention	Provide a list of the controls in place to facilitate the protection of client data. Include details covering Media Protection, Media Disposal, Monitoring of data transmissions, Active Directory controls, etc.			
Data Loss Prevention	Provide an inventory of physical devices (including mobile devices) and systems.			
Data Loss Prevention	Provide an inventory of software platforms and applications (installed either on devices or in the cloud) used by the Registrant, including software name, version, devices on which the software is installed, and last patch date.			
Data Loss Prevention	Provide any incident response tickets related to data loss/leakage during the Review Period.			
This tool is provided by Fairview Cyber for informational purposes only.				