Privacy Policy & Information Security

Under Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information ("Regulation S-P"), privacy rules promulgated pursuant to Section 504 of the Gramm-Leach-Bliley Act, an investment adviser is:

- prohibited from disclosing, except for certain specified exceptions, nonpublic personal information about its customers and consumers[1] without their consent (an institution may rely on the negative consent of the individual if it has provided an adequate means for the individual to "opt out" of, or decline, disclosure);
- required to deliver a statement describing its privacy policy to its customers on an initial and annual basis; and
- required to adopt policies and procedures to protect the nonpublic personal information of its consumers and customers.

Regulation S-P applies only to information obtained by financial institutions from individuals. Business and institutional clients of investment advisers are not covered by the regulation. In order to comply, an investment adviser must do the following:

- prepare notices describing its privacy policy;
- provide an initial privacy policy notice to each existing customer;
- provide an initial privacy policy notice to each new customer who did not receive a notice when he/she was a consumer (and thereafter provide an annual privacy policy notice to each customer), if necessary;[2]
- provide a means for a customer to "opt out" of information sharing if the institution intends to share nonpublic personal information other than in accordance with the permitted exceptions;

[1] Under Regulation S-P, "consumer" means an individual who obtains or who has obtained a financial product or service from an investment adviser or other applicable entity that is to be used primarily for personal, family, or household purposes, or that individual's legal representative and "customer" means a consumer that has established a continuing relationship with an investment adviser or other applicable entity. A investment adviser is not obligated to provide any disclosures to its consumers who are not customers unless it determines to disclose nonpublic personal information about that consumer to a nonaffiliated third party.

[2] In December 2015, Section 503 of the Gramm-Leach-Bliley Act and effectively Regulation S-P was amended to provide an exception to the annual notice requirement. A financial institution, including registered investment advisers, that (1) only provides nonpublic personal information in accordance with permitted use as described in Section 502(b)(2) or (e) or 504(b); and (2) has not changed its policies and practices with regard to the use of nonpublic personal information since its most recent disclosure delivered to consumers shall not be required to deliver another annual notice until such time as it no longer meets these noted provisions.

- provide a privacy policy notice and "opt out" notice to each consumer if the institution intends to share information about the consumer other than in accordance with the permitted exceptions;
- adopt policies and procedures that address the confidentiality and security of nonpublic personal customer and consumer; and
- ensure appropriate coverage of customer privacy and information security in annual employee training.

The privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed once annually. The CCO will document the date the PPS was mailed to each client for each year. AWA collects nonpublic personal information about you from the following sources:

- Information we receive from you on applications or other forms;
- Information about your transactions with us or others; and
- Information we receive from a consumer reporting agency.

We do not disclose any nonpublic personal information about you to anyone, except as permitted by law. If you decide to close your account(s) or become an inactive customer, we will adhere to the privacy policies and practices as described in this notice.

AWA restricts access to your personal and account information to those employees who need to know that information to provide products or services to you. AWA maintains physical, electronic, and procedural safeguards to guard your nonpublic personal information.

The following employees will manage nonpublic information: Edward Papier
The following individuals also have access to this nonpublic information: Edward Papier
The following systems may be vulnerable to a breach of your nonpublic information: Edward Papier

AWA personnel must make every effort to help ensure that reasonable steps are taken to protect against unauthorized access to client information. Adequate measures must be observed not only throughout the business day but also outside business hours in order to ensure that client data remains secure. Supervised Persons will adhere to the following procedures to safeguard the privacy of such information:

Limit Sharing of Information

- Adviser restricts access to a Client's non-public information to those employees who need to know that information to provide products or services to the Client.
- Use of personally owned mobile devices is prohibited without approval and the installation by the Firm of software on the device that allows Firm information to be segregated from personal information and Firm data to be removed by remote instruction.
- No nonpublic information will be given to any non-affiliated third parties except:
    - With the express written consent of, or instruction form the respective Client;
    - To service providers utilized to provide services to Adviser's Clients; and
    - To other entities as required or permitted by law.

- The information shared will be limited to that information necessary for the non-affiliated third-party to perform its services or as outlined in the written instruction received from the Client.
- Agreements between Adviser and third-party service providers must contain clauses that strictly limit the provider's use of any nonpublic information it obtains or has access to while providing services to Adviser or its Clients and for the reasonable safeguard of that information. When the agreements do not contain such clauses, Adviser will collect a confidentiality/non- disclosure agreement from the third-party provider.

Physical Safeguards

- Printed information (if any) for individual Clients (copies of account applications, advisory contracts, etc.) will be filed in appropriately designated folders, which are kept in a secured filing area that will remained locked when not in use.
- Supervised Persons must adopt a "clean desk policy" for any files they are working on. Supervised Persons must ensure that client files are either returned to the secured filing area or stored in a locked desk drawer or cabinet overnight.
- The doors to the Adviser's offices will be kept locked when the office is not in use. Keys and or access shall only be provided to those persons with a need for access.
- Adviser shreds discarded Client nonpublic information.
- Generally, Client files are not removed from Adviser's premises. On occasion, when it is necessary to temporarily remove files from the premises (e.g., files taken home overnight), proper care will be observed in the transport and storage of such information.

To mitigate a possible breach of the private information AWA will encrypt all data that individuals have access to or use password sensitive documents. The system will be tested and monitored at least annually.

AWA has taken extensive measures to safeguard the privacy and integrity of the information that it gathers, stores, and archives during its normal business practices. Computer security measures have been instituted where applicable including passwords, backups, and encryption. All employees are informed and instructed on various security measures including the non-discussion and/or sharing of client information, always removing client files from desktops or working areas that cannot be locked or secured, and proper storage of client securities files in locked files or other secured location. AWA uses various methods to store and archive client files and other information. All third party services or contractors used have been made aware of the importance AWA places on both firm and client information security. In addition to electronic and personnel measures AWA has implemented reasonable physical security measures at our home office location, and encouraged all remote locations, if any, to do the same to prevent unauthorized access to our facilities.

AWA will retain records for at least 5 years from the end of the fiscal year in which it was last used or updated, or as otherwise required by applicable state or federal law. With respect to disposal of nonpublic personal information, AWA will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.