Montgomery Financial Planning LLC

Privacy and Protection of Client Information

We view the protection of our clients' private information as a top priority, and we have instituted policies and procedures to ensure that client information is kept private and secure. All Supervised Persons have a duty to protect the confidential information of our clients. We maintain safeguards to comply with federal and state standards to guard each client's non-public personal information. We do not share any non-public personal information with any nonaffiliated third-parties, except in the following circumstances:

As necessary to provide a service that the client has requested or authorized, including third-party service providers such as software or web application providers;

To a client's trusted contact, agent, or professional service provider (such as an attorney or accountant), upon written authorization by the client;

As required by regulatory authorities or law enforcement officials who have jurisdiction over our firm or as otherwise required by any applicable law;

To our authorized Agent to carry out our Business Succession Plan; and

To our attorneys, accountants, auditors, or other professional consultants, as necessary to determine compliance with industry standards.

We have adopted a Privacy Policy, which is delivered to each client at the beginning of the client relationship and on at least an annual basis thereafter. If changes are made to the policy, the updated Privacy Policy must be delivered within 30 days. This Privacy Policy outlines how we share client information and whether the client is able to limit our sharing.

Supervised Persons are prohibited, both during and after termination of their relationship with our firm, from disclosing client non-public personal information to any person or entity outside of our firm, including a client's family members, except under the circumstances described above.

Retention and Disposal of Client Information

When a client's non-public personal information is retained in our records, either in paper documents or electronically, such records will be kept in a secure location not accessible to unauthorized persons. Any conversations involving a client's non-public personal information, if appropriate at all, must be conducted by Supervised Persons in private and care must be taken to avoid unauthorized persons from overhearing or intercepting such conversations. When records containing non-public personal information are no longer required to be retained by our firm, they will be disposed of securely (for example, paper documents will be shredded and electronic records will be securely erased or otherwise destroyed).

Third-Party Service Providers

Before sharing clients' non-public personal information with a third-party service, we will conduct a due diligence review of the third-party's policies and procedures designed to protect against unauthorized access to or use of client information. (See also Due Diligence of Service Providers in this Compliance Manual.) The third-party's policies must include a requirement to notify us of any unauthorized access to or use of client information as soon as possible, but no later than 72 hours after becoming aware of such breach.

Incident Response

We have adopted a policy regarding Security Incident Handling Procedures in our Cybersecurity Policy. In the event of unauthorized access to or use of client information, whether through a cybersecurity breach or otherwise, the following additional steps will be taken:

We will take immediate steps to terminate or mitigate such unauthorized access or use.

We will notify clients whose non-public information was, or is reasonably likely to have been, accessed or used without authorization, unless such access or use is not reasonably likely to have been used in a manner that would result in substantial harm or inconvenience. Notices must include information regarding the incident, such as the data affected, how individuals can respond to protect themselves, and any other key facts. If appropriate, we will offer to provide credit monitoring services to the client. Notices must be provided as soon as possible, but no later than 30 days after we become aware of such unauthorized use or access.