Privacy of Client Information

Information Collected and Shared

CAP's privacy policy statement is given to clients at the initial signing of the client contract and mailed or emailed with client consent once annually, if the policy is updated. The CCO will document the date the privacy policy was delivered to each client for each year if an annual delivery is required. CAP may collect information about clients from the following sources:

- Information received from client on applications, via other forms, or during conversations;
- Information about client's transactions with CAP or others; and
- Information provided by a consumer reporting agency.

Below are the reasons for which CAP may share a client's personal information:

- With specific third parties as requested by the client (see Sample 12);
- For everyday business purposes – such as to process client transactions, maintain client account(s), respond to court orders and legal investigations, or report to credit bureaus;
- For marketing by CAP – to offer CAP's products and services to clients;
- For joint marketing with other financial companies;
- For affiliates' everyday business purposes – information about client transactions and experience; or
- For non-affiliates to market to clients (only where allowed).

If a client decides to close his or her account(s) or becomes an inactive customer, CAP will adhere to the privacy policies and practices as described in this manual, as updated.

Storing Client Information

CAP uses various methods to store and archive client files and other information. Third party services or contractors used have been made aware of the importance CAP places on both firm and client information security. CAP also restricts access to clients' personal and account information to those employees who need to know that information to provide products or services to its clients. In addition to electronic protection, procedural safeguards, and personnel measures, CAP has implemented reasonable physical security measures at its home office location, and requires remote locations to do the same to prevent unauthorized access to its facilities

The names of CAP's current and former access persons can be found in Exhibit 2.

In addition to CAP's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An on-site or off-site server that stores client information, third-party software that generates

statements or performance reports, or third-party client portals designed to store client files all hold the potential for a breach of non-public client information.

To mitigate a possible breach of the private information, CAP uses encryption software on all computers and carefully evaluates any third-party providers, employees, and consultants with regard to their security protocols, privacy policies, and/or security and privacy training.

Identity Theft Red Flags

The CFTC (U.S. Commodity Futures Trading Commission), SEC (U.S. Securities and Exchange Commission), and many state regulators, have published rules concerning identity theft encouraging or requiring investment advisers to train firm personnel to recognize "red flags" regarding possible identity theft of advisory clients. While many of these provisions may also be covered in the firm's broader privacy and AML (anti-money laundering) policies, the list below is a brief non-exhaustive listing of the items and information that all CAP personnel should monitor and safeguard to guard against any breach of a client's identity:

SAFEGUARDING IDENTIFYING INFORMATION

- Individual client's social security numbers
- Corporate or other entity client's tax identification numbers
- Individual driver's license number or other personal identification card
- Passport numbers
- Financial account numbers (credit card, bank, investment, etc.) and any accompanying passwords or access codes

POTENTIAL CAUSES OF IDENTITY INFORMATION BREACHES

- Loss of theft of computers and/or other equipment
- Hacking of computer networks
- Inadvertent exposure of client information to unauthorized individuals (non-locked files, files left on desk, cleaning services, shredding services, etc.)
- Physical break-ins / theft

CAP personnel are instructed to notify the firm if they detect or have reason to believe that any of the above shown red flag activities may have occurred or if any of the red flag information listed may have been stolen or leaked by any firm personnel. The CCO, CISO, or principal is then tasked with investigating the report and taking appropriate actions. The non-exhaustive list of possible follow-up actions includes notification of the parties involved, notification of appropriate regulatory officials if required, taking remedial actions to assist in the recovery of the stolen information, and possible sanctions of firm personnel if deemed necessary.

Staff Training

On an annual basis, CAP will conduct a firm-wide training session to ensure that staff members are properly trained and equipped to implement the above policies regarding client privacy. New staff members will receive training, led by the CCO, within one (1) month of their initial hire date.

Client Records

Client records will be retained by CAP for at least 5 years after the year in which the record was produced, or as otherwise required by law. With respect to disposal of non-public personal information, CAP will take reasonable measures to protect against unauthorized access to or use of such information in connection with its disposal.

CAP takes the privacy and confidentiality of all its clients and personnel very seriously. It will continue to make, and document, any changes needed to promote the security of client information.