Capstone RIA

Privacy Policy and Procedures for Protecting Client Information
February 2025

STATEMENT OF POLICY

The Firm is committed to protecting the confidentiality and security of consumer, customer, and former customer information that it collects and will disclose such information only in accordance with Regulation S-P, any other applicable law, rules and regulations, and this Privacy Policy.

I. Background

Regulation S-P limits the circumstances under which an adviser may disclose nonpublic personal information about a client to other persons and requires an adviser to disclose to all its clients its privacy policies. The Firm has implemented the following Privacy Policy ("Privacy Policy") and Program for Protecting Client Information (the "Program") to comply with Regulation S-P.

II. Summary of Regulation S-P

Regulation S-P has four key features:

- An adviser must provide notice to its clients about its privacy policies;
- An adviser may only disclose nonpublic personal information about clients to a nonaffiliated third party if it provides an initial privacy notice and a notice giving the client the opportunity to "opt-out" from the Firm's disclosure of the information;
- A client may request that their nonpublic personal information not be disclosed to nonaffiliated third parties (although certain information required for processing transactions is still permitted to be disclosed); and
- An adviser must adopt a program reasonably designed to (i) ensure the security and confidentiality of client records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of client records and information; and (iii) protect against unauthorized access to or use of client records or information that could result in substantial harm or inconvenience to any client.

III. Privacy Policy Scope

The Firm has adopted this Privacy Policy. Capstone RIA conducts its business affairs primarily through its employees, to whom this Privacy Policy applies. To the extent that service providers are utilized in servicing accounts, confidentiality agreements that comply with Regulation S-P will be put into place.

Service Providers

The Firm will obtain a representation from each service provider that the service provider will not disclose client and former client information other than to carry out the purposes for which the client and former client information was provided to the service provider. The Firm will seek to obtain this representation from all third-party service providers in the contract for services. To the extent the Firm has not previously obtained this representation from the service provider in the contract for services, the Firm will seek to obtain such representation in substantially the form as set forth in Attachment A.

Privacy Notices

Under Regulation S-P, the Firm must provide an initial privacy notice to its customers at the time the

advisory relationship is established and annually thereafter and provide an initial privacy notice to its "consumers" before it discloses nonpublic personal information.

Consumers. A "consumer" is an individual who obtains from an adviser, financial products that are to be used primarily for personal, family or household purposes, such as one-time investment advice. The Firm must provide an initial privacy notice to its consumers before the Firm discloses the consumers' nonpublic personal information to a nonaffiliated third party (other than as necessary to process consumer transactions). The Firm is not required to send a privacy notice to consumers if the Firm discloses nonpublic information about its consumers to third parties only pursuant to certain exceptions. The Firm may satisfy the initial notice requirement by sending a "short form" notice that explains how the consumer may obtain the Firm's privacy notice.

Customers. A "customer" is a consumer who uses the product or service of the Firm on an on-going basis (such as receiving continuous investment advice). The Firm must provide an initial privacy notice when it establishes the customer relationship (such as when an investor enters into an advisory contract) and annually thereafter.

Content of Customer Privacy Notices

The initial and annual privacy notices must contain the following information:

- categories of nonpublic personal information collected by the Firm;
- categories of nonpublic personal information disclosed by the Firm;
- categories of affiliates and nonaffiliates to whom the Firm discloses the nonpublic personal information;
- categories of nonpublic personal information about former customers disclosed by the Firm and the categories of affiliates and nonaffiliates to whom it is disclosed;
- if nonpublic personal information is disclosed to third parties, an explanation of the right to "opt-out" of such disclosure; and
- A general description of the Firm's policies and practices with respect to protecting the confidentiality and security of nonpublic personal information.

The initial privacy notice will be delivered with Part 2 of Capstone RIA's Form ADV, the investment advisory agreement for separate accounts or subscription agreement for private investment vehicle investors that is given to customers at the start of the advisory or investment relationship. The annual notice will be electronically delivered to each customer, generally accompanying the annual Part 2 delivery requirements. The Chief Compliance Officer or the delegee will review and update the privacy notice at least annually.

Opt-Out Notice

If the Firm plans to disclose nonpublic personal information (other than pursuant to certain exceptions), it will provide consumers and customers a reasonable means to "opt-out" of the disclosure of that information, in compliance with Regulation S-P. Once a consumer elects to opt-out, the Firm must honor the election as soon as reasonably practicable. The opt-out election remains in effect until the consumer revokes it.

Document Destruction Policy

The Firm is required to take reasonable measures to guard against access to information derived from credit

reports or other customer information when disposing of it, such as shredding such information, entering into a contract with a company that is in the business of disposing of consumer information in a manner consistent with Regulation S-P, destroying or erasing electronic documents that contain consumer information, and monitoring employee compliance with disposal and destruction procedures.

IV. Administration of Privacy Policy Designation of Responsibility

The Chief Compliance Officer or the delegee shall be responsible for implementing this Privacy Policy and all questions regarding this Policy should be directed to the Chief Compliance Officer or the delegee.

Amendment of the Privacy Policy

The Privacy Policy may be amended only by action of the Chief Compliance Officer or the delegee.

Non-Compliance

An employee will report to the Chief Compliance Officer or the delegee any material breach of this Privacy Policy of which the employee has become aware. Upon being informed of any such breach, the Chief Compliance Officer or the delegee is authorized to take any such action they deem necessary or appropriate to enforce this Privacy Policy and otherwise comply with Regulation S-P.

V. Program for Protecting Customer Information

The Chief Compliance Officer or the delegee are responsible for implementing and maintaining the Program.

Identifying Internal and External Risks

The Program is designed to identify foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such customer information. An assessment and evaluation will be made of the likelihood, and potential damage of these threats, the sufficiency of any safeguards in place to control such risks and, where appropriate, the Program will be revised to address such risks (the "Risk Assessment"). At a minimum, the Risk Assessment will include a consideration of the risks in each of the Firm's areas of operation, including:

- Employee training and management, including instructing and periodically reminding employees of the Firm's legal requirement and policy to keep customer information secure and confidential;
- Information systems, including network and software design, as well as information processing, storage, transmission, retrieval, and disposal; and
- Detecting, preventing, and responding to attacks, intrusions, or other system failures.

Design and Implementation of Safeguards

Information safeguards will be designed and implemented to control the risks identified through the Risk Assessment, and the effectiveness of the safeguards' key controls, systems and procedures will be regularly tested or otherwise monitored.

Overseeing Service Providers

Reasonable steps will be taken to determine that the service providers[1] who have been selected and retained

by the Firm, at a minimum, maintain sufficient customer information safeguard procedures to detect and respond to security breaches. Moreover, reasonable procedures will be implemented to discover and respond to widely known security failures by service providers. Finally, all contracts with service providers must contain assurances that such service providers have implemented and will maintain such safeguards.

Evaluation and Maintenance of the Program

The Program will be periodically adjusted, as necessary or appropriate, based on: (i) results of testing and monitoring pursuant to the Program; (ii) any material changes to the business and operation of the Firm; and (iii) any other circumstances that may have a material impact on the Firm's Program.