Compliance Policies & Procedures Manual

for

Burgess Chambers & Associates Inc

December 10, 2021

This Compliance Manual must be returned to the Company immediately upon termination of employment. The information contained herein is confidential to the Company and proprietary to Foreside Financial Group ("Foreside") and may not be disclosed to any third party (other than applicable regulatory authorities) or otherwise shared or disseminated in any way without the prior written approval of the Company and Foreside.

Table of Contents

Introduction

Purpose

Burgess Chambers & Associates Inc has adopted the following policies and procedures ("Compliance Manual" or "Manual") for compliance as a registered investment adviser under the Investment Advisers Act of 1940, as amended ("Advisers Act"). All Associated Persons of the Company, including all owners and executive officers, are expected to be familiar with and to follow the Company's policies. Associated Persons may also include temporary workers, consultants, independent contractors, and anyone else designated by the Chief Compliance Officer ("CCO").

This Compliance Manual, as of the date of its adoption above, supersedes all previously dated versions of the Company's Compliance Manual to the extent such policies and procedures are contained herein, unless expressly stated otherwise. The Manual should accurately reflect the Company's business practices. The CCO should be consulted if you believe that the Manual does not accurately reflect the Company's business practices or should otherwise be revised or updated.

This Compliance Manual is not a full operational procedures manual, does not constitute legal advice and is not inclusive of all laws, rules, and regulations that govern the activities of the Company. It is intended to provide you an understanding of the policies, regulatory rules and requirements that apply to the Company.

Definitions

These terms have special meanings as used in this Compliance Manual:

Access Person - An "Access Person" is a Supervised Person who has access to nonpublic information regarding any client's purchase or sale of securities, is involved in making securities recommendations to clients, or has access to such recommendations that are nonpublic. All of the Company's directors, officers, and partners are presumed to be Access Persons.

Advisers Act - The Investment Advisers Act of 1940.

Associated Person - For purposes of this Compliance Manual, all Supervised Persons and Access Persons are collectively referred to as "Associated Persons."

Beneficial Interest - An individual has a Beneficial Interest in a security if he or she can directly or indirectly profit from the security. An individual generally has a Beneficial Interest in all securities held directly or indirectly, as well as those owned directly or indirectly by family members sharing the same household.

Chief Compliance Officer ("CCO") - Karla B. Engard.

Client - Any person for whom, or entity for which, the Company serves as an investment adviser, renders investment advice, or makes any investment decisions is considered to be a client.

Exchange Act - The Securities Exchange Act of 1934.

ERISA - The Employee Retirement Income Securities Act of 1974.

Federal Securities Laws - The Federal Securities Laws include the Securities Act, the Exchange Act, the Sarbanes-Oxley Act of 2002, the Investment Company Act, the Advisers Act, Title V of the Gramm-Leach-Bliley Act, any rules adopted by the SEC under any of these statutes, the Bank Secrecy Act as it applies to investment companies and investment advisers, and any rules adopted thereunder by the SEC or the Department of the Treasury.

Front-Running - Trading a favored account ahead of other accounts.

Insider Trading - Trading personally or on behalf of others on the basis of Material Nonpublic Information, or improperly communicating Material Nonpublic Information to others.

IPO - An initial public offering. An IPO is an offering of securities registered under the Securities Act where the issuer, immediately before the registration, was not subject to the reporting requirements of sections 13 or 15(d) of the Exchange Act.

Material Nonpublic Information - Information that (i) has not been made generally available to the public; and that (ii) a reasonable investor would likely consider important in making an investment decision.

Nonpublic Personal Information - Regulation S-P defines "Nonpublic Personal Information" to include personally identifiable financial information that is not publicly available, as well as any list, description, or other grouping of consumers derived from nonpublic personally identifiable financial information.

PCAOB - The Public Company Accounting Oversight Board.

Qualified Custodian - Financial institutions that clients and investment advisers customarily turn to for custodial services. These include banks and savings associations and registered broker-dealers.

Security - The SEC defines the term "security" broadly to include stocks, bonds, certificates of deposit, options, interests in Private Placements, futures contracts on other securities, participations in profit-sharing agreements, and interests in oil, gas, or other mineral royalties or leases, among other things. "Security" is also defined to include any instrument commonly known as a security.

SEC - The Securities and Exchange Commission.

Securities Act - The Securities Act of 1933.

Supervised Person - A "Supervised Person" is any partner, officer, director (or other person occupying a similar status or performing similar functions), or employee of an investment adviser, or other person who provides investment advice on behalf of the investment adviser and is subject to the supervision and control of the investment adviser. This may also include all temporary workers, consultants, independent contractors, and anyone else designated by the Chief Compliance Officer. For purposes of the Code, such 'outside individuals' will generally only be included in the definition of a supervised person, if their duties include access to certain types of information, which would put them in a position of sufficient knowledge to necessitate their inclusion under the Code. The Chief Compliance Officer shall make the final determination as to which of these are considered supervised persons.

Questions

Any questions concerning the policies and procedures contained within this Compliance Manual or regarding any regulations or compliance matters should be directed to the CCO, Karla B. Engard.

Receipt and Acknowledgment

At the time of hire, all Associated Persons are required to acknowledge that they have read and that they understand and agree to comply with the Company's compliance policies and procedures. Annually thereafter, all personnel shall be required to acknowledge and certify that they have complied with the Company's compliance policies and procedures during the preceding year.

Limitations on Use

This Compliance Manual must be returned to the Company immediately upon termination of employment. The information contained herein is confidential to the Company and proprietary to Foreside and may not be disclosed to any third party (other than applicable regulatory authorities) or otherwise shared or disseminated in any way without the prior written approval of the Company and Foreside.

Annual Compliance Reviews

The Company will conduct a documented review of its policies and procedures, at least annually, to determine their adequacy and the effectiveness of their implementation in consideration of:

1. the business being conducted by the Company, its IARs, and supervisory personnel;
2. any changes in the Advisers Act and/or applicable state or federal statutes, rules and regulations; and,
3. any compliance matters that arose during the previous year.

This review incorporates any compliance matters that arose during the preceding year, any substantive changes in the Company's business activities, and any applicable regulatory developments. During each annual review, the CCO, and staff, if applicable, evaluate and test both the efficacy and the implementation of the Company's written policies and procedures.

Ongoing Monitoring and Forensic Testing

The CCO and staff, if applicable, will monitor and periodically test compliance with the Company's policies and procedures. In addition to monitoring personal securities transactions and other Associated Person activities, the CCO and other supervisors, if applicable, periodically analyze the Company's books and records to detect patterns that may be indicative of compliance violations. Reviews of policies and procedures may also be warranted in the event of a material change to the Company's business practices.

Maintenance and Review of Compliance Program

Background

Rule 206(4)-7 under the Advisers Act requires each registered investment adviser to:

- Adopt and implement written policies and procedures reasonably designed to prevent violation, by the Company and its Associated Persons, of the Advisers Act and the rules thereunder;
- Review the adequacy of these policies and procedures, and assess the effectiveness of their implementation, at least annually; and
- Designate a Chief Compliance Officer who is responsible for administering the policies and procedures.

Policies and Procedures

In recognition of its obligation to maintain and review its compliance program, the Company:

i. has adopted policies and procedures (the Compliance Manual);
ii. will amend the Compliance Manual as appropriate;
iii. will perform risk assessments of its compliance program; and
iv. will perform an annual review of its policies and procedures.

These policies and procedures can be found in the following sections of this Compliance Manual.

Compliance Manual Amendments

The Company has adopted this Compliance Manual in order to reflect the Company's obligations under Federal Securities Laws, including the Advisers Act and associated rules.

The CCO is responsible for ensuring that the Compliance Manual is current and accurate at all times and for distributing the most current Compliance Manual to Associated Persons. No changes may be made to the Compliance Manual without the CCO's prior approval. The CCO should be consulted immediately if the Compliance Manual does not address a material compliance risk or is inconsistent with the Company's practices.

The Company will maintain a copy of the current Compliance Manual and each prior version along with details on the date of adoption and nature of each amendment or revision. The Company shall also maintain records of each Associated Person's acknowledgment of receipt of the Compliance Manual and any revisions thereto.

Compliance Risk Assessment Procedures

To create appropriate compliance risk controls, the Company reviews its compliance risks and requirements across the entire entity. This is accomplished by evaluating the Company's various lines of business, identifying related conflicts of interest, and determining the relevant compliance rules and regulations that govern the Company's investment advisory activities. Once relevant data is gathered and the Company has identified and assessed its compliance risks, the Company then reviews its controls, policies, and procedures to ensure they are reasonably designed to eliminate or mitigate those risks. Thereafter, risks are re-assessed in response to material changes in the Company's business, compliance reviews, regulatory examinations, or new rules and regulations are adopted.

Training

The CCO or designee will review applicable compliance policies and procedures with all new Associated Persons. The CCO or designee will conduct compliance training with Associated Persons, either individually or in groups, as necessary.

Designation of Chief Compliance Officer

Karla B. Engard is designated as the Company's Chief Compliance Officer ("CCO") and is empowered with full authority and responsibility to develop and administer the Company's on-going compliance program. The CCO will report directly to **Burgess Chambers**, **President**, of the Company. The CCO may designate one or more persons to carry out compliance responsibilities ("designee") but remains, at all times, ultimately responsible for the Company's compliance program and its implementation. Such individuals will report directly to the CCO. The CCO should be notified immediately if the Company has failed to identify or appropriately address any compliance issue.

Professional Designations or Certifications

Background

The SEC and state regulators do not endorse any financial professional designations or certifications. The use of a specific designation or certification by any person in connection with providing investment advice that indicates or implies that the person has special training in advising or servicing a client in such a way as to mislead any client is considered a dishonest and unethical business practice in violation of federal and state securities laws.

Policies and Procedures

The Company permits Associated Persons to refer to professional designations or certifications (collectively "designations") provided the individual has earned the designations and is in good standing with the sponsoring organization(s). Requests to use designations must be submitted in writing to the CCO for review and approval.

Use of Senior Specific Certifications or Designations

Professional designations implying expertise regarding seniors or retirees will be subject to heightened scrutiny. The CCO will follow guidelines set forth below when reviewing and determining whether certain senior specific certifications or designations would be permissible by Company personnel. Use of such designations by any person in connection with the provision of advice as to the value or the advisability of investing in, purchasing, or selling securities, either directly or indirectly or through publications or writings, or by issuing or promulgating analyses or reports relating to securities that indicates or implies that the user has special certification or training in advising or servicing senior citizens or retirees, in such a way as to mislead any person is prohibited. The prohibited use of such certifications or professional designations includes, but is not limited to, the following:

1. use of a certification or professional designation by a person who has not actually earned or is otherwise ineligible to use such certification or designation;
2. use of a nonexistent or self-conferred certification or professional designation;
3. use of a certification or professional designation that indicates or implies a level of occupational qualifications obtained through education, training, or experience that the person using the certification or professional designation does not have; and
4. use of a certification or professional designation that was obtained from a designating or certifying organization that:
    a. is primarily engaged in the business of instruction in sales and/or marketing;
    b. does not have reasonable standards or procedures for assuring the competency of its designees or certificants;
    c. does not have reasonable standards or procedures for monitoring and disciplining its designees or certificants for improper or unethical conduct; or
    d. does not have reasonable continuing education requirements for its designees or certificants in order to maintain the designation or certificate.

In determining whether a combination of words (or an acronym standing for a combination of words) constitutes a certification or professional designation indicating or implying that a person has special certification or training in advising or servicing senior citizens or retirees, the Company will consider the following factors:

1. use of one or more words such as "senior," "retirement," "elder," or like words, combined with one or more words such as "certified," "registered," "chartered," "adviser," "specialist," "consultant," "planner," or like words, in the name of the certification or professional

designation; and
2. the manner in which those words are combined.

A certification or professional designation does not include a job title within an organization that is licensed or registered by a state or federal financial services regulatory agency, when that job title:

1. indicates seniority or standing within the organization; or
2. specifies an individual's area of specialization within the organization.

Pre-Approval from CCO
When a supervised person wishes to list a professional designation, they must first notify the CCO who will be responsible for:

1. Confirming with the certifying authority that the individual does have the certification, and is in good standing;
2. Obtaining the information describing the nature of the designation and minimum qualifications required to obtain the designation; and
3. Amending, or causing to be amended and uploaded to IARD, the IAR's 2B Supplement disclosing the certification.

The CCO may request documentation from the supervised person demonstrating satisfaction of all requirements for use of any professional designation, or that the designation is in good standing. It is the responsibility of the person holding the designation to ensure that the designation remains in good standing and to immediately notify the CCO if there is a change in the status of the designation.

The CCO will notify the Associated Person in writing of the approval or denial regarding the use of the professional designation along with any additional applicable restrictions regarding use of such designation in connection with the individual's position with the Company.

State Specific Restrictions

Certain states have adopted their own policies on the use of certifications or professional designations. If an individual is conducting business on behalf of the Company in a state which has a more restrictive regulation than the Company does, the individual must follow that state's more restrictive rules. The CCO will include a review of state specific requirements as part of the overall approval process.

Advertising and Marketing

Policy

BCA and its advisory professionals use various advertising and marketing materials to obtain new advisory clients and to maintain existing client relationships. BCA's policy requires that any advertising and marketing materials must be truthful and accurate, consistent with applicable rules, and reviewed and approved by a designated officer. BCA's policy prohibits any advertising or marketing materials that may be misleading, fraudulent, deceptive and/or manipulative.

All advertising and marketing materials must have the following disclosure or clearly state that advisory services are offered through or by Burgess Chambers and Associates, Inc., a registered investment advisor.

Background

An advertisement is generally defined as any written communication, which includes websites and e-mails, directed to more than one person concerning advice or recommendations about the purchase or sale of securities or any other advisory service.

The SEC anti-fraud rules under the Advisers Act prohibit advisers from engaging in advertising practices which are fraudulent, deceptive, or manipulative activities. The manner in which investment advisers portray themselves, services and their investment returns to existing and prospective clients is highly regulated. SEC no-action letters also provide guidelines and prohibitions relating to an adviser's advertising and marketing practices.

Responsibility

The Chief Compliance Officer, or designee(s), has the responsibility for implementing and monitoring our policy, and for reviewing and approving any advertising and marketing to insure any materials are consistent with our policy and regulatory requirements. This designated person is also responsible for maintaining, as part of the BCA's books and records, copies of all advertising and marketing materials with a record of reviews and approvals in accordance with applicable recordkeeping requirements.

Procedure

BCA has adopted procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- All advertisements and promotional materials must be reviewed and approved prior to use by a designated officer, President, the Chief Compliance Officer, or another officer of the firm (other than the individual who prepared such material).
- The initialing and dating of the advertising and marketing materials will document approval.
- Each advisory professional is responsible for ensuring that only approved materials are used and that approved materials are not modified without the express written approval of the Chief Compliance Officer, or designee(s).
- The Chief Compliance Officer, or designee(s), must also review other written communications prepared for existing clients or prospective clients that would be deemed marketing material.
- The Chief Compliance Officer, or designee(s), is responsible for maintaining copies of any advertising and marketing materials, including any reviews and approvals, for a total period of five years following the last time any material is disseminated.

Client Contracts

Background

While the Advisers Act does not require the use of written investment advisory contracts, it does regulate certain aspects of investment advisory contracts including assignment of contracts, notification to clients of partnership changes (if the investment adviser is organized as a partnership), restrictions on performance-based fees, prohibition on waiver of compliance with the Advisers Act, and prohibition on hedge and arbitration clauses.

Under Section 205 of the Advisers Act, the Company may not assign an advisory contract without the client's consent. The definition of "assignment" contained in the Advisers Act is quite broad and would be deemed to occur as a result of a transfer of a controlling block of securities of either an investment adviser, or of the investment adviser's parent company.

In recognition of the fact that this broad definition encompasses many types of transactions that while technically an assignment, do not in fact alter the actual control or management of an investment adviser, the Commission adopted Rule 202(a)(1)-1 which deems transactions that do not result in a change of actual control or management of the investment adviser not to be considered an assignment under the Advisers Act. Neither the Advisers Act nor the rules thereunder specify the manner in which an investment adviser must obtain client consent to an assignment of an advisory contract. However, the SEC staff has, in the past, taken the position that if an investment adviser notifies a client in writing of an assignment and advises the client that the assignment will take place if the client does not object within a reasonable time period, (such as 60 days) the client's silence may be treated as appropriate consent. The acceptability of the use of such negative consent is fact-specific and must be determined on a case-by-case basis.

Except as provided under Rule 205-3, Section 205 of the Advisers Act prohibits an advisory contract from providing for compensation to the investment adviser on the basis of a share of capital gains upon or capital appreciation of the client's funds. Except for performance fees, the Advisers Act does not specifically address or explicitly regulate the types or amount of advisory fees the Company may charge clients for its advisory services. Rather, the Advisers Act regulatory scheme relies primarily on disclosure to address the appropriate level of fees and requires an investment adviser, as a fiduciary, to make full and fair disclosure to clients about the fees it charges.

The Advisers Act also prohibits any contract or other provision that purports to waive compliance with the Advisers Act or rules thereunder (i.e. hedge clause).

Policies and Procedures

The CCO is responsible for ensuring that the Company's client contracts comply with this policy and are signed and maintained in each client file.

Standard Contract Provisions

While the Advisers Act does not expressly require that advisory contracts between the Company and its clients be in writing, as a matter of good business practice, the Company requires that each client complete a written client contract, which must:

- Set forth that the client contract is not assignable without the consent of the client;
- Describe the discretionary authority provided by the client to the Company(as applicable);
- State the agreed-upon advisory fee;
- Authorize the Company to instruct the qualified custodian to deduct its advisory fees directly

from the client's account (as applicable); and
- Include authorization by the client for the Company to vote proxies on behalf of the client, or expressly indicate that the Company will *not* vote proxies when discretion is granted by the client.

The Company should also consider including the following provisions, as appropriate:

- Provide for the refund of unearned advisory fees paid in advance in the event of termination of the client contract;
- Include a signed acknowledgment by the client of receipt of all disclosure documents (i.e. Form ADV Part 2, Privacy Notice);
- Include consent by the client to receive disclosure documents electronically (as applicable);
- Describe the procedures and time required to terminate the client contract;
- Describe the procedures for fee settlement in the event of termination of the client contract; and,
- Is signed by both the client and an authorized representative of the Company.

Assignment

The term assignment is defined broadly to include any direct or indirect transfer of an investment advisory contract by an investment adviser or any transfer of a controlling block of an investment adviser's outstanding voting securities. However, a transaction that does not result in a change of actual control or management of the investment adviser (e.g., reorganization for purposes of changing an investment adviser's state of incorporation) would not be deemed an assignment for these purposes.

Other Provisions

- Associated Persons may not enter into an advisory contract with a client that provides for advisory fees that are different from the Company's standard advisory fees without prior written approval of the CCO;
- The CCO is responsible for ensuring that clients who have multiple accounts under the Company's management receive appropriate breakpoints, as applicable; and
- If a client terminates a client contract, the Company shall return to such client any pre-paid, unearned advisory fee, pro-rated for the number of days in which advisory services were rendered. Any reduction for reasonable startup expenses may be made only with the prior written approval of the CCO and only if previously disclosed to the client in writing.

Performance Fees

The Company does not currently receive fees that are related to the performance of client accounts. Performance-based compensation includes compensation based on a share of the capital gains upon, or the capital appreciation of, the assets, or any portion of the assets, of a client (hereafter "performance-based compensation"). In the event the Company charges performance-based compensation in the future, all such clients must meet the definition of a "qualified client" as defined in Rule 205-3 of the Advisers Act.

Waiver of Compliance

The Company is prohibited from including any contractual provision of an advisory contract from purporting to waive compliance with pertinent securities laws or any rule(s) thereunder. Any condition, stipulation, or provision so used shall be void.

Hedge Clauses
The Company will not include any legend, hedge clause, or other provision which, is likely to lead a client to believe that the client has waived, in any way, any available right of action the client may have against the Company under federal and/or state securities laws.

Prepaid Advisory Fees
In no event shall the Company charge advisory fees that are both in excess of $1,200 and paid more than six months in advance of advisory service being rendered.

Death of a Client
Upon notification of the death of a client, the Company will work closely with the custodian to ensure the appropriate paperwork is on file before any changes are made to the account or control person of the account. The Company should review the advisory contract to determine when the contract terminates. The custodian may freeze the account until a personal representative is appointed. If the client contract terminates upon written notice of a client's death, the advisory fee will be prorated for the quarter in which the termination occurred. Any unearned fees will be returned to the client's account. If the death of a client does not terminate or change the terms of the contract, the client's executor, guardian, attorney-in-fact, trusted contact person or other authorized representative should be contacted to determine the ongoing management or termination of the account.

Use of Social Networking Sites

Associated Persons Use of Social Media
The absence, or lack, of explicit reference to a specific site does not limit the extent of the application of this policy. Where no policy or guideline exists, or if you do not understand what constitutes social media ask the CCO. Do not guess at the answer.

For purposes of this policy, "social media" and social networking includes any activity that integrates technology, social interaction, and content creation, and includes but is not limited to blogs, networking sites (Facebook, LinkedIn, Snapchat), photo sharing (flickr, Instagram), video sharing (YouTube, Vimeo, Vine), microblogging (Twitter), wikis, podcasts, and virtual worlds, as well as comments posted on the sites.

Associated Persons are permitted to post only on social media that has been specifically approved by the CCO.

Use of all other social media for work purposes is strictly prohibited. Associated Persons' use of approved social media is subject to the following restrictions:

1. The use of any social networking site for the purpose of advertising the Company's advisory services or soliciting clients must first be pre-approved by the CCO. The CCO's approval shall be evidenced in writing;
2. No social networking site may be used for the purpose of advertising the Company's advisory services or soliciting clients unless administered by the Company. The Company shall maintain a list of all Associated Persons who have administrative access to the account;
3. All content posted on social networking sites is considered "Advertising" as defined herein and is therefore subject to all requirements and restrictions set forth in this Compliance Manual;
4. All Company-related content posted shall be pre-approved by the CCO. Evidence of the CCO's approval shall be documented as part of the Company's books and records;
5. References to the Company's performance or clients' performance or level of satisfaction are prohibited;
6. Prohibited Content: Associated Persons may not post any information about recommendations,

investment decisions, specific products or services, performance, or any information that could cause harm to the Company's reputation;
7. Third Party Content: Associated Persons should not solicit third-party content. Third-party postings should be limited to authorized users and should be promptly reviewed by the CCO. The Company should disclose on the site that it does not approve or endorse any third-party communications posted on the site;
8. Testimonials Prohibited: "Recommendations" or "Likes" from Company clients may be viewed as improper testimonials and are prohibited;
9. Associated Persons may not make reference to the Company's advisory services on their personal sites; and
10. Information Protection and Privacy: The Company holds information about clients in strict confidence. Associated Persons must never identify an individual as being a client, or post any nonpublic information about a client, in a public forum. The Company recognizes that social media sites (especially third party sites) pose elevated information security risks, and the Company ensures that firewalls are in place to protect client or proprietary data from exposure to the social media site(s).

Social media content is also subject to the Company's policies and procedures on correspondence and electronic communication. See the Client Correspondence and Electronic Communications section of this Manual for further information.

The CCO, or designee, shall review approved social media periodically to ensure compliance with these restrictions. Associated Persons should consult with the CCO if they have any questions about the preceding policies.

Outside the Workplace

Outside the workplace, Associated Person's rights to privacy and free speech protect online activity conducted on their personal social networks and through their personal email address. Associated Persons postings on their personal online sites should never be attributed to the Company and should not appear to be endorsed by or originated from the Company.

Associated Persons should remember that their online lives are ultimately linked whether or not the Company is mentioned in their personal online networking activity. At all times, Associated Persons are subject to the following Company procedures:

1. Without exception, Associated Persons may not make reference to the Company's advisory services on their personal sites;
2. The Company logos and trademarks may not be used without prior written consent from the CCO; and
3. Without exception, Associated Persons may not reference any Company clients.

Associated Persons should consult with the CCO if they have any questions about the preceding policies.

Approval of Outside Employment/Activities

Background

Associated Persons may, under certain circumstances, engage in outside business activities. Associated Persons should carefully consider any outside business activity which conflicts with, or has the appearance of conflicting with the business of the Company or its clients. Certain Associated Persons may be required to disclose outside business activities to clients in their Form ADV Part 2B, Brochure Supplement (see Form ADV Disclosure Requirements).

Policies and Procedures

An Associated Person must receive prior written approval from the CCO for any outside business activity (i) that is investment-related, (ii) involves clients or potential clients, (iii) relates to the business of the Company, (iv) conflicts with or has the appearance of conflicting with the interests of the Company or its clients (v) involves serving as a financial officer of another entity (including for non-for-profit companies), (vi) for which such Associated Person is compensated, or (vii) that involves a substantial amount of the Associated Person's time. This includes, but is not limited to, any activity as a proprietor, partner, officer, director, employee, trustee, agent, or similar capacity, but excludes non-investment related activities that are exclusively charitable, civic, religious, or fraternal, and are recognized as tax exempt for which no compensation is obtained. Approval is granted on a case-by-case basis, subject to careful consideration of potential conflicts of interest, disclosure obligations and any other relevant regulatory issues. Associated Persons should use the *Outside Business Activities Notification Form* or other form as required by the Company to report outside business activities. Certain Form ADV disclosures and amendments may also be required.

Associated Persons may not borrow from or become indebted to any person, business or company having business dealings or a relationship with the Company, except with respect to customary personal loans (such as home mortgage loans, automobile loans, and lines of credit), unless the arrangement is disclosed in writing and receives prior approval from the CCO.

An Associated Person may not participate in any business opportunity that comes to his or her attention as a result of his or her association with the Company or in which he or she knows that the Company might be expected to participate or have an interest, without:

- Disclosing all necessary facts to the CCO;
- Offering the particular opportunity to the Company; and
- Obtaining written authorization to participate from the CCO.

Any personal or family interest in any of the Company's business activities or transactions must be immediately disclosed to the CCO. For example, if a transaction by the Company may benefit that Associated Person or a family member, either directly or indirectly, then the Associated Person must immediately disclose this possibility to the CCO.

If an Associated Person receives written approval to engage in an outside business activity and subsequently becomes aware of a material conflict of interest that was not disclosed when the approval was granted, the conflict must be promptly brought to the attention of the CCO.

Advisory Agreements

Policy
BCA's policy requires a written investment advisory agreement for each client relationship which includes a description of our services, discretionary/non-discretionary authority, advisory fees, important disclosures and other terms of our client relationship. BCA's advisory agreements meet all appropriate regulatory requirements and contain a non-assignment clause and do not contain any "hedge clauses".

Background
Written advisory agreements form the legal and contractual basis for an advisory relationship with each client and as a matter of industry and business best practices provide protections for both the client and an investment adviser. An advisory agreement is the most appropriate place for an adviser to describe its advisory services, fees, liability, and disclosures for any conflicts of interest, among other things. It is also a best business practice to provide a copy of the advisory agreement to the client and for the agreement to provide for all client financial and personal information to be treated on a confidential basis.

Responsibility
The Chief Compliance Officer has the responsibility for the implementation and monitoring of the firm's advisory agreement policy, practices, disclosures and recordkeeping.

Procedure
BCA has adopted procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- BCA's advisory agreements and advisory fee schedules, and any changes, for the firm's services are approved by management.
- The fee schedules are periodically reviewed by BCA to ensure that fees are fair, current and competitive.
- The Chief Compliance Officer, or designee(s), periodically reviews the firm's disclosure brochure, marketing materials, advisory agreements and other material for accuracy and consistency of disclosures regarding advisory services and fees.
- Performance-based fee arrangements are appropriately disclosed, reviewed and approved by the President.
- Written client investment objectives or guidelines are obtained, or recommended as part of a client's advisory agreement.
- Client investment objectives or guidelines are monitored on an on-going and also periodic basis for consistency with client investments/portfolios.
- Any solicitation/referral arrangements and solicitor/referral fees must be in writing, reviewed and approved by the President, meet regulatory requirements and appropriate records maintained.
- Additional compensation arrangements are to be monitored by the President or designee(s), approved and disclosed with appropriate records being maintained.

Disclosure Document

Form ADV Part 1 and 2
Form ADV Part 1 is submitted electronically and is used to register with the Securities and Exchange Commission or one or more state securities authorities and to amend those registrations.

The Company will use Part 2 of the Form ADV to meet its disclosure obligations. The Company will continue to amend its Form ADV Part 2 (also referred to as "Disclosure Brochure") when the information therein becomes materially inaccurate. The Part 2 is a uniform form used by investment advisers registered with both the SEC and state securities authorities. The Part 2 includes two sub-parts, Part 2A and Part 2B. Part 2A includes disclosure items about the investment adviser all of which must be addressed in the Company's disclosure brochure. The Part 2B is a brochure supplement which includes information about the advisory personnel on whom each particular client relies for investment advice.

Delivery of Form ADV Part 2 & Supplements

- **Initial Delivery** - the Company will provide a copy of its current Disclosure Brochure (Part 2A) and relevant supplemental brochures (Part 2B) to clients prior to or at the time the client executes an agreement for services with the Company. The Company will obtain proof of delivery of the Company's Disclosure Brochure, and relevant supplemental documents, by either confirmation of receipt in the client agreement or through a separate acknowledgement signed by the client.
- **Interim Delivery** - the Company will deliver an updated disclosure brochure to its clients promptly whenever the Company amends its disclosure brochure to add a disciplinary event or to change material information already disclosed as a disciplinary event on the Company's Form ADV (or a document describing the material facts relating to the amended disciplinary event). Otherwise, the Company is not required to provide an interim delivery of its Disclosure Brochure.
- **Annual Delivery** - On an annual basis, the Company will provide to each client either a) a copy of its current (updated) disclosure brochure that includes or is accompanied by a summary of material changes (see below); or b) a summary of material changes that includes an offer to provide a copy of the current disclosure brochure. The Company must make this annual delivery no later than 120 days after the end of its fiscal year. The Company will maintain a list of all clients that participated in the annual mailing/offer, and evidence of the date the offer or delivery was made.

    a. During any given year, if the Company has not filed any interim amendments to its Disclosure Brochure since the last annual amendment and the disclosure brochure continues to be accurate in all material respects, the Company is not required to prepare, deliver, or offer a summary of material changes (or a current copy of its disclosure brochure) to existing clients.

Delivery of Form ADV Part 3

Form ADV, Part 3 ("Form CRS" or "Relationship Summary") must be delivered to all retail investors. For the purposes of Form CRS, a retail investor is a "natural person, or the legal representative of such natural person, who seeks to receive or receives services primarily for personal, family or household purposes." This definition excludes natural persons seeking investment services for commercial or business purposes; however, if a person is seeking services for a mix of personal and non-personal purposes, the Form CRS must be delivered to such person. If the Company does not have any prospective or existing retail clients, the Company is not required to prepare or file Form CRS.

- **Initial Delivery** - Consistent with the Disclosure Brochure (Part 2A), the Company will provide a copy of its Form CRS (Part 3) to each retail investor prior to or at the time the client executes an agreement for services with the Company. The Company will also obtain proof of delivery of the Company's Form CRS, which may be in the form of an acknowledgement of receipt contained in the client agreement, or in a separate acknowledgement, or by an electronic mail return-receipt or by confirmation that the information was accessed, downloaded, or printed.
- **Interim Delivery** - After initial delivery, the Company must deliver its most recent Form CRS to

existing retail clients before or at the time:

- A new account is opened that is different from the retail client's existing account(s); or
- Changes are made to the retail client's existing account(s) that would materially change the nature and scope of the Company's relationship with the retail client. For example, the Company must deliver a Form CRS:
    - upon opening a new account that is different from the retail investor's existing account (the firm is not required to deliver a relationship summary when amending an existing account agreement solely to add another account holder or beneficiary);
    - when recommending that the retail client roll over assets from a retirement account into a new or existing account or investment; or
    - when recommending or providing a new investment advisory service or investment that does not necessarily involve the opening of a new account and would not be held in an existing account, for example, the first-time purchase of a direct-sold mutual fund or insurance product that is a security through a "check and application" process, i.e., not held directly within an account.

The Company will maintain a list of all clients and prospects who received a copy of the Form CRS and document evidence of the date the delivery was made.

Upon a retail client's request, the Form ADV, Part 3 must be delivered to the client within 30 days. The CCO, or designee, oversees the Company's distribution of Part 3 to all prospective and current clients.

Delivery methods of Form ADV Part 3

A current version of the Company's Form CRS must be posted prominently on the Company's public website in a location and format that is easily accessible for retail clients. The Company must also deliver its Form CRS either electronically or in paper format as described below.

The Company may also deliver the Form CRS (including updates) electronically once it has explicit consent from the retail client. If the Company's Form CRS is delivered electronically, it must be presented prominently in the electronic medium, for example, as a direct link or in the body of an email or message, and must be easily accessible for retail clients.

If the Company's Form CRS is delivered in paper format as part of a package of documents, the Company must ensure that the Form CRS is the first among any documents that are delivered in the package.

The CCO, or designee, oversees the Company's distribution of Parts 2A, 2B and Part 3 to all prospective and current clients.

Amendments and Material Changes to Form ADV

The Company shall keep the disclosure brochure(s) and relationship summaries they file with the SEC and/or state securities regulator(s) current by updating them at least annually, and updating them promptly when any information in the Disclosure Brochure and Relationship Summary becomes materially inaccurate.

The standard of materiality is whether there is a substantial likelihood that a reasonable investor (here, client) would have considered the information important in deciding to retain (or continue to retain) the investment adviser for advisory services. There is no specific definition for materiality. Rather, materiality depends on the factual circumstances that may vary with each situation.

The Company's Form ADV should be amended to correct inaccuracies, promptly (within 30 days of the event), if:

1. the information in Items 1, 3, 9, or 11 of Part 1A becomes inaccurate in any way;
2. the information in Items 4, 8, or 10 of Part 1A becomes "materially" inaccurate;
3. the information in the Disclosure Brochure or Relationship Summary becomes "materially" inaccurate.

Under federal and state law, investment advisers are fiduciaries and must make full disclosure to their clients of all material facts relating to the advisory relationship. To satisfy this obligation, an investment adviser may have to disclose information to clients not specifically required by the Form ADV or in more detail than the Disclosure Brochure items may require.

All other changes to the ADV may be made at year's end when the Company files its annual updating amendment.

Summary of Material Changes

Item 2 of the Part 2 requires an investment adviser amending its disclosure brochure to identify and discuss the material changes in its disclosures since the last annual updating amendment. This summary of material changes must be included on the cover page to the disclosure brochure or the following page, or as a separate document accompanying the disclosure brochure.

Annual Updating Amendment of Form ADV

Within 90 days after the Company's fiscal year end, the Company must file an annual updating amendment, which is an amendment to the Company's Form ADV that reaffirms the eligibility information contained in Item 2 of Part 1A and updates the responses to any other item for which the information is no longer accurate.

The amount of the Company's assets under management is generally updated as part of the Company's annual filing requirement. However, if the Company is amending its disclosure brochure for a separate reason between annual amendments, and the amount of its assets under management is materially inaccurate, the Company will also amend its reported assets under management.

The CCO is responsible for arranging the submission of the Company's annual filing. In preparing to submit the annual updating amendment, the CCO, and other parties within the Company that the CCO so designates, will review the Company's Form ADV in its entirety to ensure all disclosures are accurate and current based on the Company's current business model.

The CCO, or designee, oversees the Company's filing of annual amendments on Form ADV.

Updating Form CRS

The Company must update and file its Form CRS within 30 days whenever any information in the Form CRS becomes materially inaccurate. The filing must include an exhibit highlighting the most recent changes by redlining the revised text or including a summary of material changes.

The Company will communicate any changes in the updated Form CRS to retail investors who are existing clients within 60 days after the updates are required to be made without charge. The Company may make the communication by delivering the amended Form CRS or by communicating the information through another disclosure that is delivered to its clients. The updated Form CRS delivered to clients must contain the exhibit highlighting the most recent changes.

The CCO, or designee, oversees the Company's filing of amendments on Form CRS.

Filing Interim Amendments of Form ADV

In between annual amendments, Parts 1A and 2A of Form ADV must be updated and re-filed promptly if any information in response to (i) Items 1 (Identifying Information), 3 (Form of Organization), 9 (Custody), or 11 (Disciplinary Information) of Part 1A becomes inaccurate in any way, or (ii) Items 4 (Successions), 8 (Participation or Interest in client Transactions) or 10 (Control Persons) of Part 1A becomes materially inaccurate, or (iii) information provided in Part 2A becomes materially inaccurate.

If the Company is submitting an interim amendment to its Form ADV Part 2A in between annual amendments, and the amount of client assets it manages or its fee schedule listed in response to Item 4.E has become *materially* inaccurate, the Company will update those item(s) as part of the interim amendment.

The CCO, or designee, oversees the Company's filing of other-than-annual (interim) amendments on Form ADV.

Calculating Regulatory Assets Under Management

In calculating regulatory assets under management ("RAUM"), firms may only include the *securities portfolios* for which it provides ***continuous and regular supervisory or management services***.

In addition to client accounts, all securities portfolios managed by the Company for the Company, family members, and any proprietary accounts, as well as securities portfolios for which the Company receives no compensation, are included.

Most discretionary accounts should be included in calculating the Company's RAUM. An RIA has discretion when it has authority to decide which securities to purchase or sell for the client. This also includes discretionary authorization to hire and fire third-party managers in a client's account.

Non-discretionary accounts should be included in the Company's RAUM calculation only if the RIA selects or makes recommendations regarding specific securities or other investments *and* is responsible for arranging or effecting the purchase or sale of the investment in the client's account.

In calculating the Company's RAUM, for reporting purposes on the Form ADV Part 1A, the Company will:

1. Look first at whether each account is a securities portfolio. A *securities portfolio* means any account a majority of whose value (excluding cash and cash equivalents, such as demand deposits) consists of securities. The entire value of any portfolio constituting a "securities portfolio" (including the part comprised of non-securities assets) will be included as part of the Company's "regulatory assets under management."
2. If the account is a securities portfolio, the Company will then establish whether that account receives continuous and regular supervisory or management services. Only assets that are managed on a continuous and regular basis - as defined in the instructions to the Form ADV - are relevant.

Disciplinary and Financial Disclosure Requirements - Part 2A

An investment adviser has a duty to provide clients and prospects with disclosure of all material facts regarding:

- Any precarious financial position involving the investment adviser; and
- Any legal or disciplinary event, involving the Company or its Associated Persons that is material

to an evaluation of the Company's integrity or its ability to meet contractual commitments to clients.

Investment adviser representatives are required to contact the CCO immediately if they become involved in, or threatened with, litigation or any administrative investigation or proceeding of any kind, become subject to a judgment, order, or arrest, are contacted by a regulatory authority, or are aware of any precarious financial position or other legal or disciplinary event.

Associated Persons will report all disciplinary (legal, regulatory, or otherwise) or precarious financial events to the CCO. The CCO will assess whether such events are required to be disclosed pursuant to the Form ADV instructions or to the investment adviser's role as a fiduciary. The CCO will make such disclosures as necessary. These disclosures must be made to existing and/or prospective clients if the event is material to their evaluation of the integrity of the investment adviser, its management personnel, supervised persons, or its IARs.

Item 9 of the Form ADV Part 2A includes a list of legal or disciplinary events that are presumed to be material for a period of ten (10) years from the time of the event if they were not resolved in the investment adviser's or management person's favor or subsequently reversed, suspended or vacated, or the Company has not rebutted the presumption of materiality to determine that the event is not material (see Note below). For purposes of calculating this ten-year period, the "date" of an event is the date that the final order, judgment, or decree was entered, or the date that any rights of appeal from preliminary orders, judgments or decrees lapsed.

Under federal and state law, investment advisers are fiduciaries and must make full disclosure to their clients of all material facts relating to the advisory relationship. If the Company or a management person has been involved in a legal or disciplinary event that is not listed in Item 9 of the Form ADV, but nonetheless is material to a client's or prospective client's evaluation of the Company or the integrity of its management, even if more than ten years have passed since the date of the event, the Company will disclose the event.

Note: In the event that an issue arose that might require disclosure, under certain circumstances the Company is permitted to rebut the presumption that a disciplinary event is material. If an event is immaterial, the Company would not be required to disclose it. In such event, review of the legal or disciplinary event involving the Company or a management person must determine whether it is appropriate to rebut the presumption of materiality by considering all of the following factors: (1) the proximity of the person involved in the disciplinary event to the advisory function; (2) the nature of the infraction that led to the disciplinary event; (3) the severity of the disciplinary sanction; and (4) the time elapsed since the date of the disciplinary event. If the Company concludes that the materiality presumption has been overcome, the Company must prepare and maintain a file memorandum of such determination in its records.

Annual Review of Disclosures

The CCO shall annually review the Company's Form ADV and update the disclosures therein. Disclosures made in the Company's Form ADV may appear or be used in other documents or communications to clients or prospective clients. The CCO shall periodically review, reconcile and update disclosures made in any contracts, advertising and marketing materials, and any other documents that are provided to clients or prospective clients to ensure the disclosures are consistent with the Form ADV.

Additional Disclosure Requirements

The Company has implemented policies to ensure that the Company meets the additional disclosure requirements as set forth in the relevant sections within this Compliance Manual: solicitor fees, privacy notice disclosures, and proxy voting disclosures. Disclosures on each of these subject items are included in the Company's Form ADV, advisory agreement, or other required document.

Books and Records

Background

Rule 204-2 under the Advisers Act requires investment advisers to maintain certain books and records listed in the following *Specific Record Keeping Requirements* table. Investment advisers should also establish policies and procedures governing:

- The accurate creation of books and records;
- Any appropriate limitations on the availability of certain books and records to certain Associated Persons and outside entities; and
- The proper disposal of books and records that need not be maintained for business or regulatory compliance purposes.

The accurate creation and proper maintenance and use of books and records are an important foundation of any investment adviser's operations and compliance with applicable Federal Securities Laws.

Record retention policies and procedures should be tailored to reflect an investment adviser's size and operations. Furthermore, any record retention program should be periodically reevaluated, particularly following significant regulatory, operational, or technological changes. Record retention program reviews should evaluate, among other things:

- The effectiveness of the current record retention program;
- Whether the use of electronic and/or hard-copy storage media are meeting the investment adviser's needs;
- Associated Persons' awareness of, and compliance with, the investment adviser's record retention program;
- Whether the investment adviser's current practices are accurately reflected in its written policies and procedures;
- Whether the creation, maintenance, and confidentiality of certain books and records poses particular compliance or business risks for the investment adviser; and
- Whether the investment adviser has devoted appropriate amounts of resources to meet its record retention needs.

Associated Persons should be aware that all of the records of a registered investment adviser can be subject to review by SEC examiners, irrespective of whether the records are required to be retained pursuant to Rule 204-2. Associated Persons should be aware that the SEC's examination authority includes emails and other electronic communications that relate to a registered investment adviser's business activities, as well as emails and other electronic communications that are sent or received on the investment adviser's computer systems.

Policies and Procedures

It is the Company's policy to create and maintain all books and records that are required under the Investment Advisers Act and related SEC rules. The CCO has the overall responsibility for the implementation and monitoring of the Company's books and records policy and recordkeeping requirements. The Company will maintain true, accurate, and current records that are well organized at all times via a filing system sufficient to allow their retrieval within a reasonable amount of time. The Company is at all times subject to surprise examinations of its books and records by the SEC and other governmental authorities.

It is a violation of law to forge, falsify, tamper with, obliterate, or prematurely destroy these records. Doing so could subject the personnel involved to criminal penalties, regulatory sanctions and/or termination of employment.

Books and records required by Rule 204-2 under the Advisers Act will be maintained for at least five years from the date that the record was created or last altered, whichever is more recent. Certain required records must be kept for longer periods of time as indicated below at *Specific Record Keeping Requirements*. Required records will be kept onsite for at least two years after they are created or last altered, and will be organized to permit easy location, access, and retrieval.

Associated Persons may only remove original records from the Company's office with the CCO's approval.

All Associated Persons must be familiar with, and abide by, the Company's record retention policies and procedures. The CCO is responsible for overseeing the Company's record retention program. Any questions about the Company's records retention policies and procedures should be directed to the CCO.

The Company maintains all required books and records at its principal office.

Pending Litigation or Regulatory Inspection

The Company will take steps to ensure that no relevant books or records are destroyed if litigation or a regulatory inspection is pending.

Retention Requirements

Books and records will be maintained for at least five years from the date that the record was created or last altered, whichever is more recent. Certain required records must be kept for longer periods of time as indicated below at *Specific Record Keeping Requirements*. Required records will be kept onsite for at least two years after they are created or last altered, and will be organized to permit easy location, access, and retrieval.

Specific Record Keeping Requirements (to the extent they apply)

Accounting Records	
Journals	Journals that include cash receipts and disbursements records, and any other records of original entry forming the basis of entries in any ledger.
Ledgers	General and auxiliary ledgers that reflect asset, liability, reserve capital, and income and expense accounts.
Account Documentation	Checkbooks, bank statements, canceled checks, and cash reconciliations.
Invoices	Bills or statements of account (paid or unpaid).
Financial Statements	Financial statements (income statement, trial balance, and balance sheet) and internal working papers.

Advisory Records	
Trade Tickets	A memorandum of each order given by the Company for the purchase or sale of a security. The memorandum may be an order ticket that is date-stamped or otherwise marked to comply with the requirements below. Such memoranda shall: 1. show the terms and conditions of the order (buy or sell); 2. show any instruction, modification, or cancellation; 3. identify the person connected with the Company who recommended the transaction to the client; 4. identify the person who placed the order; 5. show the account for which the transaction was entered; 6. show the date of entry; 7. identify the bank, broker, or dealer by or through whom such order was executed; and 8. identify orders entered into pursuant to the exercise of the Company's discretionary authority.
Written Materials	Written materials received and sent by an IAR or by the Company to clients, including postal and electronic mail ("e-mail") and instant messages, if any. There are three classes of covered written materials, which include: (1) recommendations and advice given or proposed; (2) receipt, disbursement, or delivery of client funds and securities; and (3) placing and executing orders to purchase or sell securities. Examples of communications that would qualify to be kept under the above requirement include: 1. e-mail to any client about a proposed trade in their account; 2. a letter or e-mail sent by the Company to a client's custodian regarding the disbursement of the Company's management fee; 3. an e-mail complaint from a client or investor; 4. a portfolio manager's e-mail to a client on an update to a financial plan or asset allocation strategy; and 5. trade confirmations received by the Company (whether in hard copy or electronic format).
Performance Communications	Originals of all written communications received and copies of all written communications sent by the Company to a single person relating to the performance or rate of return of any or all managed accounts or securities recommendations: Provided, however that: 1. the Company shall not be required to keep any unsolicited market letters and other similar communications of general public distribution not prepared by or for the Company; and 2. if the Company sends any notice, circular, or other advertisement offering any report, analysis, publication, or other investment advisory service to more than 10 persons, the Company shall not be required to keep a record of the names and addresses of the persons to whom it was sent; except that if such notice, circular, or advertisement is

	distributed to persons named on any list, the Company shall retain with the copy of such notice, circular, or advertisement a memorandum describing the list and the source thereof.
Discretionary Authority	A list of all accounts over which the Company has discretionary authority with respect to the funds, securities, or transactions, if any.
Continuously Managed Accounts	Company shall maintain, for all managed accounts, to the extent that the information is reasonably available or obtainable, records showing separately for each client the securities purchased and sold, and the date, amount and price of each such purchase and sale, and for each security in which any such client has a current position, information from which the Company can promptly furnish the name of each such client, and the current amount or interest of such client, if any.
Limited Trading Powers of Attorney	All powers of attorney and other evidence of the granting of discretionary authority by any client.
Written Agreements	Any written agreement or contract that the Company is a party to, including but not limited to; written contracts with clients; third-party service providers; and/or solicitors.
Personal Trading Records	A record of any securities transactions in which the Company or any IAR acquires a direct or indirect beneficial ownership. (The Company receives duplicates of Associated Person brokerage statements and confirms).
Form ADV Documentation (Parts 2A. 2B and 3)	A copy of each disclosure brochure (Form ADV 2A) and brochure supplement (Form ADV Part 2B) and Relationship Summary (Form CRS), and each amendment or revision to the disclosure brochure, brochure supplements and Relationship Summary; any summary of material changes that is not contained in the disclosure brochure or brochure supplements; and a record of the dates that each disclosure brochure, brochure supplement and Relationship Summary, each amendment or revision thereto, and each summary of material changes was given to any client or any prospective client who later becomes a client. A memorandum describing any legal or disciplinary event listed in Item 9 of Part 2A or Item 3 of Part 2B of Form ADV (Disciplinary Information) and presumed to be material, if the event involved the Company or any of its supervised persons and is not disclosed in the disclosure brochure or brochure supplement of Part 2B of Form ADV.
Privacy Policy Notice	Documentation of initial delivery and receipt of Privacy Policy Notice and evidence of Annual Delivery of Privacy Policy Notice, if

	applicable, including a list of clients who were sent the Company's Privacy Policy Notice and the date of delivery/mailing.
Solicitor's Acknowledgments	All written acknowledgments obtained from and copies of the disclosure documents provided to clients who were referred to Company by an unaffiliated, third-party solicitor, if any.
Entity Documents	Articles of Incorporation/Organization, partnership agreement, minute books, etc. These records must be maintained continuously in the Company's office until termination of the business and in an easily accessible place of which the appropriate regulatory authority has been notified for three years after termination of the entity.
Organization Chart	This should include documents reflecting the Company's owners, officers, directors, partners, controlling persons, and employees. This should also include ownership percentage of the Company, whether any individual is also an officer, director, partner, employee, or affiliate of any other public or privately held organization (trust, corporation, business venture).
Regulatory Communications	Communications received from and sent to the SEC, state or other regulatory authority.
Trade Errors	Documentation of the error and supporting documentation on reconciliation.
Client Complaint	Documentation of complaint and supporting documentation on resolution.
Securities Transaction Journal	A record, by client, of the securities purchased and sold, and the date, amount, and price of each such purchase and sale. Including aggregation and allocation of client orders (if applicable).
Securities Cross Reference	A record, by security, of any client invested in that security and the current amount invested.
Soft Dollars	Information related to compliance with Section 28(e) and appropriate treatment of mixed-use products, if any.

Advertising Records	
	A copy of each notice, circular, advertisement, newspaper article, investment letter, bulletin, or other communication that the Company circulates or distributes to any person, including copies of the Company's website.

	All accounts, books, internal working papers, and any other records or documents that are necessary to form the basis for, or demonstrate the calculation of, the performance or rate of return of any or all managed accounts or securities recommendations in any notice, circular, advertisement, newspaper article, investment letter, bulletin, or other communication that the Company circulates or distributes, directly or indirectly, to any person. With respect to the performance of managed accounts, the retention of all account statements, if they reflect all debits, credits, and other transactions in a client's account for the period of the statement, and all worksheets necessary to demonstrate the calculation of the performance or rate of return of all managed accounts shall be deemed to satisfy the requirements of this paragraph.

Registration Records	
IAR Registrations	Originals of Forms U4 for all IARs. This requirement may be satisfied by producing copies of such documents via the IARD.
Firm Registration/Notice Filings	Originals of Forms ADV and related documentation supporting the Company's registration.

Proxy Voting Records	
Policies and Procedures	The Company does not vote proxies.

Compliance Program Rule Records	
Policies and Procedures	A copy of the Company's policies and procedures that are in effect, or at any time within the past five years were in effect.
Annual Review	Any records documenting the Company's annual review of those policies and procedures.
Signed Acknowledgments	Associated Person signed acknowledgments of receipt and understanding of compliance policies initial and annually thereafter.
Associated Person Training	Evidence of compliance training, as needed.

Code of Ethics Rule Records	
Code of Ethics	A copy of the Company's code of ethics that is in effect, or at any time within the past five years was in effect.
Violation Record	A record of any violation of the code of ethics, and of any action taken as a result of the violation.
Written Acknowledgments	A record of all written acknowledgments for each person who is currently, or within the past five years was, a supervised person of the Company.
Access Person Reports	A record of each report (initial and annual holdings and quarterly transaction reports) made by an access person, including any information provided in lieu of such reports (i.e., duplicate account statements and/or confirmations).

Access Persons List	A list of the persons who are currently, or within the past five years were, access persons of the Company.
Decision Records	A record of any decision, and the reasons supporting the decision, to approve the acquisition of securities (IPOs or limited offerings) by access persons, for at least five years after the end of the fiscal year in which the approval is granted.
Insider Trading	Documentation related to Associated Persons in receipt of inside information and corrective actions taken by the Company.

Electronic Recordkeeping

The Company is permitted to maintain and preserve all records electronically. In addition to, or as a substitute for, storing documents in paper format, records required to be maintained and preserved on film, magnetic disk, tape, optical storage disk or other electronic storage medium. The Company must:

1. arrange and index the records in a manner that allows easy and prompt location, access, and retrieval of a particular record;
2. be able to produce a legible, true and complete printout of the record, or be able to project records (if held on microfiche);
3. store, for at least five years, a duplicate copy of the records; and
4. maintain procedures for maintenance, safekeeping, and access.

Upon request by a regulatory authority, the Company must be able to provide:

- A legible, true, and complete copy of the record in the format in which it is stored;
- A legible, true, and complete printout of the record; or
- The means to access, view, and print the records from the format in which they are stored.

The Company prohibits the access of electronic records by Associated Persons other than those who have a need to access such records in order to carry out or perform their duties as assigned by the Company.

Reliance on Third Parties for Recordkeeping

The Company may rely upon one or more third parties to create and retain certain of the records referred to above provided that it obtains an undertaking from the third party to provide a copy of the documents promptly upon request, and that the Company receives a vendor confidentiality agreement, if needed.

E-Mail Retention

E-mails that pertain to any advice or recommendations made, transactions executed, orders received, and any other communication with clients must be maintained. When storing e-mail communications, the Company will arrange and index such communication like any other electronically stored record. This will be done in such a manner that permits easy location, access, and retrieval. The Company will separately store a copy of these records as part of its Disaster Recovery Plan and establish procedures to reasonably safeguard e-mails from loss, alteration, or destruction and limit access to these records to properly authorized individuals.

The CCO will provide promptly any of the following, if requested by any regulatory authority:

1. A legible, true, and complete copy of an e-mail in the medium and format in which it is stored;
2. A legible, true, and complete printout of the e-mail; or
3. Means to access, view, and print the e-mail.

The Company will backup and archive client records, including e-mails on a Daily basis. The archive is maintained at an offsite location. All such correspondence will be kept for a period of not less than five years.

Corporate Records

Policy

As a registered investment adviser and legal entity, BCA has a duty to maintain accurate and current "Organization Documents." As a matter of policy, BCA maintains all Organization Documents, and related records at its principal office. All Organization Documents are maintained in a well-organized and current manner and reflect current directors, officers, members or partners, as appropriate. Our Organization Documents will be maintained for the life of the firm in a secure manner and location and for an additional three years after the termination of the firm.

Background

Organization Documents, depending on the legal form of an adviser, may include the following, among others:

- Articles of Incorporation, By-laws,
- Shareholder Agreements or other similar agreements
- Minute Books
- Stock certificate books/ledgers • organization resolutions
- Any changes or amendments of the Organization Documents

Responsibility

The Chief Compliance Officer has the responsibility for the implementation and monitoring of our Organization Documents policy, practices, and recordkeeping.

Procedure

BCA has adopted procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- BCA's Chief Compliance Officer, or designee(s), will maintain the Organization Documents in BCA's principal office in a secure location.
- Organization Documents will be maintained on a current and accurate basis and periodically reviewed and updated by the Chief Compliance Officer, or designee(s), so as to remain current and accurate with BCA's regulatory filings, among other things.

Correspondence

Background

Correspondence includes incoming and outgoing written and other communications to clients or prospective clients regardless of the method of transmission (mail, facsimile, personal delivery, courier services, electronic mail, etc.). Correspondence also includes portfolio seminars, panel presentations, speeches, and other types of information originated by an Associated Person of the Company and provided to one or more clients or prospective clients. Interactive conversations (e.g., personal meetings, telephone conversations, other than scripted sales calls, and posting to "chat rooms") generally are not considered correspondence. Advertising, sales literature, and market letters are not included in this definition of correspondence; rather, they are covered in Advertising Section of this Manual.

Policies and Procedures

Persons associated with the Company should use discretion in communicating information to clients and prospective clients. This policy applies to all communications used with existing or prospective clients, including information available in electronic format, such as a website.

The Company endeavors to ensure client communications are presented fairly, in a balanced manner, and that client communications are not misleading. In addition, the Company endeavors to disclose material facts to its clients.

Guidelines for Outgoing Correspondence

Associated Persons shall send and receive all correspondence at such locations and through such channels as are designated by the Company.

No Company related correspondence, including electronic correspondence, may be sent, or received through a personal address of an Associated Person without prior written approval of the CCO. The following are guidelines regarding outgoing correspondence:

1. Truthfulness and good taste shall be required;
2. Exaggerated or flamboyant language should be avoided;
3. Projections and predictions are never permitted except in accordance with the Company's policies regarding advertising;
4. The Company prohibits photocopying and distributing copyrighted material in violation of copyright law;
5. Use of the Company's letterhead and other official stationery is limited to Company-related matters;
6. No material marked "For Internal Use" or something to this effect may be sent to anyone outside the Company; and
7. No Associated Person is authorized to make any statements or supply any information about a security that is the subject of a securities offering other than the information contained in offering materials that have been approved for such offering. Violations of this policy can subject the Associated Person and the Company to severe civil and, in some cases, criminal liability.

Guidelines for Incoming Correspondence

1. Obvious non-client and non-legal correspondence may be forwarded directly to the addressee;
2. Complaints shall be immediately forwarded to the CCO; and
3. Original client correspondence shall be retained for the Company's files.

Complaints

Background

As part of a regulatory examination, the Company will be required to produce documentation of any client complaints, information about the process used to address the complaint, and the final resolution.

Policies and Procedures

It is the Company's policy to respond to client complaints promptly. All such information will be treated as confidential and will not be brought to the attention of any third party without the express permission of legal counsel or the CCO.

The Company defines a "complaint" as any written or oral statement of a client, or any person acting on behalf of a client, alleging inappropriate conduct involving the activities of the Company, and Associated Persons of the Company, or any person under the control of the Company in connection with the management of the client's account.

The CCO shall be responsible for handling all client complaints. All Associated Persons must promptly report the receipt of a written or oral complaint to the CCO, and provide the CCO with all information and documentation in their possession relating to such complaint. Failure to report a complaint is cause for corrective action, up to and including, dismissal.

Associated Persons must cooperate fully with the Company and with regulatory authorities and provide the CCO with all relevant information to assist with the investigation of any complaint.

The Company shall maintain a separate file for all written, oral, and electronically transmitted client complaints in its main office. Records maintained shall include the following information:

- Identification of each complaint;
- The date each complaint was received;
- Identification of each person servicing the account;
- A general description of the matter;
- Copies of all correspondence involving the complaint; and
- A written report of the action taken with respect to the complaint unless it is already included in a letter to the complainant.

Any offers of settlement, or actual settlements, may only be made with the approval of the CCO.

E-Mail & Other Electronic

The rapid expansion of the internet and other means of electronic communication present new challenges for investment advisers. Because of their prevalence and familiarity, it is easy to overlook the risks associated with an investment adviser's use of electronic communications.

As with other types of communications, electronic communications are subject to certain provisions of Federal Securities Laws, including the anti-fraud provisions of the Advisers Act, the protection of confidential client information pursuant to Regulation S-P, and record retention in accordance with Rule 204-2 under the Advisers Act. Furthermore, the use of the internet and other electronic communications may expose an investment adviser to disruptions caused by viruses or computer hackers.

All software, files, email messages, voice mail messages, computers, PDAs, computer networks, and communications systems (collectively, "electronic resources") are the property of the Company. Associated Persons' communications using electronic resources are held to the same standard as all other business communications. Associated Persons must act with good judgment, integrity, competence, dignity, and in an ethical manner when using electronic resources. Such resources may not be used to receive or transmit communications that are discriminatory, harassing, offensive, unlawful, or otherwise inappropriate.

Associated Persons may not attempt to gain unauthorized access to any computer or database, tamper with any electronic security mechanism, misrepresent a user's identity, disseminate viruses or other destructive programs, or download, install, or execute software without prior approval from the CCO.

Incoming and outgoing electronic communications are subject to the same review and retention policies as paper correspondence and communication. The Company's electronic communications systems should be used for authorized business purposes only. This policy extends to off-hour usage of electronic communications systems and where permitted, to communications concerning Company business on home, personal, or other electronic communications systems whether owned by the Company, the Associated Person or otherwise. As used in this policy, the term "electronic communications" includes, but is not necessarily limited to business communications made through any of the following media:

1. Telephone (including internet telephony devices and related protocols);
2. Electronic mail ("e-mail");
3. Instant messaging ("IM"), including private messaging applications or features within social networking platforms;
4. Social networking sites, such as Facebook, LinkedIn, Twitter, etc.;
5. Facsimile, including e-fax services;
6. The internet, file transfer protocols ("FTP"), Remote Host Access, blogs, etc.;
7. Video teleconferencing; and,
8. Internet Relay Chat ("IRC"), bulletin boards, and similar news or discussion groups.

The following summarizes the key points of the Company's electronic communications policy.

1. The Company's electronic communications systems are to be used for business purposes only;
2. Without the prior consent of the CCO, electronic communications with clients or the public concerning Company business are permitted only on Company communications systems;
3. Electronic communications are not private and may be monitored, reviewed, and recorded by the Company;
4. No Associated Person, other than specifically authorized personnel, is permitted to post anything on the Company's website; and
5. Without the pre-approval of the CCO, Associated Persons may not post or blog any information concerning the Company, its business, or clients to the internet (or similar third-party system), containing references to the Company, communications involving investment advice, references to investment-related issues or information or links to any of the aforementioned.

Dissemination of Client Information

Associated Persons may send information to clients and other parties (such as, brokers, custodians, and banks) electronically, being mindful of the requirements of keeping client information private as outlined within the Company's Privacy Policy.

Electronic Delivery of Regulatory Information

The Company or Associated Persons may electronically deliver disclosure documents such as disclosure brochures, brochure supplements, and privacy notices to clients and prospective clients as long as the following practices are followed:

1. **Consent, Notice and Access.** Obtain written consent for electronic delivery from the recipient and ensure that the recipient is given notice of electronic delivery and has access to the electronic information; and
2. **Evidence to Show Delivery.** The Company must have reason to believe that the electronically delivered information will result in the satisfaction of the delivery requirements under applicable securities laws. The Company will evidence satisfaction of its delivery obligations using either of the following methods:
    a. Ensuring clients have notice and access to such information and obtaining clients' informed consent to the electronic delivery of the information provided the informed consent specifies the electronic medium through which the information will be delivered, the period during which the consent will be effective, and describes the information that will be delivered; or,
    b. Obtaining evidence that the intended recipient actually received delivery of the document(s), such as a return receipt or documentation showing the information was accessed, downloaded, or printed.

Disclosure documents being delivered electronically should be sent as read-only PDF files or attachments. Every electronic communication should contain the Company's standard disclosures and should provide the recipient with guidance on how to discontinue receiving important documents electronically.

Emails, Instant Messages, and Faxes Sent to More Than One Person

The staff of the SEC would likely consider any email, instant message, or fax ("electronic communication") to be an advertisement if it is sent to more than one person other than an Associated Person, and if it offers:

- Any analysis, report, or publication concerning securities, or which is to be used in making any determination as to when to buy or sell any security, or which security to buy or sell;
- Any graph, chart, formula, or other device to be used in making any determination as to when to buy or sell any security, or which security to buy or sell; or
- Any other investment advisory service with regard to securities.

Electronic communications that are advertisements are subject to the *Advertising and Marketing* policies and procedures described in this Manual. Consult the CCO if there is any question as to whether an electronic communication is an advertisement under the Advisers Act.

Electronic Communications Surveillance

All electronic communications sent or received on the Company's electronic resources are property of the Company. The CCO is responsible for monitoring the electronic communications of the Company's Associated Persons. The CCO conducts such a review at least quarterly. Subject to applicable law, such electronic communications and electronic resources may also be searched, reviewed, or produced for any purposes by the Company, third-party contractors, the SEC, and other regulatory authorities.

Consent and compliance with the *Electronic Communications* policies and procedures, including the *Electronic Communications Surveillance* policies and procedures, is a term and condition of employment. Failure to abide by these policies may result in disciplinary action, including dismissal.

Consult the CCO if you are unsure about the application of the *Electronic Communications* policies and procedures.

Privileged Emails
All emails between the Company and legal counsel should include "Privileged and Confidential" in the subject line. Associated Persons should be aware that emails are not automatically protected by attorney-client privilege because they are marked "Privileged and Confidential," but this labeling convention will be useful if the Company must make a privilege claim.

Personal Emails
Associated Persons are strictly prohibited from using public email services (such as Hotmail or Gmail) for any business purpose.

Text Messaging
Associated Persons may not communicate with clients via text/SMS messaging regarding investment recommendations, specific products or services, investment performance, or for other business purposes.

Instant Messages and Chat Rooms
Associated Person participation in chat room discussions on the internet regarding the Company, its clients, or the Company's current or potential investments is strictly prohibited.

The Company Website
The SEC generally treats an investment adviser's website as an advertisement. Consequently, it is the Company's policy to control the content and its presentation on the website through the following procedures:

- Associated Persons may not make a material change, modification, addition or deletion to the content on the website, including the addition or deletion of links, without the express approval of the CCO or designee;
- All information placed on the website may be for informational purposes only. No information that constitutes an offer to sell or buy a security or a form of investment advice may be placed on the website. The website will contain a disclaimer making this representation;
- All content placed on the site shall be truthful and not misleading; and
- The website shall contain a section referenced on the home page that contains the website's terms and conditions of use by viewers.

The use of hyperlinks in the Company's website to third-party information has the potential of creating liability to the Company for the hyperlinked information. Accordingly, hyperlinks shall be posted only if the CCO or designee has concluded that the hyperlinked information is not misleading. The context of the hyperlinked information should not create an inference that the Company has approved or endorsed the hyperlinked information.

Electronic Security
The internet and other forms of electronic communication may not be secure. It may be possible for internet users to intercept emails, file attachments, and other data transmissions. When possible, Associated Persons should seek to limit the amount of confidential and proprietary information that is transmitted electronically.

If an Associated Person knows or suspects that one or more passwords, the Company's proprietary information, or nonpublic information about a client has been lost or improperly disclosed or accessed, that Associated Person must promptly report the loss or disclosure to the CCO. Similarly, Associated Persons must report any actual or suspected misuse of the Company's electronic resources to the CCO. Unusual system behavior, such as missing files, frequent crashes, or misrouted messages should also be reported to the CCO.

Associated Persons must be extremely cautious when addressing electronic communications because of the potential consequences of sending such communications to the wrong recipient. Associated Persons should use the same care when preparing an electronic communication that they would use when drafting a letter on the Company's letterhead. Associated Persons should double-check the recipient's email address or fax number before sending such communications. Internal documents, including those marked "For Internal Use Only," may not be transmitted to third parties except as authorized by the CCO.

If an Associated Person inadvertently sends an electronic communication to the wrong recipient, he or she must promptly report the incident to his or her supervisor, even if the consequences of the mistaken transmission appear minimal. The Associated Person and the supervisor should promptly notify the CCO if they determine that the mistaken transmission contained nonpublic information about a client, or material information that is proprietary to the Company.

Retaining Electronic Communications

The Company's policy is to retain all electronic communications that it sends and receives. Unsolicited advertisements (also known as "spam") received by the Company need not be retained. Faxes should be kept in the same filing systems that are used for letters. All emails are retained by Orlantech.

Proxy Voting/Class Action Litigation

Background

An investment adviser owes a duty of care and loyalty to its clients with respect to monitoring corporate events and exercising proxy authority in the best interests of such clients. The Company will adhere to Rule 206(4)-6 of the Advisers Act and applicable laws and regulations in regard to the voting of proxies. As a result, investment advisers must conduct a reasonable review into matters on which the adviser votes and to vote in the best interest of the client.

Policies and Procedures

The Company does not vote proxies on behalf of clients. All proxy materials received on behalf of a client account are to be sent directly to the client or to a designated representative of the client, who is responsible for voting the proxy. Company personnel may answer client questions regarding proxy-voting matters in an effort to assist the client in determining how to vote the proxy. However, the final decision of how to vote the proxy rests with the client.

Class Action Lawsuits

From time to time, securities held in the accounts of clients will be the subject of class action lawsuits. The Company has no obligation to determine if securities held by the client are subject to a pending or resolved class action lawsuit. It also has no duty to evaluate a client's eligibility or to submit a claim to participate in the proceeds of a securities class action settlement or verdict. Furthermore, the Company has no obligation or responsibility to initiate litigation to recover damages on behalf of clients who may have been injured because of actions, misconduct, or negligence by corporate management of issuers whose securities are held by clients.

Where the Company receives written or electronic notice of a class action lawsuit, settlement, or verdict directly relating to a client account, it will forward all notices, proof of claim forms, and other materials, to the client. Electronic mail is acceptable where appropriate if the client has authorized contact in this manner.

Portfolio Management

Background

As part of its fiduciary duty to clients, an investment adviser must have a reasonable basis to believe that its investment recommendations are suitable. Advisers must act with prudence and exercise due care throughout the portfolio management process. Investment advisers also have a duty to periodically review accounts under management to ensure that such accounts are invested consistently with clients' mandates and the investment advisers' disclosures. Moreover, investment advisers must allocate investment opportunities in a manner that is fair to all clients.

Policies and Procedures

Investment Discretion

Subject to a grant of discretionary authority, the Company shall invest and reinvest the securities, cash, or other property held in the client's account in accordance with the client's stated investment objectives as identified by the client during initial interviews and information gathering sessions. The Company is granted discretion pursuant to authorization provided in the executed agreement for services which is maintained in the relevant client file.

We recommend asset allocation strategies and Portfolio Managers that we believe will meet specific objectives rather than recommending specific securities. The Portfolio Managers (PM) will perform the actual security analysis.

BCA's recommendations may vary depending upon each client's specific financial situation and the limitations imposed by the client or applicable law. As such, we determine allocations based upon clients' predefined objectives, risk tolerance, time horizon, financial horizon, financial information, liquidity needs, and other various suitability factors. Clients' restrictions and guidelines may affect the composition of your portfolio.

We do not perform quantitative or qualitative analysis of individual securities. Instead, we will advise clients on how to allocate assets among various classes of securities or portfolio managers. We may recommend replacing the PM if there is a significant deviation in characteristics or performance from the stated strategy and/or benchmark.

Our strategies and investments may have unique and significant tax implications. However, unless we specifically agree otherwise, and in writing, tax efficiency is not our primary consideration.

Monitoring Investment Mandates and Restrictions

Client accounts managed by the Company are subject to investment restrictions or limitations described in client contracts or account opening documents. It is the CCO's role to ensure that investments are made consistent with client limitations or restrictions. Client accounts are reviewed by the CCO.

We will monitor accounts on a periodic basis and will conduct account reviews utilizing a team approach at least annually. Additional reviews may be conducted based on various circumstances, including, but not limited to:

- contributions and withdrawals
- market moving events
- security specific events, and/or
- changes in your risk/return objectives

- asset rebalancing recommendations
- new asset classes
- Portfolio Manager (PM) searches

We will provide clients with additional or regular written reports in conjunction with account reviews. Reports we provide will contain relevant account and/or market-related information including account performance and compliance monitoring.

Allocation Policy (Side-by-Side Management)

In the event that a new limited investment opportunity, such as an IPO, is equally suitable for and satisfies the investment objectives of more than one client, the Company shall allocate such opportunity in a fair, equitable and unbiased manner. In allocating limited investment opportunities, the Company shall not favor proprietary accounts or performance-based accounts over other client accounts. Each limited investment opportunity shall be reviewed by the CCO for compliance with this policy and documentation maintained to support allocation decisions.

Third-Party Adviser Initial Due Diligence

The Company will refer and/or recommend the services of third-party advisers to clients for account/portfolio management services. Prior to utilizing any third-party adviser the Company will conduct a due diligence review of the third-party adviser. Due diligence may consist of the following:

1. Reviewing Form ADV or other disclosure documents;
2. Reviewing the third-party adviser's qualifications, expertise, and strategies;
3. Conducting in person or telephonic interviews with the third-party adviser;
4. Confirming the registration status of the third-party adviser;
5. Requesting and reviewing any disciplinary/regulatory history of the third-party adviser and all persons associated with the third-party adviser;
6. Requesting and reviewing any regulatory examination deficiency letters and responses thereto;
7. Requesting any reviewing any internal and/or external compliance audit reports and responses thereto;
8. Requesting and reviewing the third-party advisers policies and procedures;
9. Requesting any client complaints regarding the third-party adviser; and
10. Reviewing the third-party adviser's custodial relationships.

On Going Due Diligence and Supervision of Third-Party Advisers

The Company's CCO, senior management, and/or investment committee (if any) will be responsible for supervising and conducting on-going due diligence of any third-party adviser utilized by the Company. This will be accomplished through some or all of the following:

1. Obtaining an annual certification of compliance with the third-party adviser's policies and procedures;
2. Requesting and reviewing amendments to the third-party adviser's Form ADV or other disclosure documents;
3. Reviewing the performance of the third-party adviser;
4. Conducting periodic meetings with compliance personnel and senior management of the third-party adviser;
5. Requiring notification of changes in the third-party adviser's portfolio management team or investment strategies;
6. Obtaining and reviewing copies of any complaints, and pending and/or threatened litigation;
7. Obtaining and reviewing any internal and/or external compliance audit reports and responses thereto;
8. Requiring the third-party adviser to provide copies of any regulatory deficiency letters and

responses thereto and follow-up on any items of concern; and

9. Periodically reassess supervisory procedures applicable to the third-party adviser in light of:
    a. Changes in a third-party adviser's investment strategy or portfolio managers;
    b. Significant changes in the third-party adviser's business;
    c. Dramatic changes in market conditions; or,
    d. Any other event likely to have a significant effect on the third-party adviser's operations.

Once all information has been collected, the Company will review the materials and determine if the Company will refer and/or recommend the third-party adviser to clients. Records of the review and a final decision will be maintained in the Company's compliance files.

The Company provides:

- **Consulting Services**
- **Recommendation of Portfolio Managers (PM)**
- **Discretionary Portfolio Management**

We offer discretionary and non-discretionary consulting and advisory services to individuals, pension and profit sharing plans, trusts, estates, charitable organizations, corporations, and other business and governmental entities.

Refer to the *Oversight of Service Providers* section of this Manual for additional policies.

Cash Payment for Client Solicitation

Background

A "solicitor" is generally defined as any individual, person, or entity who, directly, or indirectly receives compensation, for soliciting, referring, offering, or otherwise negotiating for the sale of investment advisory services to clients on behalf of an investment adviser. Solicitation arrangements can arise in several situations, including if the Company were to agree to split a portion of its fees with another investment adviser who refers clients or make cash payments to Associated Persons who introduce clients.

Rule 206(4)-3 under the Advisers Act specifically prohibits a registered investment adviser from directly or indirectly paying a cash fee to a person who solicits on behalf of the investment adviser unless there is a written agreement in place, the solicitor provides appropriate disclosure of the compensation they receive, and the solicitor is supervised by the investment adviser as if the solicitor were an associated person of the Company.

Separately, the SEC adopted a "pay-to-play" rule, Rule 206(4)-5 in 2010 which prohibits the investment adviser (whether registered or not) from paying a third-party placement agent or solicitor to solicit a government entity, unless such solicitor is a "regulated person" subject to comparable "pay-to-play" restrictions as are contained in the rule itself. Please refer to the Company's policy on Political and Charitable Contributions, and Public Positions for a summary of those restrictions as they relate to the Company and any third-party solicitor.

Policies and Procedures

It is the Company's policy to not compensate, either directly or indirectly, any person (individual or entity) for client referrals or the development of new advisory business. A "solicitor" is generally defined as any individual, person or entity who, directly or indirectly, receives compensation for soliciting, referring, offering, or otherwise negotiating for the sale investment advisory services to clients on behalf of an investment adviser.

If required by any state rules and regulations, the Company will also ensure that any person (individual or entity) acting as a solicitor is properly registered as an IAR of the Company or separately as a registered investment adviser prior to receiving solicitor's compensation. When making assessments on registration requirements, the Company will evaluate whether the solicitor's activities may exceed the scope of those included in the definition above. Any activities beyond those mentioned above, as well as acting as a solicitor for more than one investment adviser, may be deemed as personal advisory services and would subject the solicitor to normal investment advisory (representative) registration requirements.

The Company understands that it has an affirmative duty to ensure it takes necessary steps to comply with SEC Rule 206(4)-3 or relevant state law, and the terms of a Written Solicitor's Agreement, should it decide to enter into such arrangements in the future. Moreover, the Company understands that it should be able to demonstrate what steps it has taken to verify compliance with the rule.

No solicitation arrangement may be entered into without the express written approval of the CCO. In no event shall a solicitation arrangement be entered into verbally. Such arrangements will not be honored and no payments will be made thereunder.

Directed Brokerage

Background

Pursuant to SEC interpretations of the Investment Advisers Act of 1940, an investment adviser has a fiduciary obligation to seek "best execution" of clients' transactions under the circumstances of the particular transaction. The investment adviser must consider the full range and quality of the broker's services in placing a trade with that broker, including, among other things, the value of research provided as well as execution capability, commission rate, financial responsibility, and responsiveness to the investment adviser. The determinative factor is not necessarily the lowest possible commission cost but whether the transaction represents the best qualitative execution for the managed account.

Policies and Procedures

The Company may engage in various types of permitted activities, as discussed herein related to trading client accounts. In all cases, these activities will be disclosed in the Company's Form ADV Part 2A Disclosure Brochure.

Best Execution

Pursuant to SEC interpretations of the Investment Advisers Act of 1940, an investment adviser has a fiduciary obligation to seek to obtain "best execution" of clients' transactions under the circumstances of the particular transaction. The investment adviser must consider the full range and quality of the broker's services in placing a trade with that broker, including, among other things, the value of research provided as well as execution capability, commission rate, financial responsibility, and responsiveness to the investment adviser. The determinative factor is not necessarily the lowest possible commission cost but whether the transaction represents the best qualitative execution for the managed account.

As a registered investment adviser, the Company recognizes its fiduciary obligation to seek best execution of clients' transactions. Best execution has been defined as the "execution of securities transactions for clients in such a manner that the clients' total cost or proceeds in each transaction is the most favorable under the circumstances." The best execution responsibility applies to the circumstances of each particular transaction and an investment adviser must consider the full range and quality of a broker-dealer's services, including execution capability, commission rates, value of research, and financial responsibility and responsiveness, among other things.

The CCO will evaluate the quality and cost of services received from broker/dealers on a periodic basis (at least annually). As part of the evaluations, the Company will consider the quality and cost of services available from alternative broker/dealers. In addition, consideration will be given to time and cost of changing broker-dealers (cost/benefit) and the impact on clients.

Mutual Fund Share Classes

Mutual funds are sold with different share classes. Share classes are described in the mutual fund's prospectus. Generally, mutual funds will only be purchased at net asset value when that fund is available at net asset value to the client. In all cases, the Company shall conduct an initial assessment prior to purchase to determine whether clients are purchasing the most beneficial mutual fund share classes available. As a fiduciary, the assigned IAR shall conduct an initial share class assessment when a mutual fund is purchased, a new advised account is opened with mutual funds in the account, or upon receipt of mutual funds into the client's advised account. The assigned IAR shall convert when available mutual fund share classes to more beneficial share classes. Note: due to contingent deferred sale charges (CDSC), also known as back-end sales loads, it may not be in the client's best interest to liquidate mutual funds with such charges. Conversely, from time to time, some mutual fund companies may allow for the free exchange of one share class to another less expensive share class. Thus, the Company shall conduct a periodic review and convert when available mutual fund share classes to more beneficial share classes. The receipt by the Company (or an affiliate) of any 12b-1 fees related to mutual fund investments held by the Company's clients must be disclosed to clients and to plan fiduciaries under ERISA.

Disclosure

The brokerage practices of the Company will be fully disclosed in the Company's Form ADV Part 2, including a summary of factors the Company considers when selecting broker-dealers and determining the reasonableness of their commissions.

Conflicts of Interests

The Company will be sensitive to various conflicts of interest that may arise when selecting broker-dealers to execute client trades, and where necessary, it shall address such conflicts by disclosure.

Valuation

Background

An investment adviser's performance and fee calculations are dependent upon the prices assigned to assets held in client accounts. Clients need to know the fair value of their holdings and that they can be harmed if the investment adviser overcharges its advisory fee based on overvalued holdings.

Securities that are frequently traded on public exchanges, such as large cap domestic equities, are relatively easy to price. However, the valuation of assets for which there is no readily available pricing information is a highly judgmental process. An investment adviser should adopt and implement policies and procedures that are reasonably designed to price investments in a manner that is fair, accurate, and consistent with any disclosures. Particular attention should be paid when pricing structured products, illiquid securities, or other difficult-to-price securities.

Policies and Procedures

Assets with for which market quotations are readily available shall be valued at current market value. Other assets shall be valued at fair value.

Fair Valuation of Non-marketable Assets

The valuation of non-marketable investments is a highly judgmental process which cannot be reduced to a simple formula. Such valuations are determined based upon factors deemed most relevant and appropriate by the Company. These factors include, but are not limited to, market conditions, purchase price, estimated liquidation value, meaningful third-party transactions in the private market, and/or third party assessments.

Fair value is generally defined as the price that would be received in the sale of an asset or paid to transfer a liability in an orderly transaction between market participants under current market conditions. The Financial Accounting Standard Board's Accounting Standards Codification ("ASC") 820-10 provides guidance regarding appropriate valuation methodologies for fair valuing assets. ASC 820-10 recommends the following levels of factors that should be considered in descending order of importance:

- Level 1: Quoted prices available in active markets for identical assets;
- Level 2: Other observable factors, including, but not limited to: quoted prices for similar assets in markets that are active, quoted prices for identical or similar assets in markets that are not active, factors other than quoted prices that are observable for the assets;
- Level 3: Unobservable factors.

No matter which valuation method is used, the fair value of an asset should be the price at which it could be acquired or sold in a current transaction between willing parties in which the parties each acted knowledgeably, prudently, and without compulsion. Fair value should not be based on what can be obtained from an immediate "fire sale" disposition, nor on what a buyer might pay at some later time or under more favorable circumstances.

Valuation Process for Non-Marketable Assets

The Company's policy is to ensure that all portfolio investments are recorded at fair value on a consistent, transparent, and reasonable basis. The CCO will be responsible for determining the fair value of the client assets consistent with any applicable provisions specified in the written agreement(s). The CCO will choose the appropriate valuation method based on the facts and circumstances of each particular investment. In addition, the Company may engage independent third parties to provide assessed market value of certain assets.

Valuation Books and Records

The CCO is responsible for ensuring that documentation is maintained relating to valuations, including the basis for the methodology used and all relevant backup information.

The CCO is responsible for ensuring that valuations are performed in accordance with this policy. The CCO shall ensure that valuations are conducted by personnel with appropriate experience and sophistication, and that there is an appropriate level of independence in the pricing process.

ERISA

Background

The Employee Retirement Income Security Act of 1974 ("ERISA") concerns the establishment, operation, and administration of employee benefit plans. ERISA sets standards for fiduciaries of such plans, and prohibits certain transactions that may involve conflicts of interest. ERISA is administered and enforced by the U.S. Department of Labor.

ERISA contains a number of provisions affecting investment advisers engaged in managing or providing other advisory activities with respect to ERISA accounts. ERISA rules and regulations are quite complex and in cases of uncertainty Company personnel should seek expert advice before engaging in business dealings or signing contracts. The following paragraphs address major compliance issues deriving from the ERISA statute and rules, as they may apply to the Company's business. Importantly, many of the provisions of ERISA are also applicable to IRAs and certain other accounts that are not subject to ERISA but that are subject to similar rules set forth in the Internal Revenue Code ("IRC"). References to "ERISA Clients" or "ERISA Plans" should be read to include IRAs and other similar retirement accounts.

Policies and Procedures

The Company may provide advisory services to clients that are governed by ERISA. It is the Company's policy to comply with all provisions of ERISA and the IRC when providing services to such accounts.

The Company has adopted the following procedures specific to client accounts that are governed by ERISA:

1. On-going awareness and periodic reviews of an ERISA client's investments and portfolio for consistency with the "prudent man rule";
2. On-going awareness and periodic review of any client's written investment policy statement and/or guidelines so as to be current and reflect a client's objectives and guidelines;
3. Verification that the plan fiduciaries have established and maintain and renew, on a periodic basis any ERISA bonding that may be required; or if plan documents require the investment manager to maintain required ERISA bonding, the Company will ensure that such bonding is obtained and renewed on a timely basis; and
4. Identify and monitor any party in interest affiliations or relationships existing between the Company and any client ERISA plans to avoid any prohibited transactions.

In providing such services, the Company will obtain due diligence materials or representations from persons acting on behalf of the ERISA plan that:

1. Identify who is responsible for administering the plan;
2. Identify who is the plan's trustee and/or "named fiduciary;"
3. Verify that the plan official engaging the Company has the requisite authority to engage the Company for the proposed engagement; and
4. Identify all stated objectives and restrictions governing the plan account.

The term "Financial Advisor" as used within these ERISA Considerations policies and procedures refers to Associated Persons who render investment advice to retirement plan clients on behalf of the Company.

Plan Fiduciary

The Company becomes a "plan fiduciary" subject to ERISA rules where it exercises any authority or control with respect to managing plan assets or renders investment advice for a fee or other compensation, direct or indirect, with respect to any plan assets or has any authority to do so. "Plan assets" include assets held in separate employee accounts under "404(c)" plans (see below). Plan fiduciary status is significant because of the liabilities attached. There may be more than one plan fiduciary of an ERISA plan. With limited exceptions, every plan fiduciary is personally jointly and severally liable for any violation of the ERISA statute and rules by every other plan fiduciary. Also, plan fiduciaries are subject to an elaborate set of "prohibited transaction" rules barring certain types of transactions, including but not limited to transactions between the plan fiduciary and the plan. While many managers cannot avoid plan fiduciary status because of the discretion they have over plan assets, many investment advisers who are non-discretionary service providers to plans make an effort to avoid plan fiduciary status because of the liability consequences that attach to this status and the application to them of the prohibited transaction rules.

Since its inception, ERISA has had a "safe harbor" for so-called "404(c)" Plans that are plans that are intended to permit employee/participant direction of investment of their own accounts. Section 404(c) of ERISA provides that other fiduciaries are not liable for losses that result from participant investment direction if certain conditions are met. These include an announcement by the plan sponsor of the plan's status as a 404(c) plan and the plan having at least three (3) investment options with materially different risk/return profiles.

Additionally, DOL regulations allow a plan to offer participants an "ERISA Covered default investment alternative" in which participant assets may be invested if the participant does not make an affirmative investment election. The ERISA Covered default investment alternative must be one of a combination of:

1. Age-based life cycle or targeted retirement date funds or accounts;
2. Risk-based balanced funds; or
3. An investment management service.

The plan sponsor may engage a "fiduciary adviser" to provide an "eligible investment advice arrangement" to plan participants, without violating the prohibited transaction rules (see exemption sub-section below). The sponsor must exercise a fiduciary level of prudence in picking and monitoring the fiduciary adviser and the eligible investment advice arrangement. Once this is done, the sponsor can then invoke the safe harbor and avoid liability for management decisions made with respect to plan assets.

Fiduciary Adviser

A "fiduciary adviser" is a person who is a fiduciary of the plan by reason of the provision of investment advice to a participant or beneficiary. This is different from an "investment fiduciary" who provides advice only to the plan sponsors or investment committee.

Definition of ERISA Covered Account

Subject to certain exceptions, an ERISA Covered Account will generally include any private sector ERISA Covered retirement plan sponsored by an employer or a union or both. IRAs are not subject to ERISA but should be treated as ERISA plans for most purposes. For purposes of these policies and procedures, the following types of client accounts will be considered ERISA Covered Accounts:

1. IRAs, such as Traditional IRAs, Roth IRAs, inherited IRAs, rollover IRAs, Simplified Employee Pension ("SEP") IRAs, Savings Incentive Match Plan for Employees ("SIMPLE") IRAs, and Salary Reduction Simplified Employee Pension ("SARSEP") IRAs;

2. Archer Medical Savings Accounts;
3. Health Savings Accounts ("HSA"s);
4. Coverdell Educational Savings Accounts;
5. Tax-ERISA Covered benefit plans sponsored by employers that cover their employees and that are subject to ERISA (ERISA Plans), such as defined benefit pension plans and defined contribution plans;
6. Individual participant accounts under any ERISA Plan that is a defined contribution plan, such as an ERISA 403(b) or 401(k) plan, for which the client is the beneficial owner; and
7. Tax-ERISA Covered benefit plans that do not cover any employees, which therefore are not subject to Title I of ERISA (Non-ERISA Plans), such as Keogh plans and solo 401(k) plans maintained by sole proprietors.

Fiduciary Obligations

Where the Company provides services to ERISA Covered Accounts in a fiduciary capacity, the Company and its advisory representatives must:

1. act solely in the interest of the participants and their beneficiaries;
2. use any fees received, directly or indirectly, in connection with transactions involving plan assets (i.e., 12b-1 fees) initiated at the discretion or upon the recommendation of the fiduciary adviser for the benefit of the plan (i.e., to offset other plan expenses such as investment adviser fees);
3. act with the care, skill, prudence and diligence that a prudent man would use in the same situation;
4. diversify plan investments to reduce the risk of large losses unless it is clearly prudent not to do so; and
5. act according to the terms of the plan documents, to the extent the documents are consistent with ERISA.

Eligible Investment Advice Arrangement Exemption

An "eligible investment advice arrangement" is an arrangement (1) which either (a) provides for "fee leveling," whereby any fees (including any commission or compensation) received by the fiduciary adviser for investment advice or with respect to an investment transaction with respect to plan assets do not vary depending on the basis of any investment option selected, or (b) uses a computer model under an investment advice program for participants or beneficiaries. In addition (2) the arrangement must be expressly authorized by a plan fiduciary other than the person offering the investment advice program, any person providing investment options under the plan, or any affiliate; (3) an annual audit of the arrangement must be conducted by an independent auditor hired by the plan fiduciary (with deficiencies reported to the DOL); (4) the plan fiduciary must provide a detailed written disclosure statement to participants and beneficiaries containing the items required by the Rule and (5) all records must be maintained by the fiduciary adviser for six (6) years after the provision of the investment advice.

Investment Policy Statement

Generally, ERISA plans may have adopted an Investment Policy Statement which:

1. defines the purpose of the plan;
2. describes suitability; and,
3. establishes risk parameters, return requirements, and portfolio diversification standards.

The CCO or the relevant portfolio manager of the Company should review and be familiar with the Investment Policy Statement of any ERISA plan for which the Company acts as an investment adviser.

Fidelity Bond

ERISA Section 412 generally requires investment advisers with discretion over plan assets to ensure that a fiduciary bond is in place to protect the plan against loss from acts of fraud or dishonesty. If the Company renders investment advice to an ERISA plan, but does not have discretionary authority, typically it is not required to be bonded solely because it provides investment advice. A fidelity bond is only required where the Company has discretion, or has the power to exercise physical contact or control over the assets and the power to transfer to itself or a third party, or to negotiate the assets for value on behalf of the plan.

Amount and Terms

Generally, the bond must be for not less than 10 percent of the funds handled, subject to a minimum of $1,000 and a maximum of $500,000 ($1,000,000 if the plan holds securities issued by the plan sponsor). The fidelity bond cannot have a deductible, and each ERISA plan must be named as an insured party under the bond. Alternatively, if permitted by the ERISA plan sponsor, the Company should seek to obtain the necessary coverage under the employer's bond.

Dual Fees

ERISA rules prohibit an investment adviser to an ERISA plan from imposing a dual fee or otherwise using its power as a fiduciary to cause a plan to pay an additional fee to the investment adviser or an affiliate of the investment adviser. Among other things, this generally prohibits the Company from receiving commissions or mutual fund "trails" from ERISA plan assets where the Company is also receiving an advisory fee. However, ERISA Prohibited Transaction Exemption 77-4 permits a pension fund adviser to invest ERISA plan assets in an investment company it sponsors only under specific conditions described therein.

Self-Dealing

ERISA plan fiduciaries are prohibited under Section 406(b) of ERISA from participating in any self-dealing transactions. Under this rule, the Company may not, while acting as a fiduciary:

1. Handle any transaction involving plan assets for its own account (including dual fees, discussed above);
2. Represent any party in any transaction involving plan assets where the party's interests are adverse to the interests of the plan or its beneficiaries (including, for example, cross-trades); or
3. Receive any personal compensation from any party in connection with a transaction involving plan assets (which could include trails or third-party commissions).

Prohibited Transactions

ERISA Section 406(a) discusses certain prohibited transactions between ERISA plans and parties with a relationship to the plan, including the plan's sponsor, fiduciaries, service providers, and their affiliates. This section prohibits a plan from:

1. Engaging in any sale or exchange of assets between a party in interest and the plan;
2. Involvement in any loan or extension of credit between a party in interest and the plan;
3. Furnishing goods, services, or facilities between a party in interest and the plan; or,
4. Transferring of any plan assets to a party in interest.

There are statutory and regulatory exemptions for many routine transactions but these exemptions apply only if all of the conditions of the relevant exemption are satisfied. It is usually advisable to consult with ERISA Covered counsel to determine whether an exemption is available and how to satisfy the conditions of the exemption.

Liability for Breach of ERISA Rules

If a plan fiduciary breaches its fiduciary duty or any of the prohibited transaction rules, it becomes liable to the plan for any resulting losses including lost profits. The breaching fiduciary may be removed from its fiduciary role or subjected to other appropriate equitable or other remedies.

Additionally, a plan fiduciary may be held JOINTLY AND SEVERALLY LIABLE to the plan for breach by any other plan fiduciary.

Great care must be taken to identify when the Company is acting as a plan fiduciary with respect to any ERISA client or account. In cases where the Company has discretionary control over any assets of an ERISA plan, the Company and its Financial Advisors must ensure that contract provisions are clear and fully explained and understood by plan executives/trustees:

- To provide prudent advice;
- To charge reasonable fees and only fees approved by the ERISA client;
- To disclose and obtain client "sign off" on all conflicts of interest;
- To avoid engaging in prohibited transactions or ensuring that all of the conditions of any applicable exemption are satisfied.

ERISA Regulations

Due to the complicated regulations under ERISA and the IRC, prior to rendering investment advice to an account governed by ERISA and/or the IRC, each IAR must consult with the CCO who shall be responsible for approving the arrangement and, if necessary, consulting with legal counsel.

Registration

Background

Money managers, investment consultants, and financial planners are regulated in the United States as "investment advisers" under the Advisers Act or similar state statutes.

Policies and Procedures

The Company and all Associated Person providing investment advisory services on its behalf shall maintain active registration(s) unless a valid exemption exists.

It is the responsibility of the CCO to be aware of the particular requirements of the states in which the Company operates and to ensure that the Company and its IARs are properly registered, licensed, and/or qualified to conduct business.

State Notice Filing/Registration Requirements

The Company is registered as an investment adviser with the Securities and Exchange Commission ("SEC") and has "notice" filed in states where it believes such filings are required. Unless otherwise permitted by regulation, the Company may not solicit or render investment advice for clients domiciled in a state where the Company is not properly notice filed.

In general, a notice filing is required in a state where the Company:

i. has a place of business;
ii. holds itself out as an investment adviser;
iii. has more than five clients (the statutory minimum varies from state-to-state); or
iv. has IARs with a place of business in that state.

Currently Louisiana, New Hampshire, Nebraska, and Texas do not recognize a statutory minimum; therefore, the Company must notice file in these jurisdictions prior to engaging in advisory services.

Registration of Investment Adviser Representatives

Investment Adviser Representatives ("IARs") refers to Associated Persons who provide investment advisory services on the Company's behalf and are required to be registered in the state(s) where they provide such services. Regardless of whether the Company is SEC or state registered, a state may require IAR registration before services can be offered by the IAR in that specific jurisdiction.

IAR qualifications may vary from state to state, but generally most states require the successful completion of the Series 65 examination, or the combination of the Series 7 *and* Series 66 examinations. For individuals who have not taken and passed the required exam(s) within two years of their application date, most states will require prior registration with an investment advisory firm within two years of the application date.

Most states provide examination waivers or exemptions for individuals holding active professional designations, such as a CFP®, CFA, ChFC, CIC, or PFS. Some states also provide examination waivers for applicants with specific experience in the financial industry.

Persons associated with the Company may not provide investment advice to a client until they receive notice from the CCO or their designee that they have been granted (if required) an IAR registration/approval from the relevant state(s). Currently, Texas requires IAR registration regardless of whether the Company maintains a place of business in that state.

The CCO shall ensure that all Associated Persons requiring registration as an "IAR" are appropriately registered, via Form U4 application.

Registration Amendments

All information reported on an individual's Form U4 must be kept up to date. Each IAR must notify the CCO in writing within 30 days of information required on the Form U4 becoming inaccurate or outdated. If the Form U4 is inaccurate, the CCO or designee will file an amendment to the IAR's Form U4 with the appropriate jurisdiction(s) via the IARD.

On an annual basis, the CCO or designee will distribute a copy of the Form U4 to each IAR for their review. The CCO is responsible for ensuring updates are made to Form U4, and as applicable, the IAR's Form ADV Part 2B Brochure Supplement.

Annual Renewal

The Company must file an annual renewal and pay applicable registration/filing fees each calendar year through the IARD. The CCO is responsible for ensuring the continuity of the Company's registration/filing status.

In addition, the CCO is also responsible for ensuring the proper renewal of each of the Company's IARs' registrations on an annual basis.

Filing Fees

The state(s) in which the Company is notice filed and IARS are registered may charge fees which will be deducted from the IARD account established with FINRA. The CCO will be responsible for maintaining sufficient funds with FINRA to facilitate the payment of registration fees for the Company and its IARs, as well as annual renewal fees when they are due.

Withdrawal from SEC Registration

If the Company reports regulatory assets under management of less than $90 million on its annual updating amendment, the Company shall withdraw from registration with the SEC by filing the Form ADV-W electronically through the IARD within 180 days of the Company's fiscal year end; unless, the Company can rely on another exemption for purposes of maintaining its federal registration (e.g. registered investment advisers with at least $25 million in regulatory assets under management, whose principal place of business is in New York, may remain registered with the SEC). The withdrawal will be effective immediately upon filing.

If the Company is continuing business as a state-registered investment adviser, the Form ADV-W will permit the Company to request "partial withdrawal." Here, the ADV-W should not be filed until the Company has been approved/granted registration with any state(s) in which the Company conducts investment advisory services and registration is required.

Regulatory Reporting

It is the Company's policy to fully cooperate with any inspection or investigation conducted by the SEC or any other federal or state regulatory authority, or self-regulatory organization with proper jurisdiction. The Company's CCO is responsible for managing regulatory inspections. The CCO may engage counsel or outside consulting assistance to advise on matters related to regulatory inspections or other compliance matters.

The Company is subject to a regulatory inspection at any time. Accordingly, all activities must be conducted on a daily basis in accordance with this Compliance Manual to assure ongoing regulatory compliance. Upon receiving word that an SEC or state regulatory agency intends to inspect the Company, or arrives at the home office location unannounced, the following procedures must be followed:

1. The CCO must be notified immediately (a Principal of the Company or other designee should be notified if the CCO is not available).
    a. The CCO (or other designee) will be the contact person during the inspection.
2. Inspector identification must be provided (a business card is insufficient). Before any document or information is shared with any regulatory authority, the following must be established:
    a. A photo ID must be presented to the CCO or designee for validation;
    b. No documents or office access shall be provided unless the CCO or designee is present; and
    c. If the CCO is, or will be, unavailable at the time of the audit the Company should request a date change.
3. The CCO will coordinate document delivery.
4. The Company will document the records and files provided to the inspector(s).
5. The Company will provide adequate working space for the examiners.
6. Company personnel must maintain respect and professionalism when dealing with examiners.
7. The CCO should check in with the examiners periodically throughout the day to inquire how the exam is proceeding.
    a. Notes should be taken documenting all discussions with the examiners.
8. An exit interview should be requested before the examiners complete the inspection.

Investment Processes

Policy

As a registered adviser, and as a fiduciary to our advisory clients, BCA is required, and as a matter of policy, obtains background information as to each client's financial circumstances, investment objectives, investment restrictions and risk tolerance, among many other things, and provides its advisory services consistent with the client's objectives, etc. based on the information provided by each client.

Background

The U.S. Supreme Court has held that Section 206 (Prohibited Activities) of the Investment Advisers Act imposes a fiduciary duty on investment advisers by operation of law.

Also, the SEC has indicated that an adviser has a duty, among other things, to ensure that its investment advice is suitable to the client's objectives, needs and circumstances.

Every fiduciary has the duty and a responsibility to act in the utmost good faith and in the best interests of the client and to always place the client's interests first and foremost.

As part of this duty, a fiduciary and an adviser with such duties, must eliminate conflicts of interest, whether actual or potential, or make full and fair disclosure of all material facts of any conflicts so a client, or prospective client, may make an informed decision in each particular circumstance.

Responsibility

The firm's advisory professional's responsible for the particular client relationship have the primary responsibility for determining and knowing each client's circumstances and monitoring the management the client's portfolio consistent with the client's objectives. BCA's President has the overall responsibility for the implementation and monitoring the performance of our client's investment managers and their investment policy and performance.

Procedure

BCA has adopted procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- BCA's Advisory Professionals obtain substantial background information about each client's financial circumstances, investment objectives, and risk tolerance, among other things, through an in-depth interview and information gathering process which includes client profile or relationship forms.
- Advisory clients may also have and provide written investment policy statements or written investment guidelines that the firm reviews, approves, and monitors as part of the firm's advisory services, subject to any written revisions or updates received from a client.
- BCA provides the firm's Form ADV Part 2 (Brochure) to all prospective clients which discloses the firm's advisory services, fees, conflicts of interest and portfolio and/or supervisory reviews and investment reports provided by the firm to clients.
- BCA may provide periodic reports to advisory clients which include important information about a client's financial situation, portfolio holdings, values and transactions, among other things. The firm may also provide performance information to advisory clients about the client's performance, which may also include a reference to a relevant market index or benchmark.
- Advisory professionals may also schedule client meetings on a periodic basis, or request basis, to review a client's portfolio, performance, market conditions, financial circumstances, and investment objectives, among other things, to confirm the firm's investment decisions and services are consistent with the client's objectives and goals. Documentation of such reviews should be made in the client file.
- Client relationships and/or portfolios may be reviewed on a more formal basis on a quarterly or other periodic basis as designated by the President and/or other supervisors of advisory professionals

Performance

Policy
BCA, as a matter of policy and practice, does not manage discretionary accounts. Should performance information be used, BCA's policy requires that any performance information and materials must be truthful and accurate, and prepared and presented in a manner consistent with applicable rules and regulatory guidelines and reviewed and approved by the President or designee(s). BCA's policy prohibits any performance information or materials that may be misleading, fraudulent, deceptive and/or manipulative.

Background
An investment adviser's performance information, in reference to discretionary accounts, is included as part of a firm's advertising practices which are regulated by the SEC under Section 206 of the Advisers Act, which prohibits adviser from engaging in fraudulent, deceptive, or manipulative activities. The manner in which investment advisers portray themselves and their investment returns to existing and prospective clients is highly regulated. These standards include how performance is presented. SEC Rule 206(4)-1 proscribes various advertising practices of investment advisers as fraudulent, deceptive or manipulative and various SEC no-action letters provide guidelines for performance information.

Responsibility
The Chief Compliance Officer has the responsibility for implementing and monitoring our policy for the preparation, presentation, review and approval of any performance information to insure any materials are consistent with our policy and regulatory requirements. This designated person is also responsible for maintaining, as part of the BCA's books and records, copies of all performance materials, including the supporting records to demonstrate the calculation of any performance information for the entire performance information period consistent with applicable recordkeeping requirements, as well as records of reviews and approvals.

Procedure
BCA has adopted procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

- All performance information and materials must be reviewed and approved prior to use by the President or Chief Compliance Officer (other than the individual who prepared such material), who is familiar with applicable rules and standards for performance advertising.
- The initialing and dating of the performance materials will document approval.
- Each advisory professional is responsible for ensuring that approved materials are not used or modified without the express written authorization of the President or Chief Compliance Officer.
- The Chief Compliance Officer or designee(s) is responsible for maintaining copies of any performance materials and supporting documentation for the calculation of performance materials.

Supervision & Internal Controls

Background

Pursuant to Section 203(e) of the Advisers Act, if an investment adviser fails to reasonably supervise an Associated Person or any other person subject to the investment adviser's supervision, and that person violates Federal Securities Laws, then the SEC may censure, limit the activities of, or revoke the registration of the investment adviser. However, Section 203(e)(6) states that an investment adviser will not be deemed to have failed to reasonably supervise any person if the investment adviser:

- Established procedures, and a system for applying such procedures, that would reasonably be expected to prevent and detect, insofar as practicable, any such violation by such other person; and
- Reasonably discharged the duties and obligations incumbent upon it by reason of such procedures and system without reasonable cause to believe that such procedures and system were not being complied with.

Policies and Procedures

The Company's management recognizes its duty to supervise the actions of its Associated Persons. Compliance with the policies and procedures contained in this Compliance Manual assists the Company's management in fulfilling its supervisory obligations. As appropriate, this Compliance Manual identifies the individuals who have supervisory authority over the Company's various activities. Associated Persons who are unfamiliar with any activities, or who require assistance carrying out their duties, are expected to consult with an appropriate supervisor.

All Associated Persons must comply with the letter, and the spirit, of this Compliance Manual. Associated Persons are expected to use good judgment, and to report any suspected violations of the Company's policies or Federal Securities Laws to the CCO. The Company's CCO will communicate with senior management and will investigate any suspected violations of Federal Securities Laws or any weakness in the Company's compliance program and shall determine the appropriate remedial action or resolution.

Responsibilities

The Company's officers will reasonably supervise the activities of its Associated Persons. The Company's Associated Persons with supervisory responsibilities are required to supervise the activities of their subordinates and report any material issues to the CCO or senior management.

The Company's Associated Persons may have explicitly defined supervisory responsibilities because of a position or title, and/or de facto supervisory responsibilities because of activities, roles, abilities, or operational authority within the Company. All Associated Persons with explicit or implicit supervisory authority have affirmative duties to:

1. Ensure that the Company's practices are consistent with its written policies and procedures, and are not inconsistent with disclosures to clients;
2. Ensure that all persons under their supervision know and understand the contents of the Compliance Manual as it relates to their day-to-day activities;
3. Effectively monitor Associated Persons over whom they have supervisory authority;
4. Promptly notify the CCO of any occurrences that may violate any laws, rules, regulations, and/or this Compliance Manual involving any person under their supervision; and
5. Ensure that the Company responds appropriately, and in a timely manner, to any actual or

suspected wrongdoing, undisclosed conflicts of interest, ineffective internal controls, or other compliance risks.

Supervision over certain responsibilities is generally delegated to various Associated Persons within the Company. Such delegation of responsibilities must occur to ensure that the Company provides clients with the highest level of service.

The Company expects its Associated Persons to report to their supervisors any issues arising in which they may be unfamiliar or may otherwise require the assistance and judgment of senior management. Associated Persons must also report any activities that run contrary to the Code of Ethics and that may adversely affect the reputation of the Company. The Company shall commit to a full unbiased review of the matter and implement the necessary corrective and/or disciplinary action, if applicable. The Company requires the full commitment of its Associated Persons to the tenets set forth in the Code of Ethics. Associated Persons that elect to ignore and/or violate the tenets of the Code of Ethics shall be disciplined, including the possible termination of their employment with the Company.

Should an Associated Person or IAR of the Company have any questions regarding the applicability/relevance of any statutes, rules or regulations, or any section of these policies and procedures, he or she should address those questions with the CCO.

Escalating Perceived Risks

In addition to reporting suspected violations of the Company's policies or Federal Securities Laws to the CCO, Associated Persons are expected to discuss any perceived risks, or concerns about the Company's business practices with their direct supervisor. Supervisors should act prudently and exercise good judgment when determining an appropriate response to any reported risks or concerns. The CCO should be informed by supervisors of any potentially serious risks, material weaknesses in internal controls, or inappropriate business practices.

Nothing herein shall prohibit or impede in any way an Associated Person, or former Associated Person, from reporting a possible securities law violation directly to the SEC or other regulatory authority. In addition, the Company will not retaliate in any way against an Associated Person, or former Associated Person, for providing information relating to a possible securities law violation to the SEC or other regulatory authority.

Failure to Supervise

All individuals acting in a supervisory role are potentially liable for violations committed by those individuals they directly or indirectly supervise. Supervisors may be able to counter such violations with effective "reasonable" supervision through the implementation of customized compliance policies, procedures, and controls.

Branch Office Supervisory Duties

To the extent the Company maintains any branch office locations, the requirements set forth in this section apply equally to all such locations. Supervision of remote office locations and their Associated Persons is the ultimate responsibility of the CCO, and the on-site designated supervisor (if any). The CCO, or designee, will conduct an on-site review of the remote office locations periodically to verify their compliance with the Company's policies and procedures.

Cybersecurity

Cybersecurity is important to the integrity of the market system and customer data protection. The Company's cybersecurity policies and procedures are designed to:

1. Identify and control cybersecurity risks;
2. Protect the Company's networks and client information;
3. Curb risks arising from remote customer access and funds transfer requests;
4. Mitigate risks related to vendors and other third parties; and,
5. Detect and report unauthorized activity on our network.

Access to and Security of Electronic Records

The Company has implemented the following cybersecurity procedures to protect Nonpublic Personal Information and the Company's proprietary information. This policy shall apply to all electronic devices (i.e. computers, laptops, tablets, smartphones, and other similar devices), whether Company or employee owned, which are used to conduct Company business (hereafter "electronic devices"):

1. Associated Persons are prohibited from using any electronic device for Company business unless issued or approved by the Company;
2. The Company uses passwords to protect electronic devices and systems utilized on such devices. Associated Persons must never share their passwords or store passwords in a place that is accessible to others;
3. Associated Persons should shut down or lock their computer when they leave the electronic device for any extended period of time;
4. Associated Persons should change passwords periodically. If a password is compromised, the Associated Person must change his or her password immediately and promptly notify the CCO of the breach;
5. The CCO should seek to ensure that the Company's electronic devices require relatively "strong" passwords, such as those that contain combinations of lower case letters, upper case letters, and numbers or symbols;
6. Associated Persons should refrain from using passwords that would be easily guessed, such as children's names, birthdays, or commonly used strings like "password" or "12345";
7. Any theft or loss of an electronic device must immediately be reported to the CCO;
8. All laptops and portable storage devices containing Nonpublic Personal Information should be encrypted;
9. The CCO is responsible for implementing and maintaining appropriate protections for electronic devices and the systems utilized on such devices, including:
    i. Anti-virus software;
    ii. Firewalls;
    iii. Prompt implementation of system patches and updates;
    iv. Encryption of all wireless data transmissions;
    v. When technically feasible, encryption of files containing Nonpublic Personal Information and the Company's proprietary information traveling across public networks, and
    vi. Monitoring of the Company's electronic devices and taking appropriate action in response to intrusion and unauthorized use;
10. To the extent practicable, Nonpublic Personal Information and the Company's proprietary information will be kept on portions of the network that are only available to Associated Persons with a legitimate need to access the information;
11. The CCO is responsible for setting Associated Persons' access permissions on the Company's computer network, assigning unique identifications and passwords to each person with computer access, to the extent feasible, network users should be restricted to those network resources necessary for each Associated Person's business functions;

12. Secure connections shall be established, such as through a "VPN", when accessing the Company's network remotely;
13. The CCO will promptly disable system access for any terminated employee;
14. To the extent technically feasible, system access shall be blocked after multiple unsuccessful attempts to gain access or limitations placed on access for particular systems; and
15. Prior to sale or disposal, electronic devices will be permanently erased or destroyed. The CCO, who oversees this process, is aware that information can be retained on conventional media, such as laptops and compact discs, as well as electronic equipment such as fax machines and photocopiers.

Online Account Access

Many cybersecurity experts have identified account takeovers as the top risk facing investment advisers and their clients. If the Company provides clients with online account access to virtual private networks, the Company will create books and records to preserve the following information:

1. The name of any third party managing the service;
2. An explanation of the functions that can be performed online, such as withdrawals or other external transfers of funds and/or securities;
3. How the client is authenticated for online account access and transactions;
4. Any software or alternative methods used to detect unusual transaction requests;
5. How clients' PIN numbers are protected; and
6. Any information provided to customers to reduce cybersecurity risks.

The Company uses either single-factor or two-factor authentication before permitting access to the account. Single-factor authentication is a user name and password. Two-factor authentication requires a client to answer a question or provide additional information before gaining access to the account.

Detection of Unauthorized Access to Company Networks

The Company restricts access to network resources to the extent necessary to accomplish their business functions. The Company may detect unauthorized access to its network through the following means:

1. Utilization of software to detect malicious code on the Company's networks and mobile devices;
2. Maintaining statistical baseline information about anticipated events on the Company's network;
3. Aggregating and correlating event data from multiple sources;
4. Establishing written incident alert thresholds;
5. Monitoring the Company's network environment to detect potential cybersecurity events;
6. Monitoring the Company's physical environment to detect potential cybersecurity events;
7. Monitoring the activity of third party service providers with access to the Company's networks;
8. Monitoring the presence of unauthorized users, devices, connections, and software on the Company's networks;
9. Evaluating requests initiated remotely to identify potentially fraudulent requests;
10. Utilization of data loss prevention software;
11. Conducting penetration tests and vulnerability scans; and,
12. Testing the reliability of event detection processes.

Relationship to Other Company Programs

This policy incorporates by reference other policies intended to protect the Company and its clients from cyber threats, including, for example, Regulation S-P and Business Continuity Plan.

Identification of Risks/Cybersecurity Governance

The Company conducts periodic risk assessments to identify cybersecurity threats, vulnerabilities, and potential business consequences. The Company documents the date on which the risk assessment took place. The Company has taken the following steps to identify and control risks:

1. The Company has prepared a list of all computers and devices connected to its network, as well as an inventory of every application supported on our networks;
2. Connections to the Company's network from external sources are catalogued; and
3. Login and log-out practices are assessed for adequacy, appropriate retention and secure maintenance.

Succession Plan

Background

Investment advisers owe a fiduciary duty to their clients to have succession plans in place to ensure continuity of services and the daily operations of the business, or to smoothly wind down the Company's businesses in the event of death, disability, or incapacity of key members of the investment adviser.

A succession plan should detail the steps that an investment adviser and its Associated Persons will take in the event of a death, disability or incapacity of key members of the investment adviser which would compromise the ability of the Company to provide its customary level of service to its clients without prompt action (each a "Succession Event"). This plan, including all contact information for clients, Associated Persons, regulators, custodians, and service providers, should be updated regularly and each revision should be communicated to Associated Persons.

Policies and Procedures

The Company's Succession Plan is an essential part of its operations. All Associated Persons are responsible for understanding their role in the event of a Succession Event. Burgess Chambers, President and CEO of the Company, has the overall responsibility for the implementation of the Company's Succession Plan. The Mr. Chambers is responsible for ensuring that the Company's Succession Plan is reviewed annually. Any changes to the Succession Plan shall be approved by Mr. Chambers. Robert Masrieh, Chief Financial Officer of the Company, shall have access to all of the necessary information to carry out the Succession Plan. Necessary information may include, but is not limited to the following:

- List of clients, client contact information and other client information as necessary (including telephone numbers, addresses, investment objectives, financial information and suitability) and contract information;
- Contact information for the Company's attorneys, accountants and successor;
- Contact information for the Company's service providers; and
- Contact information for the Company's creditors, vendors, Associated Persons and regulators.

The list of client information and client contracts is maintained in the home office. The list of contact information is part of the Disaster Recovery Plan and is maintained in a separate location.

If a Succession Event affects the management of accounts, such as the incapacity of an individual vested with investment decision making authority, Mr. Masrieh or designee, will determine the steps necessary to ensure continuity of account management services. This may include designating another qualified individual at the Company to assume discretionary management authority over client accounts (unless prohibited under the Client Agreement or applicable law), or communication to clients that their assets will no longer be managed by the Company and that clients should take steps to transition their assets to another investment adviser.

Mr. Masrieh shall also, if necessary:

- Determine whether the Company is able to continue to operate as a legal entity given the ownership structure and registration status of the Company and any successor person's or entities' registration status;
- Contact the Company's attorney, and/or successor/new ownership to inform them of the status of the Company and take further action as appropriate;

- Contact the Company's creditors, vendors, Associated Persons and regulators as appropriate; and
- Direct the custodian to rebate advisory fees that are paid in advance as provided in the client contract.

Disposal of Client Records and Information

The CCO has the sole authority to permit the destruction of any required record. No required record will be destroyed before the required retention period has lapsed and before the CCO has authorized such destruction in writing.

If the Company has a pending or ongoing regulatory or legal proceeding, all document destruction must cease immediately and documents must be preserved in a manner specified by counsel. Among other things, the Company should be careful to avoid any inadvertent destruction of electronic documents through backup processes that overwrite old backups.

The Company will dispose of client records as follows:

1. discard any proprietary documents or electronic media in a manner that ensures such documents and electronic media are shredded, permanently erased, or otherwise destroyed so that the information cannot be reconstructed;
2. store such material in a secure area until it is collected for shredding; and
3. destroy or erase all data when disposing of computers, diskettes, magnetic tapes, hard drives, or any other electronic media containing nonpublic and consumer report information.

Associated Persons should be aware that some devices, such as scanners, photocopiers and fax machines, may save electronic copies of documents that have been scanned, copied, or transmitted. Associated Persons should consult with the device's instruction manual or manufacturer to ensure that any stored information is erased before the device is removed from the Company's offices.

The Company must ensure that any companies engaged to dispose of nonpublic information perform their duties in accordance with this policy. The Company may ensure appropriate disposal by, among other things:

- reviewing an independent audit of the disposal company's operations;
- obtaining information about the disposal company from references or other reliable sources; and/or
- requiring that the disposal company be certified by a recognized trade association or similar third party.

The Company may enter into confidentiality agreements with prospective counterparties that call for the Company to destroy documentation associated with transactions that are not consummated. Such agreements will include provisions that describe the applicable record retention requirements and indicate that the Company will comply with all such requirements.

Identity Theft Protection Program

Background

The SEC adopted Regulation S-ID pursuant to the requirement under Section 615(e)(1) of the Fair Credit Reporting Act. Regulation S-ID applies to investment advisers that are registered or required to be registered under the Investment Advisers Act of 1940. Under Regulation S-ID, the Red Flag Rule, a financial institution must implement a written program to detect, prevent and mitigate identity theft in connection with the opening or maintenance of "covered accounts". "Covered Accounts" include any account that a financial institution maintains for which there is reasonably foreseeable risk to clients from identity theft, including financial, operational, compliance, reputational, or litigation risks.

Policies and Procedures

The Company's policy is to protect clients and their accounts from identity theft. This Identity Theft Prevention Program ("ITPP" or "Program") addresses: 1) identifying relevant identity theft red flags for the Company; 2) detecting those red flags; 3) responding appropriately to any that are detected to prevent and mitigate identity theft; and 4) updating the ITPP periodically to reflect changes in risks.

Approval

The CCO and the Company's senior management have approved this ITPP.

Oversight and Continued Administration of the ITPP

The CCO is responsible for oversight of the ITPP. The CCO is responsible for development, implementation, and administration of the Program, and shall ensure that the Company's staff have been trained, as necessary, to effectively implement the ITPP.

Oversight of Service Providers

The CCO shall ensure that the services provided by the Company's third-party service providers are conducted in accordance with reasonable policies and procedures designed to detect, prevent, and mitigate the risk of identity theft. Such services may include, but are not limited to, custody services, data retention and destruction, client account access, maintenance of client contact information and records (CRM systems), and any other service provided to the Company by a third party through which the third-party service provider has access to client information.

Definitions

1. **Financial Institution**. The Company is a "financial institution" if it provides, either directly or indirectly through its custodian, consumer "transaction accounts," which are accounts that allow account holders to make withdrawals for payment or transfer of funds to third parties by telephone transfers, checks, debit cards or similar means. Since "consumer" is defined as an individual, an investment adviser without individuals as clients would not be a financial institution under this definition.
2. **Client**. For the purpose of this section, client means those clients who are consumers (natural persons).
3. **Covered Accounts**. If the Company is a financial institution, it must then analyze whether it offers "covered accounts," which are any accounts that involve a reasonably foreseeable risk from identity theft to clients or the safety and soundness of the Company.
4. **Identity Theft**. This term means a fraud committed or attempted using the identifying information of another person without authority.

Determination of Covered Accounts

The Company shall, not less frequently than annually, determine whether it offers or maintains covered accounts. As part of this determination, the Company shall conduct a risk assessment taking into consideration the following:

1. The methods the Company provides to open accounts;
2. The methods the Company provides to access accounts; and
3. The Company's previous experiences with identity theft.

The Company has determined that it offers or maintains one or more covered account, and is therefore required to adopt an ITPP designed to detect, prevent, and mitigate identity theft in connection with the opening a covered account or with any existing covered account. The Company must ensure that the ITPP:

1. Identifies relevant red flags for the covered accounts offered or maintained, and incorporates those red flags into the ITPP;
2. Detects red flags that have been incorporated into the Program;
3. Requires an appropriate response to any red flags that are detected to prevent and mitigate identity theft;
4. Ensures periodic updates to the Program to reflect changes in risks to clients and to the safety and soundness of the Company from identity theft; and
5. Requires oversight and continued administration of the Program.

Identifying Relevant Red Flags

To identify relevant identity theft red flags, the Company should consider the following risk factors:

1. how it offers or maintains covered accounts;
2. the methods it provides to open or access these accounts; and
3. previous experience with identity theft.

In identifying red flags for covered accounts, the Company should consider the following *potential sources of red flags*:

1. incidents of identity theft that the Company has experienced;
2. methods of identity theft perpetrated upon the Company's clients; and
3. applicable regulatory guidance

The Company should also consider the sources of red flags, including identity theft incidents the Company has experienced, changing identity theft techniques that may be likely, and applicable supervisory guidance. In addition, the Company should consider red flags from the following categories:

1. suspicious documents;
2. suspicious personal identifying information;
3. the unusual use of, or other suspicious activity related to, a covered account and;
4. notice from clients, victims of identity theft, law enforcement authorities, or other sources regarding possible identity thefts.

Red Flags Identified by the Company

Based on review of the risk factors, sources, and examples of red flags, the Company has identified red flags, which are contained in the first column below "Red Flag Identification and Detection Grid" ("Grid").

Red Flag Identification and Detection Grid	
Category: Suspicious Documents	
1. Identification presented looks altered/forged.	Associated persons who deal with clients will scrutinize identification presented in person to make sure it is not altered or forged.
2. The identification presenter does not look like the identification's photograph or physical description.	Associated Persons who deal with clients will ensure that the photograph and the physical description on the identification match the person presenting it.
3. Information on identification differs from what the identification presenter is saying.	Associated Persons who deal with clients will ensure that the identification and the statements of the person presenting them are consistent.
4. Information on the identification does not match other information the Company has on file for the presenter.	Associated Persons who deal with clients will ensure that the identification presented and other information on file from the account are consistent.
5. New accounts appear to be forged or torn up and reassembled.	Associated Persons who deal with clients will scrutinize each new account to make sure it is not altered, forged, or torn up and reassembled.
6. Other information on the identification is inconsistent with the information provided by the client or with the information that is on file.	Associated Persons who deal with clients will review accounts for inconsistencies in information provided and information on file.
Category: Suspicious Personal Identifying Information	
7. Inconsistencies exist between information presented and other things we know about the presenter or can find out by checking readily available sources.	Associated Persons will check personal identifying information presented.
8. Inconsistencies exist between information presented such as address, date of birth, and/or inaccuracies in social security number.	Associated Persons will check personal identifying information presented to make sure they are consistent and accurate.
9. Personal identifying information presented has been used on an account the Company knows was fraudulent.	Associated Persons will compare information presented with addresses and phone numbers on accounts found or reported fraudulent.

10. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop or a prison address, or a phone number is invalid, or is for a pager or answering service.	Associated Persons will validate the information presented when opening an account by looking up addresses on the internet to ensure they are real and not for a mail drop or a prison, and will call the phone numbers given to ensure they are valid and not for pagers or answering services.
11. The SSN ("social security number") presented was used by someone else opening an account or other clients.	Associated Persons will compare the SSNs presented to see if they were given by others opening accounts or other clients.
12. The address or telephone number presented has been used by many other people opening accounts or other clients.	Associated Persons will compare address and telephone number information to see if they were used by other clients.
13. A person who omits required information on an account or other form does not provide it when told it is incomplete.	Associated Persons will track when clients have not responded to requests for required information and will follow up with clients to determine why they have not responded.
14. Inconsistencies exist between what is presented and what is on file.	Associated Persons will verify key items from the data presented with information on file.
15. A person seeking access cannot provide authenticating information beyond what would be found in a wallet, or cannot answer a challenge question.	Associated Persons will authenticate identities for existing clients by asking challenge questions that have been prearranged with the client and for clients by asking questions that require information beyond what is readily available from a wallet.
Category: Suspicious Account Activity	
16. Soon after notification of a change of address request for an account, the Company is asked to add additional access means (such as debit cards or checks) or authorized users for the account.	The Company will verify change of address requests by sending a notice of the change to both the new and old addresses so the client will learn of any unauthorized changes and can notify the Company of any discrepancies.
17. An account develops new or inconsistent patterns of activity, such as a material change in spending or electronic fund transfers, increase in use of margin, or an account closed for cause.	The Company will review its accounts on at least a monthly basis and check for suspicious new patterns of activity such as a big change in spending, increases in use of margin, account closures for cause and/or electronic fund transfers.
18. An account that is inactive for a long time is suddenly used again.	The Company will review its accounts on at least a monthly basis to see if long inactive accounts become very active.

19. Mail sent to a client is returned repeatedly as undeliverable even though the account remains active.	The Company will note any returned mail for an account and immediately check the account's activity.
20. The Company learns that a client is not getting his or her paper account statements.	The Company will record on the account any report that the client is not receiving paper statements and immediately investigate them.
21. The Company is notified that there are unauthorized charges or transactions to the account.	The Company will verify if the notification is legitimate and involves a client account and then investigate the report.
Category: Notice From Other Sources	
22. The Company is told that an account has been opened/used fraudulently by a client, an identity theft victim, or law enforcement.	The Company will verify that the notification is legitimate and involves a client account, and then investigate the report.
23. The Company learns that unauthorized access to the client's personal information took place or became likely due to data loss (e.g., loss of wallet, birth certificate, or laptop), leakage, or breach.	The Company will contact the client to learn the details of the unauthorized access to determine if other steps are warranted.

Detecting Red Flags

The Company will review its Covered Accounts, how accounts are opened and maintained, and how to detect red flags that may have occurred in them. Detection of red flags is based on the Company's methods of obtaining information about clients and verifying such information, authenticating clients who access the accounts, and monitoring transactions and change of address requests. (For opening Covered Accounts, this may include obtaining identifying information about, and verifying the identity of the person opening the account by obtaining documentation verifying the client's identity. For existing Covered Accounts, it can include authenticating clients, monitoring transactions, and verifying the validity of a change of address.

The Company will consider the red flags that are named above when obtaining identifying information about, and verifying the identity of, a person opening a covered account. The Company must also consider these red flags when authenticating clients, monitoring transactions, and verifying the validity of change of address requests for existing accounts.

Preventing and Mitigating Identity Theft

The Company will review its Covered Accounts, how they are opened, and previous experience with identity theft, as well as new methods of identity theft likely foreseen. Based on this and review of the SEC's identity theft rules and suggested responses to mitigate identity theft, as well as other sources, the Company has developed the procedures below to respond to detected identity theft red flags.

The Company must respond appropriately to any red flags detected based upon the degree of risk posed, considered aggravating factors that may heighten the risk of identity theft, such as a data security incident that results in unauthorized access to a client's account records held or offered by the Company or a third party, or notice that a client has provided information related to a covered account to someone fraudulently claiming to represent the Company, the account custodian, or to a fraudulent website.

Appropriate responses include:

1. Monitoring a covered account for evidence of identity theft;
2. Contacting the client;
3. Changing any passwords, security codes, or other security devices that permit account access;
4. Reopening the account with a new account number;
5. Not opening a new account or closing an existing account;
6. Notifying law enforcement; or
7. Determining that no response is warranted under the particular circumstances.

Procedures to Prevent and Mitigate Identity Theft

When the Company has been notified of a red flag or it detects a red flag, the Company will take the steps outlined below, as appropriate to the type and seriousness of the threat:

New Clients. For red flags raised by new clients:

1. Review information. The Company will review a new client's information collected as part of the custodial new account process (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).
2. Obtain/Check government identification. The Company will also obtain/check a current government-issued identification card, such as a driver's license or passport.
3. Seek additional verification. If the potential risk of identity theft indicated by the red flag is probable or large in impact, The Company may also verify the person's identity through non-documentary methods, including, but not limited to:
    a. Contacting the client;
    b. Independently verifying the client's information by comparing it with information from, public database or other source;
    c. Checking references with other affiliated financial institutions; or
    d. Obtaining a financial statement.
4. Deny the new account. If the Company finds that the client is using an identity other than his or her own, it will decline to accept the client.
5. Report. If the Company finds that the client is using an identity other than his or her own, it will report it to appropriate local and state law enforcement. Where organized or wide spread crime is suspected, the FBI or Secret Service will be contacted. If mail is involved, the US Postal Inspector will be contacted. The Company may also report it to the SEC, state regulatory authorities, and its custodian.
6. Notification. If the Company determines personally identifiable information has been accessed, it will prepare any specific notice to clients or other required notice under state law.

Existing Clients. For red flags raised by someone seeking to access an existing client account:

1. Monitor. The Company will monitor, limit, or temporarily suspend activity in the account until the situation is resolved.
2. Contact the client. The Company will contact the client using verified contact information, describe what has been found and verify with them that there has been an attempt at identify theft.
3. Account Changes. The Company will facilitate reopening a covered account with a new account

number, and facilitate closing an existing covered account.

4. Heightened risk. The Company will determine if there is a particular reason that makes it easier for an intruder to seek access, such as a client's lost wallet, mail theft, a data security incident, or the client providing account information to an impostor pretending to represent the Company or to a fraudulent website.
5. Check similar accounts. The Company will review similar accounts to determine if there have been attempts to access the accounts without authorization.
6. Collect incident information. For a serious threat of unauthorized account access the Company may collect, if available:
    a. Custodian Firm name, contact name and telephone number;
    b. Dates and times of activity;
    c. Securities involved (name and symbol);
    d. Details of trades or unexecuted orders;
    e. Details of any wire transfer activity;
    f. Client accounts affected by the activity, including name and account number; and
    g. Whether the client will be reimbursed and by whom.
7. Report. If the Company finds that the client is using an identity other than his or her own, it will report it to appropriate local and state law enforcement. Where organized or wide spread crime is suspected, the FBI or Secret Service will be contacted. If mail is involved, the US Postal Inspector will be contacted. The Company may also report it to the SEC, state regulatory authorities, and its custodian.
8. Notification. If the Company determines personally identifiable information has been accessed that results in a foreseeable risk for identity theft, it will prepare any specific notice to clients or other required notification under state law.
9. Review of insurance policy. Since insurance policies may require timely notice or prior consent for any settlement, the Company will review its insurance policy to ensure that its response to a data breach does not limit or eliminate insurance coverage.
10. Assist the client. The Company will work with its clients to minimize the impact of identity theft by taking the following actions, as applicable:
    a. Recommending a change of password, security codes or other ways to access the threatened account;
    b. Recommending/Offering to close the account;
    c. Recommending/Offering to reopen the account with a new account number; and/or
    d. Instructing the client to go to the FTC Identity Theft Website to learn what steps to take to recover from identity theft, including filing a complaint using its online complaint form, calling the FTC's Identity Theft Hotline 1-877-ID-THEFT (438-4338), TTY 1-866-653-4261, or writing to Identity Theft Clearinghouse, FTC, 6000 Pennsylvania Avenue, NW, Washington, DC 20580.

Internal Compliance Reporting

The Company's staff, who are involved with developing, implementing, and administering the ITPP, will report, at least annually, to the CCO on compliance with the SEC's Red Flags Rules. The report will address the effectiveness of the ITPP in addressing the risk of identity theft in connection with covered account openings, existing accounts, service provider arrangements, significant incidents involving identity theft, and management's response and recommendations for material changes to the ITPP.

The CCO must annually prepare a report on compliance by the Company with all aspects of the Program and regulatory requirements governing the Program (Section 248.201 of Reg S-ID). This report must address material matters related to the ITPP and evaluate issues regarding: a) the effectiveness of the Program in addressing the risk of identity theft in connection with opening and maintaining covered accounts; b) service provider arrangements; c) any significant incident involving identity theft and management's response, and d) recommendations for material changes to the

Program. The CCO must review this report and approve any material changes to the Program as necessary to address changing identity theft risks. The reporting required by this section of the ITPP may be incorporated into the Company's annual compliance review.

Updates and Annual Review

The CCO will update the ITPP whenever there are material changes to the Company's operations or when it experiences a material identity theft incident from a covered account. The Company will also follow new ways that identities can be compromised and evaluate the risk they pose for the Company. In addition, the CCO will review the ITPP annually to modify it for any changes in the Company's operations. The CCO will take into account the Company's experiences with identify theft, changes in methods in identity theft, changes in methods to detect, prevent and mitigate identity theft, changes in the types of accounts that the Company offers or maintains, and changes in the Company's business arrangements.

The Company must review, and if necessary, update its ITPP to reflect changes in risks to clients or to the safety and soundness of the Company from identity theft. Updates might be based on factors such as:

1. Experiences the Company has with identity theft;
2. Changes in methods of identity theft;
3. Changes in methods to detect, prevent, and mitigate identity theft;
4. Changes in the types of accounts that the Company offers or maintains;
5. Changes in the Company's service provider arrangements; and
6. Changes in the Company's business arrangements, including, but not limited to, mergers, acquisitions, alliances, and joint ventures.

Training

The CCO will train Company staff, as necessary, to effectively implement the ITPP. Training may consist of Company meetings to review and discuss the ITPP with Company personnel and to address any questions or concerns about the Company's procedures to prevent and mitigate identity theft.

Fraudulent Transfers

The Company will not accept instructions for wire transfers or other transfers via email or other written form without also contacting the client. The Company will take steps to ensure the transfer request is legitimate before acting and facilitating the disbursement.

The CCO, or designee, is responsible for administering the Company's policies on fraudulent transfers.

Definition

A fraudulent transfer is an illegal transfer of property. Fraudsters may directly target investment advisers and their clients by email spoofing to request a fraudulent wire transfer, check transfer, or other transfer of client funds to a third party bank account, which could include forged letters of authorization. The email appears to have been sent from the client, but is actually sent from a fake-but-similar email account (or could even be the client's actual account).

Note: the email may be addressed on a first name basis to whomever the client typically works with; if there has been a wire transfer request in the past, the thief may even simply copy the format of the old email to capture the client's writing style.

Fraud Attempt Steps

1. Fraudster hacks into client's email account, searches history and monitors emails, finds investment adviser;
2. Fraudster asks investment adviser for account balance, proactively offers excuse for not being able to talk, inquires about withdrawal procedures;
3. Fraudster submits an urgent wire request to investment adviser who in turn submits the wire request to the brokerage firm (custodian); and
4. Once the transfer is complete, the client cannot get the money back.

Identify Warning Signs

1. Fraudsters try to create urgent or discomfort to discourage contact, e.g. please execute this request immediately;
2. Emails often appear authentic, but poor or stiff grammar is often (not always) a hallmark of fraudulent emails;
3. Email indicates that client is unreachable via telephone;
4. Attempts are more often routed to domestic banks (not always);
5. Funds are routed to a third-party account as opposed to the client's existing and known bank accounts;
6. Phone number on request does not match the phone number on file;
7. Email address(es) for wire transfer are not legitimate; and
8. Request is inconsistent with client's prior history.

Transfer of Client Funds

Where an Associated Person receives a request to transfer "money" on deposit in a client's account, the Associated Person must do the following:

1. Do not reply to the email request;
2. Call the client at the existing phone number of record for verbal confirmation on the disbursement request before wiring money out of the account(s):
    a. Verbal verification is required - It is entirely possible to receive a wire transfer request from the client's own email, with the client's own signature, and the client's typical writing style, except the request is a fraud; and
    b. Do not use a phone number provided in the email;
3. The calling party should be familiar with the client and recognize the client's voice;
4. If the account has been hacked, inform the client to change their passwords immediately and to contact other financial institutions to ensure their account(s) have not been compromised;
5. Verify the client's signature on the wire transfer form by comparing it to prior signed documents:
    a. All wire transfers require the client's signature;
6. The Associated Person must create a contemporaneous record of the call back and maintain a copy in the client's file;
7. Alert a supervisor and the CCO immediately of all such requests; and
8. Alert the service team at the client's account custodian.

E-mail and Fax Requests to Transfer Funds and/or Securities

The Company verifies e-mail and fax requests to transfer funds and/or securities through the following means:

1. An Associated Person will attempt to contact the client by phone;
2. If the associated person cannot contact the client by phone, he/she will attempt to communicate with the client's emergency contact; and
3. If the request still cannot be verified, the IAR handling the client's account will review the account history to determine if the circumstances surrounding the transfer are suspicious in

view of the client's profile, personal situation, and historical transactions.

If the request cannot be authenticated and is inconsistent with the client's profile, personal situation, and historical transactions, it will not be honored.

Information Security Program

Background

The Company is committed to protecting the confidentiality of all nonpublic information regarding its clients and Associated Persons ("Nonpublic Personal Information").

Policies and Procedures

It is the Company's policy to protect and maintain the accuracy of client personal information. To protect client personal information, including consumer report information, the Company has developed this Written Information Security Program ("WISP"). The intent of this WISP is to safeguard the Company's storage of, access to, and disposal of, client personal information, including consumer report information, obtained and/or maintained in hard copy and/or electronically, as well as access and protection of its computer and information systems. Written and electronic records containing personal information shall be securely destroyed or deleted at the earliest opportunity consistent with business needs and legal retention requirements. See the *Books and Records* section for details regarding record retention. The Company's WISP consists of this parent section in conjunction with the subsections herein.

The following summarizes the key points of the Company's WISP:

1. Designating one or more Associated Persons to maintain the WISP;
2. Developing security policies for Associated Persons relating to the storage, access, and transportation of records containing personal information outside of the Company's business premises;
3. Imposing disciplinary measures for violations of the WISP;
4. Preventing terminated Associated Persons from accessing records containing personal information;
5. Evaluating service providers' information security safeguards;
6. Implementing reasonable restrictions upon physical access to records containing personal information and storage of such records and data in locked facilities, storage areas, or containers;
7. Monitoring to ensure that the WISP is operating in a manner reasonably calculated to prevent unauthorized access to, or unauthorized use of, personal information and upgrading information safeguards as necessary to limit risks;
8. Reviewing the scope of the security measures at least annually or whenever there is a material change in business practices that may reasonably implicate the security or integrity of records containing personal information; and
9. Documenting responsive actions taken in connection with any incident involving a breach of security and mandatory post-incident review of events and actions taken, if any, to make changes in business practices relating to protection of personal information.

Nonpublic Personal Information ("NPI") is defined as personally identifiable information ("PII"), as well as certain listings of customers. PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified.

Personal identifiable information ("PII") is defined as an individual's first name and last name or first initial and last name in combination with any one or more of the following data elements that relate to such individual: (a) Social Security number; (b) driver's license number or state-issued identification card number; or (c) financial account number, or credit or debit card number, with or without any required security code, access code, personal identification number or password, that would permit access to an individual's financial account; provided, however, that "personal information" shall not include information that is lawfully obtained from publicly available information, or from federal, state or local government records lawfully made available to the general public.

Record or Records is defined as any material upon which written, drawn, spoken, visual, or electromagnetic information or images are recorded or preserved, regardless of physical form or characteristics.

Service provider is defined as any person that receives, stores, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to clients.

Responsibility

The CCO is responsible for implementing, supervising, and maintaining the WISP. The CCO is also responsible for training of all Associated Persons and independent contractors, including temporary and contract Associated Persons, who have access to personal information and for evaluating the ability of any of the Company's third party service providers to implement and maintain appropriate security measures.

In addition, the CCO shall maintain a secured and confidential master list of all lock combinations, passwords, and keys. The list will identify which Associated Person possess keys, key cards, or other access devices and that only approved Associated Persons have been provided access credentials. All security measures including the WISP shall be reviewed at least annually to ensure that the policies contained in the WISP are adequate and meet all applicable federal and state regulations.

Storage, Access and Transportation of Records Outside Business Premises

Since there may be regulatory prohibitions to storing certain records at a location other than the main office no records containing personal information shall be removed from the main office without the prior approval of the CCO.

Before granting approval to remove records from the main office, the CCO shall determine whether:

1. there is a legitimate business need for the records to be removed (such as an Associated Person temporarily working from home or to have the records copied in response to a subpoena); or
2. appropriate safeguards are in place to ensure the security of the records.

Storage and Access of Records on the Business Premises

Hard Copy/Paper Records

1. Records containing personal information shall be kept in a secure location such as a file room and/or locked file cabinet(s) unless the records are being currently used;
2. Access to records containing personal information shall be limited to those Associated Persons whose duties, relevant to their job description, have a legitimate need to access said records, and only for the legitimate job-related purpose;
3. Records shall be returned to the file room/file cabinet(s) as soon as practicable after the Associated Person is done working with the record;
4. Records should not be left on an Associated Person's desk when the Associated Person is not present;

5. All records containing personal information must be returned to the file room/file cabinet(s) at the end of the day;
6. In accordance with the record retention requirements of state and/or Federal law, paper documents containing personal information that are no longer required to be maintained shall be shredded so that personal data cannot practicably be read or reconstructed. At least annually, the CCO will determine what records are no longer required to be maintained and shall arrange for their disposal;
7. Associated Persons will exercise due caution when mailing or faxing documents containing Nonpublic Personal Information and the Company's proprietary information to ensure that the documents are sent to the intended recipients;
8. Associated Persons may only remove documents containing Nonpublic Personal Information and the Company's proprietary information from The Company's premises for legitimate business purposes. Any documents taken off premises must be handled with appropriate care and returned as soon as practicable; and
9. No records containing personal information shall be removed from the main office without the prior approval of the CCO.

Disciplinary Measures for Violations

A copy of the WISP is to be distributed to each current Associated Person and to each new Associated Person on the beginning date of their employment. It shall be the Associated Person's responsibility for acknowledging in writing that he/she has received a copy of the WISP and will abide by its provisions. Associated Persons are encouraged and invited to advise the CCO of any activities or operations which appear to pose risks to the security of personal information. If the CCO is involved with these risks, Associated Persons are required to advise any other manager or supervisor or business owner.

In the event that an Associated Person is found to have violated the WISP, they will be subject to disciplinary actions including, but not limited to: warnings; reprimands; suspension; termination; and/or referral to regulatory agencies. The nature and scope of the disciplinary action will be determined by the severity of the violation.

Disciplinary action will be applicable to violations of the WISP, irrespective of whether personal data was actually accessed or used without authorization.

Terminated Employees

The CCO will promptly disable system access for any terminated Associated Person. Terminated employees must return all records containing personal data, in any form, in their possession at the time of termination. This includes all data stored on any portable device and/or any data stored on any device owned directly by the terminated employee.

A terminated employee's physical and electronic access to records containing personal information shall be restricted at the time of termination. This shall include remote electronic access to personal records, voice mail, internet, and email access. All keys, key cards, access devices, badges, Company IDs, business cards, and the like shall be surrendered at the time of termination. The CCO will immediately deactivate a terminated employee's password(s) and user ID.

Working in Public Places

Associated Persons should avoid discussing Nonpublic Personal Information and the Company's proprietary information in public places where they may be overheard, such as in restaurants and elevators. Associated Persons should be cautious when using laptops or reviewing documents that contain Nonpublic Personal Information and the Company's proprietary information in public places to prevent unauthorized people from viewing the information.

Access to the Company's Premises

The Company's premises will always be locked. The CCO will review the privacy policies and procedures of third-party service providers, such as building custodians, which have access to the Company's facilities. The Company will maintain a log of individuals with keys to the office, keys to the file room/file cabinet(s), and the alarm code.

Meetings with clients should be held in conference rooms or other locations where Nonpublic Personal Information is not available or audible to others.

Visitors will be supervised while in the Company's office.

Due Diligence of Third-Party Vendors

The Company conducts due diligence of vendors' security through the following means:

1. Reviewing vendors' security policies relating to data privacy; and
2. Ensuring that service contracts require data privacy and computer security;

It shall be the responsibility of the CCO to obtain reasonable confirmation that any Third Party Service Provider or individual that receives, stores, maintains, processes, or otherwise is permitted access to any file containing personal information has implemented a WISP.

Breach of Data Security Protocol

Should any Associated Person know of a security breach at any of our facilities, or that any unencrypted personal information has been lost or stolen or accessed without authorization, or that encrypted personal information, communications and/or physical devices, along with the access code or security key has been acquired by an unauthorized person or for an unauthorized purpose, the Associated Person must notify the CCO.

The CCO shall take such action as is prudent or required by law, including, but not limited to: documenting the breach; notifying clients; notifying police and/or regulatory authorities; blocking access to the affected records (such as by freezing accounts or changing passwords); and taking any other action as may be necessary to protect the personal information.

Incident Response Plan

If any Associated Person becomes aware of an actual or suspected privacy breach, including any improper disclosure of Nonpublic Personal Information and the Company's proprietary information, that Associated Person must promptly notify the CCO. Upon becoming aware of an actual or suspected breach, the CCO will investigate the situation and take the following actions, as appropriate:

1. To the extent possible, identify the information that was disclosed and the improper recipients;
2. To the extent possible, categorize the incident based on operational impact and sensitivity of information involved;
3. Take any actions necessary to prevent further improper disclosures;
4. Take any actions necessary to reduce the potential harm from improper disclosures that have already occurred;
5. Review the data breach notification laws by state for additional information on jurisdictional reporting requirements;
6. Consider discussing the issue with counsel, regulatory authorities, and/or law enforcement officials;
7. Evaluate the need to notify affected clients and make any such notifications;
8. Collect, prepare, and retain documentation associated with the inadvertent disclosure and the

Company's response(s), including post-incident review of events and actions taken, if any; and
9. Evaluate the need for changes to the Company's privacy protection policies and procedures in light of the breach.

Associated Person Training Program
The Company provides guidance and periodic training to employees relating to information security risks and their responsibilities. The Company retains books and records to document the agenda of those training sessions and the topics covered. The Company also retains a list of the employees who attended these training sessions.

Managing a Privacy Breach

Policy
It is the Company's policy to take reasonable steps to prevent a privacy breach.

Responsibility
It is the responsibility of the CCO to administer the Company's privacy breach procedures.

Procedures
A privacy breach means the loss or unauthorized access, collection, use, disclosure, disposal, storage, or other misuse of personal client information. An example of a privacy breach would be personal information becoming lost or stolen or personal information being mistakenly emailed to the wrong person. Privacy breaches are not limited to malicious actions, such as theft or system hacking, but may arise from internal errors that cause accidental loss or disclosure.

The Company will implement the following procedures in an effort to respond effectively to a data breach.

Report the Breach
Any employee who becomes aware of a suspected or actual privacy breach involving client personal information must immediately inform the CCO.

The CCO will verify the circumstances of the possible breach, and will document whether a breach has or has not occurred.

Containing the Breach and Preliminary Assessment
When a breach has been confirmed, the CCO will take the following actions to limit the scope and impact of the breach.

1. Determining what personal client information has been breached;
2. Working with relevant staff members to promptly contain the breach by, for example, stopping the unauthorized practice, recovering the records, shutting down the system that was breached;
3. Determining if this was a one-time occurrence or an ongoing problem; and,
4. In consultation with the senior management, notify the police if the breach involves, or may involve, any criminal activity.

Evaluating the Risks Associated with the Breach
To determine what other steps are immediately necessary, the CCO, working with other Company staff as necessary, will assess the risks associated with the breach. The following factors will be among those considered in assessing the risks:

1. Personal Client Information Involved
    a. Generally, the more sensitive the data, the higher the risk. For example, social security numbers and financial information that could be used for identity theft are examples of highly sensitive personal information.
    b. What possible use is there for the personal information? Can the information be used for fraudulent or otherwise harmful purposes?
2. Cause and Extent of the Breach
    a. What is the cause of the breach?
    b. Is there a risk of ongoing or further exposure?
    c. What was the extent of the unauthorized activity, including the number of likely recipients and the risk of further access, use or disclosure?
    d. How many clients were, or are estimated to be, affected by the breach?
    e. Is the information encrypted or otherwise not readily accessible?
    f. What steps have already been taken to minimize the harm?
3. Parties Affected by the Breach
    a. How many clients were affected by the breach?
    b. Where other parties affected by the breach: employees, service providers, other individuals/organizations?
4. Foreseeable Harm from the Breach
    a. Is there any relationship between the unauthorized recipients and the subject data?
    b. What possible harm to the clients and others will result from the breach?
        i. Harm that may occur includes: physical safety, identity theft or fraud, or loss of business or employment opportunities, hurt, humiliation, damage to reputation or relationships
    c. What harm could result to the Company as a result of the breach?
        i. Loss of trust in the Company
        ii. Loss of assets
        iii. Financial exposure

Notification

The key consideration in deciding whether to notify an affected party is whether notification will avoid or mitigate harm to an individual whose personal information has been inappropriately accessed. The CCO will work with relevant staff members to decide the best approach for notification.

Some considerations in determining whether to notify parties affected by the breach include: contractual or regulatory obligations require notification, and whether there is a risk of identity theft or fraud (usually because of the type of information lost, for example, account numbers, passwords, and social security numbers).

If the Company decides to send a notification, such notification will occur as soon as possible following the breach. However, if law enforcement authorities have been contacted, those authorities will assist in determining the timing and scope of the notification.

Generally, notifications will include the following information:

a. Date of the breach.
b. Description of the breach.
c. Description of the information inappropriately accessed.
d. The steps taken to mitigate the harm.
e. Contact information for the CCO.

Notifying authorities or organizations may also be considered, for example:

a. Police: if theft or other crime is suspected.
b. Insurers or others: if required by contractual obligations.
c. Regulatory bodies: if professional or regulatory standards require notification of these bodies.

Prevention

Once prompt steps are taken to mitigate the risks associated with the breach, the CCO will investigate the cause of the breach. As a result of this evaluation, the Company will implement safeguards designed to prevent a further breach. Policies will be reviewed and updated to reflect any needed changes resulting from the security breach.

Documentation

The Company will maintain documentation to evidence compliance with its procedures as outlined above for at least five years from the date the privacy breach was resolved. Documentation will include, minimally:

a. What happened and when, including who discovered and reported the breach;
b. The data involved and the scope of the breach;
c. Individuals impacted by the breach;
d. Staff members involved in the investigation;
e. Who was notified; and,
f. The corrective actions taken, e.g. update to procedures.

Advisory Services for Government Entities (Pay-to-Play)

Background

Individuals may have important personal reasons for seeking public office, supporting candidates for public office, or making charitable contributions. However, such activities could pose risks to an investment adviser. For example, federal and state "pay-to-play" laws have the potential to significantly limit an investment adviser's ability to manage assets and provide other services to government-related clients.

Rule 206(4)-5 (the "Pay-to-Play Rule") limits political contributions to state and local government officials, candidates, and political parties by registered investment advisers and their Covered Associates. The Pay-to-Play Rule defines "contributions" broadly to include gifts, loans, the payment of debts, and the provision of any other thing of value. Rule 206(4)-5 also prohibits investment advisers and their Covered Associates from providing payments to unregulated third parties to solicit advisory business from any Government Entity and includes a provision that prohibits any indirect action that would be prohibited if the same action was done directly. A violation of any such prohibition could result in lost business opportunities, lost revenue, and/or civil or criminal liability for the Company.

Restrictions on the Receipt of Advisory Fees

The Pay-to-Play Rule prohibits the receipt of compensation from a Government Entity for advisory services for two years following a contribution to any *official of a Government Entity*. This prohibition also applies to "Covered Associates" of the investment adviser. A "Covered Associate" of an investment adviser is defined to include:

- Any general partner, managing member or executive officer, or other individual with a similar status or function;
- Any Associated Person that solicits a Government Entity for the investment adviser, as well as any direct or indirect supervisor of that Associated Person; and
- Any political action committee controlled by the investment adviser or by any person that meets the definition of a "Covered Associate."

There is an exception available for contributions from individuals of $150 per election, or $350 per election if the contributor is eligible to vote in the election. An exception is also available for otherwise prohibited contributions that are returned, so long as the contribution in question is less than $350, is discovered within four months of being given, and is returned within 60 days of being discovered. The exception for returned contributions is available no more than twice per calendar year for investment advisers with 50 or fewer Associated Persons; investment advisers with more than 50 Associated Persons can rely on this exception three times per calendar year. An investment adviser cannot rely on the exception for returned contributions more than once for any particular Associated Person, irrespective of the amount of time that passes between returned contributions.

The restrictions on contributions and payments imposed by Rule 206(4)-5 can apply to the activities of individuals for the two years before they became Covered Associates of an investment adviser. For Covered Associates who are not involved in soliciting clients the look-back period is six months instead of two years.

Restrictions on Payments for the Solicitation of Clients

The Pay-to-Play Rule prohibits the compensation of any person to solicit a Government Entity unless the solicitor is an officer or Associated Person of the investment adviser, or unless the recipient of the compensation (i.e., solicitation fee) is another registered investment adviser or a registered broker/dealer. A registered investment adviser will be ineligible to receive compensation for soliciting Government Entities if the investment adviser or its Covered Associates made, coordinated, or solicited contributions or payments to the Government Entity during the prior two years.

Additional Prohibitions

Investment advisers and its Covered Associates are prohibited from doing anything indirectly which, if done directly, would violate Rule 206(4)-5. This includes coordinating or soliciting any person to make a contribution or payment to an official of the Government Entity, or a related local or state political party.

Recordkeeping Obligations

Paragraph (a)(18) of Rule 204-2 imposes recordkeeping requirements on registered investment advisers that provide advisory services to clients that fall within Rule 206(4)-5's definition of a "Government Entity". Investment advisers with "Government Entity" clients must keep records showing political contributions by "Covered Associates" and a listing of all "Government Entity" clients. Investment advisers that have not provided advisory services to Government Entities or made payment for the solicitation of a Government Entity during the past 5 years are not required to maintain books and records relating to political contributions under Rule 204-2(a)(18).

Guidance Regarding Bona-Fide Charitable Contributions

In Political Contributions by Certain Investment Advisers, Advisers Act Release No. 3043 (July 1, 2010) the SEC indicated that charitable donations to legitimate not-for-profit organizations, even at the request of an official of a Government Entity, would not implicate Rule 206(4)-5.

Applicability of Rule 206(4)-5 to Different Types of Advisory Products and Services Being Offered

The Pay-to-Play Rule applies equally to:

- Investment advisers that provide advisory services to a Government Entity ; and
- Investment advisers that manage a registered investment company (such as a mutual fund) that is an investment option of a plan or program of a Government Entity.

An "official of a Government Entity" means any person (including any election committee for the person) who was at the time of the contribution an incumbent, candidate or successful candidate for elective office of any state or political subdivision of a state, including (i) any agency, authority, or instrumentality of the state or political subdivision, (ii) a pool of assets sponsored or established by the state or political subdivision or agency, (iii) a plan or program of a Government Entity; and (iv) officers, agents or Associated Persons of the state or political subdivision or agency.

Definitions

1. **"Covered Associate"** means any general partner, managing member, executive officer or other individual with a similar status or function and any employee (and his or her supervisor) whose job duties include the solicitation of any Government Entity on behalf of the Company or any Company Affiliate. Covered Associate shall also include any consultant or other independent contractor hired by the Company or Company Affiliate who solicits a Government Entity on behalf of the Company or any Company Affiliate or supervises any Person who performs such activities. The determination of whether a staff person is a Covered Associate shall be made by the CCO.
2. **"Covered Associate Affiliate"** means, as to any Covered Associate, any Person that is directly or indirectly controlled by, or primarily for the benefit of, such Covered Associate, including but not limited to any political action committee (**"PAC"**) under direct or indirect control of such Covered Associate.
3. **"Permitted Contribution"** means any Payment or Payments by a Covered Associate that is a natural person to a Public Official of the State(s) (or subdivisions thereof) where the Covered Associate is entitled to vote and that, in the aggregate, do not exceed $350 per election to any Public Official for whom the Covered Associate is entitled to vote or that do not exceed $150 per election to any Public Official for whom the Covered Associate is not entitled to vote.
4. **"Public Official"** means (i) any individual who is, at the time any Payment is made (or coordination or solicitation of Payments by others occurs), an incumbent, candidate or successful candidate for elective office of a Government Entity; (ii) any individual who is a candidate or successful candidate for federal elective office (President, Vice President, Senator or Member of Congress) if such individual, at the time any Payment is made (or coordination or solicitation of Payments by others occurs) holds an elected or appointed office of a Government Entity; (iii) any Person known to be providing assistance with respect to the candidacy of any of the foregoing, including, but not limited to, any PAC, any inauguration or transition committee, and a local or state political party; and (iv) a foundation or other charitable institution known to be closely associated with any of the foregoing.

Reporting and Pre-Clearance of Political Contributions

This policy applies to any political contribution made directly or indirectly by the Company (or any affiliate thereof) or any "Covered Associate" of the Company to an "*official of a Government Entity*". The Company and its "Covered Associates" are prohibited from making political contributions to any official or candidate of a state or local Government Entity. If the Company or a "Covered Associate" is considering making a political contribution to any state or local Government Entity, official, candidate, political party, or political action committee, the potential contributor must complete and submit to the CCO the *Political Contribution Reporting Form* in advance of making the contribution.

No "Covered Associate" may make a political contribution to an "official of a Government Entity" exceeding $350 per election (if to an official for whom the associate was entitled to vote at the time of the contribution) or exceeding $150 per election (if to an official for whom the associate was not entitled to vote at the time of the contribution).Any political contribution to an "official of a Government Entity" exceeding $350 per election (if to an official for whom the associate was entitled to vote at the time of the contribution) or exceeding $150 per election (if to an official for whom the associate was not entitled to vote at the time of the contribution) must be pre-cleared by the CCO. Covered associates may submit the *Political Contribution Reporting Form* to request such pre-clearance.

Any political contribution by the Company, rather than its "Covered Associates," must be pre-cleared by the CCO, irrespective of the proposed amount or recipient of the contribution.

In considering pre-clearance of a political contribution, the CCO will consider whether the proposed contribution is consistent with this policy and the restrictions imposed by Rule 206(4)-5. To the extent practicable, the CCO will seek to protect the confidentiality of all information regarding each proposed contribution.
Associated Persons may make contributions to national political candidates, parties, or action committees without seeking pre-clearance as long as the recipient is not otherwise associated with a state or local political office and the contributions are not earmarked or known to be provided for the benefit of a particular "official of a Government Entity". Associated Persons should consult with the CCO if there is a question about the propriety of a potential contribution.

Payments to Third Parties

The Company and its Associated Persons shall not pay a third party, such as a solicitor or placement agent, to solicit Government Entity clients on behalf of the Company, unless that third party is an executive officer, general partner, managing member (or similar status) or employee of the Company, or an SEC-registered investment adviser in compliance with Rule 206(4)-5.

Public Office

Associated Persons must obtain written pre-approval from the CCO prior to running for any public office. Associated Persons may not hold a public office if it presents any actual or apparent conflict of interest with the Company's business activities.

Disclosure of Political Contributions by New Hires

Any potential new hire is required to disclose all political contributions for the two-year period prior to the date of employment. Political contributions made by such person during the two-year period prior to the date of employment will be attributed to the Company unless otherwise determined by the CCO.

New Associated Persons must submit a *New Hire Political Contribution Reporting Form* upon being hired by the Company, disclosing any political contributions made during the two (2) years prior to employment by the Company.

Oversight of Service Providers

Background

Investment advisers are fiduciaries and thus must act in their clients' best interests. The Company may contract with vendors to perform certain functions for the Company. While the Company may never contract its supervisory and compliance activities away from its direct control, it may outsource certain activities that support the performance of its supervisory and compliance responsibilities. Such activities may include custodians, broker/dealers, sub-advisers, email retention providers, accounting/finance (payroll, expense account reporting), legal and compliance, information technology, operations functions (statement production, disaster recovery services), and administration functions (human resources, internal audits).

Policies and Procedures

The CCO will oversee the Company's service providers that impact its operations or that could pose a risk to the Company's operations or its clients. The CCO should be familiar with each service provider's operations and understand the aspects of their operations that expose the Company to compliance risks.

Evaluating New Service Providers

The selection of a service provider will depend, in large part, on the services needed by the Company and the service provider's ability to fulfill those needs. Each service provider agreement should clearly outline the scope of the provider's responsibilities.

When evaluating a service provider for the first time, the CCO will review and consider the following information, as applicable:

1. The service provider's history and reputation in the industry, including the experiences of similar entities serviced by this provider and the provider's history of client retention;
2. The service provider's financial condition and ability to devote resources to the Company;
3. Recent corporate transactions (such as mergers and acquisitions) that involve the service provider;
4. The level of service that will be provided to the investment adviser;
5. The nature and quality of the services to be provided;
6. The experience and quality of the staff providing services and the stability of the workforce;Tthe service provider's operational resiliency, including its disaster recovery and business continuity plans;
7. The technology and process it uses to maintain information security, including the privacy of customer data;
8. The service provider's communications technology;
9. The service provider's insurance coverage; and
10. The reasonableness of fees in relation to the nature of the services to be provided.

Where potential conflicts of interest exist, the CCO must evaluate the extent to which such potential conflicts are mitigated.

Evaluating Service Provider Agreements

Written contracts should properly document the terms of service provided and the protection of confidential information. Such contracts must be maintained, current, and available for review by regulators, when requested. In the event the service provider has, or will have, access to material nonpublic information, if the contract does not contain a confidentiality agreement, the Company must obtain a separate agreement to be maintained in the file with the vendor contract.

Ongoing Oversight of Service Providers

The CCO shall be responsible for monitoring all service providers to ensure compliance with the terms and conditions of the Company's contract. At least annually, the CCO should review, as applicable:

1. The service provider's financial condition and ability to devote resources to the Company;
2. Recent corporate transactions (such as mergers and acquisitions) that involve the service provider;
3. The level of service provided to the investment adviser;
4. The reasonableness of fees in relation to the nature of the services to be provided;
5. The potential for conflicts of interest that could unfairly benefit the Company or others to the detriment of clients;
6. The experience and quality of the staff providing services and the stability of the workforce;
7. The service provider's operational resiliency, including its disaster recovery and business continuity plans;
8. The technology and process it uses to maintain information security, including the privacy of customer data; and
9. The service provider's communications technology.

Where potential conflicts of interest exist, the CCO must evaluate the extent to which such potential conflicts are mitigated.

Evaluating Potential Conflicts of Interest

In evaluating service provider arrangements, the Company and CCO should be alert for any arrangements that could unfairly benefit the investment adviser or others to the detriment of the Company or its clients. When evaluating an arrangement with an affiliated service provider that in turn subcontracts to an unaffiliated service provider, the Company and CCO shall inquire about the respective roles of the two entities and whether management or the affiliated service provider receives any benefit, directly or indirectly, other than the fees payable under the contract. The CCO must evaluate the fees paid to the affiliated and any unaffiliated service provider relative to the services each will perform.

Conflicts of interest also may arise in arrangements with unaffiliated service providers. The Company shall also inquire about other business relationships between affiliates of the investment adviser and the service provider or any of the service provider's affiliates.

Diminished Capacity or Abuse of Vulnerable Clients

Background

As a fiduciary the Company is obligated to act in the best interests of it clients. The Company recognizes that if existing or prospective clients suffer from diminished mental capacity, they may lack the ability to make knowledgeable and prudent investment decisions. Therefore, it is the Company's policy to ensure that all existing and prospective clients, and/or their authorized representatives, understand the nature and effect of the business being transacted. The Company's policy is also designed to identify red flags indicative of fraudulent activity or financial abuse of a vulnerable client and to take such actions as are reasonable and appropriate to involve the proper authorities and or client representatives to protect such clients from financial harm.

A "senior" or "elderly" investor is defined as any retail advisory client who is age 62 or older, retired, or transitioning to retirement, and retail clients in joint accounts with at least one individual meeting this definition. Although senior, or elderly, investors are the most common types of clients who might suffer from diminished mental capacity, or be at risk of financial exploitation or abuse, vulnerable clients can include minors and individuals suffering from any number of disabilities at any age. Consequently, this policy is not limited to senior or elderly clients.

The absence of, or lack of explicit reference to, a specific type of activity does not limit the extent of the application of this policy. Where no policy or guideline exists, or if you are unsure about whether you can take instructions from a client, non-client, or purported representative of a client, ask the CCO. Do not guess at the answer.

Policies and Procedures

Depending on the specific transaction or decision at issue, as well as the jurisdiction in which one is located, legal capacity has multiple definitions which are set forth in state statutory and/or case law. The most common definition which the Company is likely to encounter is in determining the client's "contractual capacity." That is generally defined as an individual's ability to understand the nature and effect of the act and business being transacted. The more complicated the transaction is, the higher the level of understanding that may be needed to comprehend its nature and effect.

"Red Flags" indicative of an investor's possible diminished capacity or reduced ability to handle financial decisions include, but are not limited to, the following. The investor:

1. appears unable to process simple concepts;
2. appears to have memory loss;
3. appears to have difficulty speaking or communicating;
4. appears unable to appreciate the consequences of decisions;
5. makes decisions that are inconsistent with his or her current long-term goals or commitments;
6. is subject to significant mood swings or otherwise displays erratic behavior;
7. refuses to follow appropriate investment advice (this may be of particular concern when the advice is consistent with previously-stated investment objectives);
8. appears to be concerned or confused about missing funds in his or her account, where reviews indicate there were no unauthorized money movements or no money movements at all;
9. is not aware of, or does not understand, recently completed financial transactions;
10. appears to be disoriented with surroundings or social setting; and
11. appears uncharacteristically unkempt or forgetful.

Procedures - Diminished Capacity

Where a client or prospective client exhibits signs of diminished mental capacity and/or a cognitive impairment, or otherwise appears to lack the capacity to understand an investment or to provide informed consent, the Associated Person working with that individual should implement the following escalation procedures:

1. Discuss the situation with a supervisor and/or the CCO;
2. If the Associated Person has not notified the CCO, the supervisor should ensure that the CCO is informed;
3. Check whether an executed trading authorization form, durable power of attorney, or other guardianship appointment form is on file. Also check to verify whether the client has named a trusted contact person. If so, consider contacting the agent, attorney or guardian and/or trusted contact person;
4. If appropriate, suggest that the client bring a close family member or friend to the next meeting;
5. The CCO will determine whether it is necessary to consult with legal counsel. If there is a trading authorization, durable power of attorney form, or guardianship appointment form on file, legal counsel should be consulted if there is any uncertainty whatsoever as to the applicability or legitimacy of those documents. Otherwise, the attorney-in-fact, guardian, or other authorized representative or trusted contact person should be contacted to discuss the Associated Person's/CCO's concerns; and
6. In the event that the client declines to bring a family member or friend with them and there is no trading authorization or durable power of attorney form on file, legal counsel should be consulted to determine the extent to which further escalation is warranted or required.

Further escalation procedures may include one or more of the following:

1. Contacting the client's spouse and/or requesting a joint meeting, particularly if the situation involves a joint account;
2. Contacting the client's adult child(ren) and/or requesting a joint meeting; and/or
3. Contacting local state, county or city Eldercare agency or such other local agency that may have responsibility over vulnerable individuals such as a local mental health resources agency.

In the event that further escalation is warranted or required, legal counsel should be consulted regarding potential privacy concerns. (See Privacy Issues below).

Financial Exploitation or Abuse

Financial exploitation or abuse occurs when somebody exploits a position of influence or trust over a vulnerable person to gain access to that person's assets, funds or property.

"Red Flags" indicative of financial exploitation or abuse include, but are not limited to, the following:

1. Sudden reluctance to discuss financial matters;
2. Sudden, atypical, or unexplained withdrawals or other changes in financial situation;
3. Abrupt changes in wills, trusts, or power of attorney;
4. Changes in beneficiaries on insurance policies or IRAs;
5. Increasing lack of contact with, and interest in, the outside world;
6. Admission of financial or material exploitation or suspected exploitation;
7. Concern or confusion about missing funds in his or her account;
8. Unusual or first-time wire transfers, especially to foreign countries;
9. Fear of eviction or nursing home placement if money is not given to a caretaker; and
10. Appearance of insufficient care despite having money.

Procedures - Financial Exploitation or Abuse

Even if abuse is only suspected, such suspicion is sufficient reason to escalate the matter to a supervisor or CCO. Where a client or prospective client appears to be the victim of financial exploitation or abuse:

1. Discuss the situation with a supervisor and/or the CCO immediately;
2. If the Associated Person has not notified the CCO, the supervisor should ensure that the CCO is informed;
3. Check whether an executed trading authorization form, durable power of attorney, or other guardianship appointment form or trusted contact person is on file. If so, determine whether the alleged perpetrator of the abuse is the agent, attorney, trusted contact person or guardian listed therein;
4. If the alleged perpetrator of the abuse is **not** the agent, attorney, trusted contact person, or guardian listed therein, contact them and alert them to the situation; and
5. If the alleged perpetrator of the abuse **is** the agent, attorney, trusted contact person, or guardian listed therein or if there is no executed trading authorization form, durable power of attorney, trusted contact person, or other guardianship appointment form on file, legal counsel should be contacted in order to determine the appropriate escalation.

Further escalation may include:

1. Contacting the client and requesting a meeting;
2. Contacting the client's spouse and requesting a meeting;
3. Contacting the client's adult child(ren) and/or requesting a joint meeting; and
4. Contacting local state, county or city police and/or Eldercare agency or such other local agency that may have responsibility over vulnerable individuals.

In the event that further escalation is warranted or required, legal counsel should be consulted regarding potential privacy concerns. (See Privacy Issues below).

To report elder abuse, contact the Adult Protective Services ("APS") agency in the state where the elder resides. The APS reporting number can be found for each state by visiting:

1. The State Resources section of the National Center on Elder Abuse website https://www.elderabusecenter.org/
2. The Eldercare Locator website or calling 1-800-677-1116. https://eldercare.acl.gov/Public/Index.aspx

Privacy Issues

In general, Regulation S-P and applicable state law prohibit the disclosure of any Nonpublic Personal Information about a consumer to a non-affiliated third party unless the Company has provided the consumer with an opt out notice and a reasonable opportunity for the consumer to opt out. However, the requirements for initial notice and the opt out do not apply when the Company discloses Nonpublic Personal Information under certain circumstances, including, but not limited to:

1. With the consent or at the direction of the consumer, provided that the consumer has not revoked the consent or direction;
2. To protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability;
3. For required institutional risk control or for resolving consumer disputes or inquiries;
    a. To persons holding a legal or beneficial interest relating to the consumer; or
    b. To persons acting in a fiduciary or representative capacity on behalf of the consumer;

4. To comply with federal, state, or local laws, rules and other applicable legal requirements;
5. To comply with a properly authorized civil, criminal, or regulatory investigation, or subpoena or summons by federal, state, or local authorities; or
6. To respond to judicial process or government regulatory authorities having jurisdiction over the Company for examination, compliance, or other purposes as authorized by law.

Therefore, depending on the circumstances, if a client is suffering from diminished mental capacity or is being taken advantage of, the Company may be able to disclose certain information to relatives, representatives, or government agencies without being in violation of Regulation S-P or applicable state privacy laws. In some states, investment advisers are required by law to report suspected financial abuse of the elderly and other vulnerable adults to state authorities. Associated person should not make such a determination, but, rather, only in consultation with the CCO and legal counsel. Any Nonpublic Personal Information so disclosed should be limited to only the amount necessary to protect the client or required by law.

Recordkeeping Requirements

The Associated Person must document what steps were taken in situations where an existing or prospective client exhibited signs of diminished mental capacity and/or a cognitive impairment. Legal and compliance personnel should create similar documentation relating to their involvement.

Privacy Policy/Regulation S-P

Background

Reg S-P requires the Company to provide its individual clients with notices describing its privacy policies and procedures. These privacy notices must be delivered to all new individual clients upon entering into an advisory agreement, and thereafter as required under applicable federal or state law. Reg S-P does not require the distribution of privacy notices to companies or to individuals representing legal entities.

In addition to Reg S-P, certain states have adopted consumer privacy laws that may be applicable to investment advisers with clients who are residents of those states.

Policies and Procedures

The Company views protecting private information regarding its clients and potential clients as a top priority. Pursuant to the requirements of the Gramm-Leach-Bliley Act (the "GLBA") and guidelines established by the Securities Exchange Commission regarding the Privacy of Consumer Financial Information (Regulation S-P), the Company has instituted the following policies and procedures in an effort to ensure that such nonpublic private information is kept private and secure. The CCO is responsible for administering these policies and procedures. This privacy policy covers the practices of the Company and applies to all nonpublic personally identifiable information, including information contained in consumer reports of the Company's current and former clients.

Associated Persons will maintain the confidentiality of information acquired in connection with their employment with particular care being taken regarding Nonpublic Personal Information. Improper use of the Company's proprietary information, including Nonpublic Personal Information, is cause for disciplinary action, up to and including termination of employment for cause and referral to appropriate civil and criminal legal authorities.

The Company will seek to limit its collection of Nonpublic Personal Information to that which is reasonably necessary for legitimate business purposes. The Company will not disclose Nonpublic Personal Information except in accordance with these policies and procedures, as permitted or required by law, or as authorized in writing by a client. The Company will never sell Nonpublic Personal Information.

With respect to Nonpublic Personal Information, the Company will strive to: (a) ensure the security and confidentiality of the information; (b) protect against anticipated threats and hazards to the security and integrity of the information; and (c) protect against unauthorized access to, or improper use of, the information. The CCO is responsible for administering these policies and procedures. Notify the CCO promptly of any threats to, or improper disclosure of, Nonpublic Personal Information.

Although these principles and the following procedures apply specifically to Nonpublic Personal Information, Associated Persons must be careful to protect all of the Company's proprietary information.

Information Practices

The Company limits the use, collection, and retention of client or potential client information to what the Company believes is necessary or useful to conduct its business or to offer quality products, services, and other opportunities that may be of interest to its clients or potential clients.

Disclosure of Nonpublic Personal Information

Associated Persons should take reasonable precautions to confirm the identity of individuals requesting Nonpublic Personal Information. Associated Persons must be careful to avoid disclosures to identity thieves who may use certain Nonpublic Personal Information, such as a social security number, to convince an Associated Person to divulge additional information. Any contacts with suspected identity thieves must be reported promptly to the CCO.

1. Each Associated Person has a duty to protect the Nonpublic Personal Information of clients collected by the Company;
2. Each Associated Person has a duty to ensure that Nonpublic Personal Information of the Company's clients is shared only with Associated Persons and others in a way that is consistent with the Company's privacy notice and the procedures contained in this Policy;
3. Each Associated Person has a duty to ensure that access to Nonpublic Personal Information of the Company's clients is limited as provided in the privacy notice and this policy; and
4. No Associated Person is authorized to sell, on behalf of the Company or otherwise, nonpublic information of the Company's clients.

Associated Persons with questions concerning the collection and sharing of, or access to, Nonpublic Personal Information of the Company's clients must look to the CCO for guidance.

In certain circumstances, Regulation S-P permits the Company to share Nonpublic Personal Information about its clients with non-affiliated third parties without providing an opportunity for those individuals to opt out. These circumstances include sharing information with a non-affiliate (1) as necessary to effect, administer, or enforce a transaction that a client requests or authorizes; (2) in connection with processing or servicing a financial product or a service a client authorizes; and (3) in connection with maintaining or servicing a client account with the Company.

Nonpublic Personal Information may only be provided to third parties under the following circumstances:

1. To accountants, lawyers, and others as directed in writing by clients;
2. To specified family members as directed in writing by clients, or as authorized by law;
3. To third-party service providers, as necessary to service client accounts; and
4. To regulators and others, as required by law.

To the extent practicable, Associated Persons will seek to remove nonessential Nonpublic Personal Information from information disclosed to third parties. Social security numbers must never be included in widely distributed lists or reports.

Prior to providing any third-party service provider with access to personal information about individual clients who are residents of Massachusetts, the Company will require, by contract, third-party service providers who may have access to such clients' information to implement and maintain appropriate security measures to protect such clients' personal information consistent with Massachusetts Standards for Protecting Personal Information (201 CMR 17.00) and any applicable federal regulations.

Service Providers

From time to time, the Company may have relationships with non-affiliated third parties (such as attorneys, auditors, accountants, brokers, custodians, and other consultants), who, in the ordinary course of providing their services, may require access to information containing nonpublic information. These third-party service providers are necessary for the Company to provide our investment advisory services. When the Company is not comfortable that service providers (e.g., attorneys, auditors, and other financial institutions) are already bound by duties of confidentiality, the Company requires assurances from those service providers that they will maintain the confidentiality of nonpublic information they obtain from or through the Company. In addition, the Company selects and retains service providers that it believes are capable of maintaining appropriate safeguards for nonpublic information, and the Company will require agreements from its service providers that they will implement and maintain such safeguards.

Processing and Servicing Transactions

The Company may also share information when it is necessary to effect, administer, or enforce a transaction requested or authorized by clients. In this context, "necessary to effect, administer, or enforce a transaction" includes what is required or is a usual, appropriate, or acceptable method:

1. To carry out the transaction or the product or service business of which the transaction is a part, and record, service, or maintain the client's account in the ordinary course of providing the financial service or financial product;
2. To administer or service benefits or claims relating to the transaction or the product or service of which it is a part; and
3. To provide a confirmation, statement, or other record of the transaction, or information on the status or value of the financial service or financial product to the client or the client's agent or broker.

Sharing as Permitted or Required by Law to Non-Affiliated Third Party

The Company may disclose information to non-affiliated third parties as required or allowed by law. For example, this may include disclosures in connection with a subpoena or similar legal process, a fraud investigation, recording of deeds of trust and mortgages in public records, or an audit or examination.

Privacy Policy Notice

The Company has developed a privacy notice, as required under Regulation S-P, to be delivered to clients. The notice discloses the Company's information collection and sharing practices and other required information. The notice will be revised as necessary any time information practices change.

Privacy Notice Delivery

Investment advisers are required to deliver a copy of their privacy notice at certain points in the investment adviser-client relationship.

Initial Privacy Notice - As regulations require, all new clients receive an initial privacy notice at the time the client relationship is established (i.e., upon execution of the agreement for services).

Annual Privacy Notice - The Company only provides Nonpublic Personal Information to non-affiliated third-parties as permitted by the following exceptions:

1. To accountants, lawyers, and others as directed by the client;
2. To specified family members as directed by clients or as authorized by law;
3. To a third-party service provider, as necessary to provide services requested or authorized by the client;
4. To a third-party service provider who performs services for the Company pursuant to an

agreement prohibiting disclosure of client information, except as necessary to perform the services; and

5. To regulatory authorities and others, as required by law.

Accordingly, the Company will not be required to provide an annual privacy notice to a client unless it has changed its privacy policies since the privacy notice was last provided to the client. In any year in which the Company either changes its privacy policies or discloses Nonpublic Personal Information to non-affiliated third-parties outside of the exceptions described above, then it will send an annual privacy notice to its clients.

The CCO oversees the distribution of the initial and any required annual privacy notices and will maintain a record of the dates of delivery and the identification of recipients of annual privacy notices.

Revised Privacy Notice

If there is a change in the Company's collection, sharing, or security practices, Regulation S-P requires that the Company amend its privacy policy and promptly distribute a revised privacy notice to existing clients.

Joint Relationships

If two or more individuals jointly obtain a financial product or service from the Company, the Company may satisfy the initial, annual, and revised notice requirements by providing one notice to those individuals jointly.

Custody

Background

Definition of Custody

Rule 206(4)-2 under the Advisers Act (the "Custody Rule") imposes certain requirements on investment advisers that have custody of client funds or securities. The rule defines custody as holding, directly or indirectly, client funds or securities, or having any authority to obtain possession of them. Custody includes:

- Actual possession of client funds or securities;
- Any arrangement (including a general power of attorney or a standing letter of authorization) under which an investment adviser is authorized or permitted to withdraw client funds or securities upon instruction to a custodian;
- Any capacity (such as general partner of a limited partnership, a comparable position for another type of pooled investment vehicle, or a trustee of a trust) that gives an investment adviser or any Associated Person legal ownership of, or access to, client funds or securities;
- Custody by a related person in connection with advisory services provided to the investment adviser's clients; and
- When the custodial agreement authorizes the investment adviser to withdraw client funds or securities upon the investment adviser's instructions to the custodian (notwithstanding a provision in the advisory agreement to the contrary), unless the investment adviser drafts a letter to the custodian limiting the investment adviser's authority to "delivery versus payment" and the client and custodian provide written consent acknowledging the new arrangement.

Custody Does Not Include:

- First-party transfers (i.e. authority to direct the transfer of funds among a client's own accounts) (affiliated custodian): the Company's written authority to transfer client assets between the client's own accounts at the same qualified custodian or between affiliated qualified custodians when both custodians have access to the sending and receiving account numbers and client account name (e.g., to make first-party journal entries).
- First-party transfers (non-affiliated custodian): the Company's limited authority to transfer a client's assets between the client's own accounts maintained at one or more qualified custodians, provided the client has authorized the investment adviser in writing to make such transfers, and a copy of that authorization is provided to the sending custodian. The client's signed written authority to the sending custodian must include the name and account numbers for sending and receiving accounts (including the ABA routing number(s) or name(s) of the receiving custodian), such that the sending custodian has identified the accounts for which the transfer is being effected as belonging to the client. The authorization does not need to be provided to the receiving custodian.
- Remittance of funds or securities to client: the Company's written authority to instruct a qualified custodian to remit funds or securities from a client's account to the same client at his or her address of record provided:
    - a copy of the written authorization is provided to the qualified custodian,
    - the Company has no authority to open an account on behalf of the client; and
    - the Company has no authority to designate or change the client's address of record with the qualified custodian.

Custody Requirements

It is a fraudulent, deceptive, or manipulative act, practice or course of business under Rule 206(4)-2 for an investment adviser to have custody of client funds or securities unless:

- **Qualified Custodian.** A qualified custodian maintains those funds and securities either in a separate account for each client under that client's name, or in accounts that contain only the investment adviser's clients' funds and securities under the investment adviser's name as agent or trustee for the clients.
- **Notice to Clients.** If the investment adviser opens an account on the client's behalf with a qualified custodian, the investment adviser must notify the client in writing of the qualified custodian's name, address, and the manner in which the funds or securities are maintained, promptly when the account is opened and following any changes to this information. If the investment adviser sends account statements to a client to which the investment adviser is required to provide this notice, the investment adviser must include in the notification provided to that client and in any subsequent account statement sent to that client a statement urging the client to compare the account statements from the custodian with those from the investment adviser.
- **Account Statements to Clients.** The investment adviser has a reasonable basis, after due inquiry, for believing that the qualified custodian sends an account statement, at least quarterly, to each client for which it maintains funds or securities, identifying the amount of funds and of each security in the account at the end of the period and setting forth all transactions in the account during that period.
- **Surprise Examination.** The client funds and securities of which the investment adviser has custody are verified by an independent surprise examination at least once during each calendar year by an independent public accountant. The first examination must occur within six months of the investment adviser becoming subject to the requirement.
- **Investment Advisers Acting as Qualified Custodians.** If the investment adviser maintains, or if it has custody because a related person maintains, client funds or securities pursuant to Rule 206(4) as a qualified custodian in connection with advisory services provided to clients, the independent public accountant retained to perform the required independent surprise examination must be registered with the Public Company Accounting Oversight Board ("PCAOB"). The investment adviser must obtain, or receive from the related person, within six months of becoming subject to Rule 206(4)-2 and thereafter no less frequently than once each calendar year, a written internal control report prepared by an independent public accountant in compliance with Rule 206(4)-2.

Policies and Procedures

As the Company is not deemed to have custody of client funds or securities, custody compliance obligations are not applicable. Should the Company acquire custody of client funds or securities, it will adopt a policy to comply with federal or state requirements regarding custody, as applicable.

Deduction of Advisory Fees from Client Accounts

Investment advisers deducting fees from client accounts are deemed to have limited custody. Deduction of fees by investment advisers presents the risk that the investment adviser or its personnel could deduct fees to which the investment adviser is not entitled under the terms of the advisory contract, which would violate the contract and which may constitute fraud under the Advisers Act.

The Company's advisory fees are debited directly from client accounts. Payment of the Company's advisory fees will be made by the qualified custodian, as that term is defined below, holding the client's funds and securities. In all such cases, the client must provide written authorization permitting the fees

to be paid directly from their account. The Company will not have access to client funds for payment of fees without written client consent. Further, the qualified custodian must agree to deliver quarterly account statements directly to the client, and never through the Company.

The Company's CCO or designee shall periodically review, on a sample basis, fee calculations to determine their accuracy based on how and when clients are billed and to ensure that the fee calculation is consistent with the client's advisory agreement and the amount of assets under the Company's management. To the extent practical, duties shall be segregated between those personnel responsible for: (1) processing invoices sent to the custodian and/or clients, as applicable; (2) reviewing the invoices for accuracy; and (3) reconciling invoices with deposits of advisory fees by custodians into the Company's account.

Note: Investment advisers are not required to obtain an independent surprise examination of client funds and securities maintained by a qualified custodian if the investment adviser has custody of the funds and securities solely as a consequence of the investment adviser's authority to make withdrawals from client accounts to pay advisory fees, provided the investment adviser is not a related person of the custodian.

The CCO shall ensure that the Company receives copies of statements sent to clients by the qualified custodian. The CCO shall ensure that the amount of a client's assets under management on which the fee is billed is accurate and has been reconciled with the assets under management reflected on the statement provided by the qualified custodian. The CCO shall also ensure that clients are billed accurately in accordance with the terms of their advisory contracts.

To accomplish this, the CCO will conduct quarterly testing of fee calculations for client accounts to determine accuracy consistent with client contracts. Copies of reconciliation work papers shall be maintained by the CCO in the applicable files.

Inadvertent Receipt of Client Funds or Securities

If the Company inadvertently receives client funds or securities, the Company will return the client's funds or securities to the sender without assuming custody by taking the following steps:

1. When the Company inadvertently receives funds/securities, a photocopy of the check or securities received will be made and placed in the client's file.
2. The Company will return the funds/securities to the sender with a letter of instruction regarding how and where the sender should forward funds/securities in the future. The Company will return such funds or securities by US Mail (registered, return receipt requested) or by courier service within three business days of receipt.
3. The Company will keep a copy of the cover letter and the return receipt/courier notice in the client file.

Upon inadvertent receipt of securities from client or other third party, the CCO is to be notified promptly and an entry made in a log maintained for that purpose. The securities should be immediately, but in any case, within three (3) business days following receipt, returned to the sender.

Upon inadvertent receipt of securities from client or other third party, securities may be forwarded to the client, former client, or Qualified Custodian, provided that the investment adviser promptly identifies the inadvertently received client assets and the client or former client to whom such assets are attributable. The Company shall maintain and preserve records of all inadvertently received client assets, including a written explanation of whether and when the assets were forwarded to the client, former client, Qualified Custodian, or original sender, as applicable.

In an SEC staff letter issued to the Investment Adviser Association on September 20, 2007, the Division of Investment Management noted that it would not recommend enforcement action against an investment adviser that instead of returning to sender, promptly forwarded tax refunds received from tax authorities or settlement proceeds received from administrators or issuers in connection with class action lawsuits to the investment adviser's client or a qualified custodian within five business days of receipt. An investment adviser relying on this SEC staff letter must adopt and implement policies and procedures to:

- Promptly identify inadvertently received client assets;
- Promptly identify the client or former client to whom such assets are attributable;
- Promptly, but in any case within five business days following receipt, forward the assets to the client, former client, or Qualified Custodian, as appropriate; and
- Maintain and preserve appropriate records of all inadvertently received client assets, including a written explanation of whether and when the assets were forwarded to the client, former client, Qualified Custodian, or original sender, as applicable.

Receipt of Third Party Funds

If the Company receives a check from a client payable to a third party such as a custodian, the Company will make a photocopy of the check, and then forward the check directly to the third party. A copy of the check and the transmittal form will be kept in a master custody file.

Notice of Qualified Custodian

If the Company opens an account with a qualified custodian on behalf of Company clients, either under the client's name or under its name as agent, the Company will ensure that the client is promptly notified in writing of the qualified custodian's name, address, and the manner in which the client funds or securities are maintained when the account is opened and following any changes to this information.

Account Statements

A qualified custodian is required to send quarterly account statements containing at least the information required by the applicable rules directly to the client (and not through the Company). The Company will instruct the client to request that a copy of the quarterly accounting statements be sent to the Company, or the Company will have access to the statements via a web portal provided by the qualified custodian.

If the Company sends account statements to clients, in addition to the statements provided by the qualified custodian, the Company must include in the notification to clients, and in any subsequent account statements sent to clients, a statement urging clients to compare account statements from the qualified custodian with those from the Company.

Definition of Qualified Custodians

Qualified custodians include banks, savings associations, SEC registered broker-dealers, futures commission merchants, and foreign financial institutions that customarily hold financial assets for its customers.

Use of Independent Representative

In the event the client does not wish to receive account statements, the Company will require the client to submit such request in writing. The client must designate an independent representative to receive those statements. A record of such request will be kept in the client's file.

An independent representative is defined as a person that (i) Acts as agent for a client and by law or contract is obliged to act in the best interest of the client or the limited partners (or members, or other beneficial owners); (ii) Does not control, is not controlled by, and is not under common control with the Company and (iii) Does not have, and has not, within the past two years, a *material* business relationship with the Company.

Account Opening and Closing Procedures

Policy

Employees may open an account at a client's request provided that procedures governing such accounts are followed. Conversely, terminated client accounts must be removed from our custodial platforms as soon as practicable.

When a new client relationship is established, the Company will gather sufficient information about the client to determine the investment advice that should be provided.

Responsibility

Several individuals may be responsible for various aspects of opening and closing a client account.

Procedures for Opening a New Advisory Account

1. Client accounts will not be managed unless client signs an agreement for the relevant services with the Company.
2. If applicable, the Company and new clients must complete forms to authorize the transfer of client assets to the broker/custodian agreed upon by client and advisor.
3. The Company and new clients must complete new account forms that are required by the broker. The forms may provide the Company with the authorization to trade on behalf of the client (limited power-of-attorney) and may also grant the Company the ability to directly debit advisory fees from the client's custodial account.
4. The Company must obtain and document information from the client for the purpose of determining investment suitability and investment objectives. Typically, an investment questionnaire is completed by the client with help from the advisory representative servicing the account.
5. The Company must note and document any client-imposed investment restrictions.
6. The Company must enter data into its system to include the client's account. Additionally, the Company must develop a file for the client, which includes, among other things: the advisory agreement, investment policy statements and correspondence, if any. Files may be electronic in whole or in part. Brokerage Statements & confirms may be kept electronically (and easily accessible if not in client file).
7. The Company must furnish new clients with Part 2 of Form ADV and the Company's Privacy Notice no later than when the client executes the advisory agreement.

Unacceptable Clients

The following types of prospective clients generally will not be accepted by the Company as a client:

1. A person under the age of majority unless represented by a legal guardian.
2. A person who has been determined to be legally incompetent unless represented by a legal guardian.
3. A person with a fictitious name unless a legal name is also provided.
4. A person who refused to disclose necessary information required by account opening documents.

Updating Client Information

The Company will maintain current information about each client. The client is responsible for proactively informing the Company regarding changes in their investment needs, goals, objectives, risk tolerance, restrictions, and financial situations.

The Company will, at least annually, request that each client, in writing, provide updated account information, as noted above. Upon written notice of changes in the client's information, the Company will promptly update the client's information.

Summary Procedures for Closing a Terminated Client Account

1. The Company is informed of a client termination by i) receiving a letter directly from the client with termination instructions (particularly on any position liquidations); or ii) verbal instructions from the client. If the client communicates this information verbally to the Company, a letter (written or electronic) is sent to the client stating that the Company acknowledges the client's desire to terminate, the date of termination, and fee payment/rebate instructions.
2. Upon notification to the Company all active management of the account assets will stop. The client may have instructed the Company to liquidate certain positions in the account prior to closing. The Company will complete the trades to the best of its ability, taking into account the effects on the price at which the securities will be liquidated.
3. The Company calculates the pro rata fee for the period based upon the client termination date.
4. Documentation showing the specific manner in which the pro rata fee was calculated, how the amount due from/payable to was identified, and a copy of the check/fee reimbursement-transfer (from the Company account to Client account)/wire instructions is maintained in the client file (or electronically on the Company's portfolio management system). The Company may furnish the terminated client with a final letter (can be electronic) memorializing the termination instructions (as discussed above) and effective date of termination.
5. The CCO will be responsible for removing the client from the Company's master custodial account.
6. All information relating to the management of a terminated client's account must be maintained in accordance with the Advisers Act (i.e. 5 years from the end of the fiscal year in which the account terminated), and the terminated client's investment returns must remain in the Company's performance composite through the last full quarter in which the account was managed.
7. The Company must cooperate with any account transfer instructions received from the terminated client, and act to complete an account transfer efficiently and expeditiously.

Model Portfolios

It is the Company's policy to allocate discretionary portfolio management assets to certain proprietary model portfolios where the portfolio manager believes such investments are in the client's best interest. In order to rely on the safe harbor under Rule 3a-4 from the definition of Investment Company, the Company shall meet the following conditions designed to ensure that participating clients receive individualized treatment.

1. Provide all prospective clients with a copy of Part 2A or its most recent Form ADV (or an equivalent disclosure brochure) and/or such other disclosures as may be required by the state in which the client is solicited, if applicable;
2. Obtain information from the client that is necessary to manage such client's account on the basis of his or her financial situation, investment objectives, and instructions;
3. The Company may choose not to accept instructions from the client on the management of the account by the Company, including the designation of particular securities or types of securities that should not be purchased for the account, or that should be sold if held in the account.
    a. The Company retains the discretion to decline any client account for any reason, including, without limitation, the imposition of restrictions or conditions on the account that the Company deems unacceptable;
4. Be reasonably available to consult with each client;

5. At least annually, the Company shall contact the client to determine if there have been any changes in the client's financial condition, investment objectives, or instructions to the Company concerning the client's account, and whether the client wishes to impose any reasonable restrictions or modify existing restrictions on the account;
6. At least quarterly, the Company notifies the client in writing to contact the Company if there have been changes in the client's financial situation or investment objectives, or if the client wishes to impose any reasonable restrictions on the management of the client's account or reasonably modify existing restrictions, and provides the client with a means through which such contact may be made. This notification may be included on quarterly statements sent to the client, or through other written notice or client communication.
7. Personnel of the Company, who are knowledgeable about the client's account and its management must be reasonably available to the client for consultation; and
8. The Company will ensure that each client retains ownership of the securities and funds in his or her account, including, without limitation, the right to withdraw securities or cash, pledge securities, vote securities, be provided in a timely manner with all confirmations of securities transactions, and proceed directly as a security holder against the issuer of any security in the client's account and not be obligated to join the Company as a condition precedent to initiating such proceeding.

The custodian holding the client's funds and securities will provide each client with periodic statements (including all account holdings, contributions and withdrawals, and the value of the account at the end of the statement period).

With regard to client investments in proprietary models, the client must have the same rights over the securities in the account as if they held those securities in their own name, including the rights to:

1. Withdraw securities or cash;
2. Vote (or choose a proxy vote) on securities in the account;
3. Proceed directly as a security holder against the issuer; and
4. Be provided with timely confirmations of each securities transaction

Branch Office Procedures

The following policies and procedures are designed to guide the Company's Supervised Persons conducting advisory business outside the main office location, and will serve as a companion to the policies and procedures set forth elsewhere in this Compliance Manual. Supervised Persons are required to operate within the parameters of all applicable policies and procedures of the Company.

Questions

Any questions concerning the policies and procedures of the Company or regarding any regulations or regulatory issues should be directed to the CCO. Under no circumstances should you guess the answer.

Outside Offices and Locations

Supervision of remote office locations and their Supervised Persons is the ultimate responsibility of the CCO, and the on-site designated supervisor.

The following functions may not take place at remote office locations:

1. Neither the remote office nor any of its Supervised Persons shall have the authority to approve advertising or sales literature, or to contractually obligate the Company through third-party vendor or other relationships. All advertising and sales literature disseminated on behalf of the Company and contractual obligations entered into on behalf of the Company are limited to actions taken at the home office.

Remote office Supervised Persons and/or key Associated Persons are required to participate in compliance meetings and remote office audits with the CCO.

Client Account Statements

Confirmations and statements are sent directly to clients by the qualified custodian. Supervised Persons or Associated Persons may not be the addressee or recipient for a client's account (exception: immediate family or trust accounts).

Client Contracts

All clients are required to enter into a written agreement for services prior to the Company providing services on behalf of the client account. Clients will be provided with copies of all signed agreements. The Company prohibits any revisions by Supervised Persons to pre-printed/established language on client contracts. Requests for changes should be referred to the CCO.

Acting as Trustees, Executors, or in Other Fiduciary Capacities

Supervised Persons are prohibited from serving as a trustee, executor, or any other capacity that triggers a custody arrangement for a client's account unless the account is for a relative (defined as immediate family member) of the representative, or resulting from a personal relationship with the grantor or beneficiary and not as a result of employment with the Company. All such arrangements require written approval from the CCO.

Custody of Client Assets

Supervised Persons are prohibited from assuming custody of client assets. If a Supervised Person or employee inadvertently receives client funds or securities, he or she must notify the CCO immediately. The CCO will instruct the individual on appropriate procedures in accordance with the Company's policies regarding the return of client funds or securities.

Private Securities Transactions
No Supervised Person or employee is permitted to participate in any private placement or initial public offering without express written approval from the CCO.

Privacy Policy
Any Supervised Person or employee is prohibited from sharing or disclosing client personal financial information with any non-affiliated third party except as necessary to establish and manage the client's account(s), as required by regulation or law, or as directed in writing by the client. In these situations, personal financial information about a client may only be provided to the broker/dealer or other custodian maintaining the client's account(s), or federal and state regulatory authorities.

Disclosure Documents
Each Supervised Person is required to provide a copy of the Company's Form ADV Part 2, Form CRS, and Privacy Policy Notice to prospective clients prior to, or at the time of execution of a client contract.

Any Supervised Person that is currently, or should become, the subject of any disciplinary proceedings must notify the CCO immediately. The following facts, *among others*, are considered *material*:

Court Proceedings (Criminal and Civil)
- Supervised Person has been permanently or temporarily enjoined from engaging in investment-related activities;
- Supervised Person has been convicted of or has plead guilty or nolo contendere to a felony or misdemeanor involving an investment related business; fraud; making false statements or omissions; wrongful taking of property; bribery; forgery; counterfeiting; or, extortion; and,
- Supervised Person was found to have been involved in a violation of an investment-related statute or regulation.

Regulatory Proceedings
Disclosure should be made for a period of ten (10) years from the time of the event.

1. Supervised Person caused an investment related business to lose its authorization to conduct business or was found to have violated an investment-related statute or regulation and was subject to an order denying, suspending, or revoking its ability to do business or engage in investment-related activities; or,
2. Supervised Person received a fine in excess of $2,500 in a self-regulatory proceeding.

Client Complaints
Upon receipt of a client complaint, the Supervised Person will immediately (within 24 hours) send the original complaint to the CCO if received in writing, or contact the CCO via telephone if the compliant is verbal. The CCO will determine appropriate course of action in addressing any complaint. Documentation of response will be maintained in the Company's compliance files located at the main office.

Holding Client Mail
The Company does not provide mail-holding services to its clients. Supervised Persons are prohibited from receiving mail on behalf of client accounts (exception: immediate family accounts).

Correspondence and Advertising
The Company requires that Supervised Persons limit their use of the internet in efforts to promote the solicitation of advisory services on behalf of the Company, unless prior approval of email or use of an alternative website is obtained from the CCO.

Advertising
Supervised Persons are not to participate in any advertising or public speaking engagements as related to the Company without prior written approval from the CCO. All proposed advertising and presentations must be submitted to the CCO for prior approval.

Outside Business Activity
All outside business activity, securities and non-securities related, must be pre-approved by the CCO prior to the Supervised Person engaging in such activity/employment. The Supervised Person's Form U4 must be updated via WebCRD promptly.

The CCO will determine if such outside business activity presents a potential conflict of interest and will decide whether additional disclosures should be made to clients via an amendment to the Company's Form ADV.

Contingency/Disaster Recovery Plan
The remote office location will maintain a separate Contingency/Disaster Recovery Plan specific to its location, if applicable.

Trade Error Procedures

An overriding principle in dealing with a trading error made by the Company (or any other party to the trade other than the client) is that the client never pays for losses resulting from such errors. A trading error is a deviation from the applicable standard of care in the placement or execution of a trade for an account. In general, the following types of errors would be considered trading errors for the purposes of these Procedures if the error resulted from a breach in the duty of care that the Company owes to the client under the particular circumstances:

1. The purchase or sale of the wrong security, wrong amount of securities, or a trade on the wrong side of the market;
2. Purchase or sale of a security in violation of client investment guidelines or other failure to follow specific client directives; and
3. Purchase of securities not legally authorized for the client's account.

Errors caught and corrected before execution, and ticket re-writes and similar mistakes that incorrectly describe properly executed trades are not considered trade errors.

In addition to a reconciliations or order records with execution reports, errors may be identified in a number of ways including review of a portfolio(s) and identifying;

1. a prohibited security;
2. a short position for an account that does not short sell;
3. a security that was previously sold or not purchased for other accounts with the same investment approach; and
4. the wrong allocation percentage.

All personnel involved with the handling of accounts should be mindful and report the appearance of trade errors.

When the Company makes an error while placing a trade for an account, the Company must bear any costs of correcting the trade. The Company shall follow these guidelines in correcting trading errors:

- When a trade error results in a realized or unrealized loss to a client, the client shall be made whole, either through a billing credit or direct payment to the client;
- Erroneous trades that result in a benefit to the client (for example, failed to sell a security in a timely manner, security price subsequently increases and then the position is sold, resulting in more gain for the client) are generally left in the client's account;
- "Soft dollars" may not be used to pay for correcting trading errors;
- All trade errors must immediately be reported to the CCO for review, investigation, and resolution.

The CCO is responsible for ensuring these guidelines are followed and properly documented in the event of a trade error.

Notification Procedures

Procedures to be followed in the event a potential trading error is identified include the following:

1. Alert the CCO immediately;
2. A determination should be made promptly as to:
    a. whether a trading error has occurred; and
    b. who is the responsible party;
3. Correct the error as soon as possible in the best interest of the client and in a manner consistent with the policy outlined above;
4. In the event of a loss, the Company will reimburse the appropriate party for the full amount of the loss;
5. The CCO shall document the error and include the following
    a. the date of the trade error;
    b. the account(s) involved;
    c. the full name of the security;
    d. a brief description of the error;
    e. the amount of the gain or loss; and
    f. how it was corrected.
6. Payments made to clients because of trade error correction must be recorded in the Company's accounting records;
7. The CCO should be mindful when a pattern of errors exists that should otherwise be addressed; and,
8. The Company will maintain a record of all trade error reports for a period of five (5) years.

Annual Policies & Procedures Acknowledgement

By signing below, I hereby acknowledge receipt of Burgess Chambers & Associates Inc's Compliance Manual. I hereby represent and affirm that I have read the Compliance Manual in its entirety and fully understand its contents. I assume the responsibilities and obligations assigned to me by the relevant sections of the Compliance Manual and I agree to abide by and accept the policies and procedures contained herein.

If I should have any questions concerning the Compliance Manual, regulations, or other information described therein, I understand that I must direct such questions to the Chief Compliance Officer.

I hereby represent that I will report any violations of the policies and procedures contained in the Compliance Manual that come to my attention. I understand that any breach of the policies and procedures contained in the Compliance Manual or any applicable securities laws, rules, and regulations may jeopardize the Company and its personnel and result in disciplinary action against me including possible termination.

I hereby certify that I am not aware of any facts that would constitute violations of the Compliance Manual, which I have not previously disclosed to the Chief Compliance Officer in writing.

Name (Print): _____

Signature: _____

Date: _____

Outside Business Activity Notification Form

Name of Associated Person: _____
(Type or Print)

It is important that you notify the Company if you are, or plan to be, involved in any outside business activity or employment. This notification must be made prior to engaging in the activity. The Company considers this signed document form as receipt during the period you are an employee of The Firm.

Please complete, sign and date this notification form and return it to the Chief Compliance Officer if you are an existing or future employee of the Company. A copy of this form should be retained for your records and changes should be promptly reported to the Chief Compliance Officer.

- Are you currently involved in any business other than working for the Company? ____ NO _____ YES
- Name of business: _____
  Address: _____
  Phone Number: _____
- Nature of business (i.e., registered investment adviser, insurance agency, real estate, etc.)._____
- Are you using a DBA in conjunction with this outside activity? ____ NO _____ YES

  If so, what is the d/b/a? _____
- Explain the organizational status of this business (i.e., a corporation, partnership, sole proprietorship, LLC, etc.). _____
- Date of employment: _____
- List your title/position: _____
- Duties of your position: _____
- Percentage of your time spent in activities involving the business: _____
- Is this business disclosed on your most current Form U4? ____ NO _____ YES
- Do you have a financial interest in the business? ____ NO _____ YES

  If so, what is the total dollar amount of such interest? _____
- How are you compensated by this business? _____
- Estimated annual income from this business? _____

I authorize the Company to investigate my outside business activities and contact any entities or individuals affiliated with such outside business activities. Furthermore, I authorize these entities or individuals to release to the Company any information that it requests about my employment, affiliation and/or activities with this organization.

The foregoing is true and correct.

_____ _____ _____

Printed Associated Person Name Associated Person Signature Date

Received and Reviewed:

Notes/comments/verifications: _____

_____

_____

_____

_____ _____

Chief Compliance Officer Date