Investment Advisor Compliance Manual
and
Written Supervised Procedures

Omnes Wealth Management LLC

Effective Date: January xx, 2026

CONFIDENTIAL – NOT TO BE DISTRIBUTED OUTSIDE THE FIRM

This Investment Advisor Compliance Manual and Written Supervised Procedures is the property of Omnes Wealth Management LLC and its contents are confidential and may not be distributed without the prior approval of the Chief Compliance Officer.

Using this Manual

Each Supervised Person of Omnes Wealth Management LLC must read and understand this Investment Advisor Compliance Manual and Written Supervised Procedures and comply with all of the policies and procedures herein.

Table of Contents

1. Overview **4**
- **A. The Compliance Program** 4
- **B. Role of the Chief Compliance Officer** 4
- **C. Fiduciary Duty** 5
- **D. Regulatory Inquiries** 5

2. Supervision and Compliance Oversight **6**
- **A. Supervisory Functions** 6
- **B. Hiring Supervised Persons** 6
- **C. Code of Ethics** 7
- **D. Insider Trading and Material Non-Public Information** 7
- **E. Conflicts of Interest** 9
- **F. Consequences of Non-Compliance** 9
- **G. Whistleblower Policy** 9
- **H. Business Continuity Plan** 10
- **I. Operational Errors** 11
- **J. Books and Records** 11
- **K. Financial Statements** 11

3. Client Relationship Management **12**
- **A. Client Prospecting** 12
- **B. Client Onboarding** 12
- **C. Ongoing Client Management** 13
- **D. Treatment of Retirement Account Rollovers** 14
- **E. Treatment of Vulnerable Clients** 16
- **F. Treatment of Client Termination** 17
- **G. Treatment of ERISA Clients** 17
- **H. Client Fees** 17
- **I. Custody** 18
- **J. Client Money Movement** 20
- **K. Client Complaints** 20
- **L. Anti-Money Laundering / Customer Identification Program** 21

4. Portfolio Management and Trading **21**
- **A. Investment Research and Monitoring** 21
- **B. Portfolio Suitability and Monitoring** 22
- **C. Trading Practices and Conflicts** 22
- **D. Trading Errors** 25
- **E. Best Execution** 25
- **F. Proxy Voting** 26
- **G. Valuation** 26

5. Client Communications: Advertising & Sales Marketing **26**
- **A. Client Communications** 26
- **B. Advertising Rule Content Standards** 26
- **C. Interactive Media Communications** 28
- **D. Review and Approval Process** 28

6. Regulatory Filings **29**
- **A. Form ADV Filings and Amendments** 29
- **B. IAR Registrations, Disclosures, and Amendments** 30
- **C. Exchange Act Filings** 30

7. Privacy, Information Security and Technology Use **31**
- **A. Cybersecurity** 31
- **B. Regulation S-P: Safeguard and Disposal Rule** 31

C. Regulation S-ID: Identity Theft Red Flag Program 32
D. Email Use 36
E. Mobile Devices 36
8. Vendor Management **37**
A. Background 37
B. Due Diligence 37
C. Additional Considerations and Limitations 38

1. Overview

A. The Compliance Program

Omnes Wealth Management LLC (herein “Omnes Wealth” or the “Advisor”) is a registered investment advisor with the State of New York and is subject to legal and regulatory requirements as set forth by the State of New York securities law and applicable federal regulations (collectively “Securities Laws”).

The Advisor must, among other things, adopt and implement written policies and procedures reasonably designed to prevent violations of Securities Laws. This Investment Advisor Compliance Manual and Written Supervised Procedures document (the “Compliance Manual”) sets forth the Advisor’s policies and procedures for complying with Securities Laws, and together with the related policies and procedures in the Privacy Policy, Code of Ethics, Business Continuity Plan, and Cybersecurity Policy form the Advisor’s compliance Program (“Compliance Program”).

This Compliance Program is designed to discuss the Advisor’s fiduciary duty to its clients (“Clients”), the role of the Chief Compliance Officer (“CCO”), any owners, employees, independent contractors and other insiders of other Advisor (“Supervised Persons”), and Supervised Persons responsible for advisory activities, including giving advice or soliciting Clients (“Advisory Persons”), the use and enforcement of the Compliance Program, the Advisor’s process for addressing complaints regarding its Compliance Program, Client management policies and business activities, portfolio management and trading practices and adherence to Client communication standards, and regulatory filings.

Amendments
The CCO will amend, modify, suspend, or terminate any policy or procedure contained in the Compliance Program documents, as well as adding any policies as necessary. The Advisor will endeavor to promptly inform Supervised Persons of any relevant changes and provide each Supervised Person with the respective updated Compliance Program document.

AdvisorCloud360®
Throughout the Compliance Program, there will be action items that the CCO and/or Supervised Persons are required to address along with various resource tools. The action items and resource tools are captured within AdvisorCloud360®.

Receipt and Acknowledgement
The Compliance Program documents are provided to each Supervised Person upon hire and annually thereafter. They will also be distributed on an ad hoc basis if there are any material amendments. Electronic copies are posted and stored internally in a location that is accessible by all Supervised Persons. All Supervised Persons must review each Compliance Program document and sign an acknowledgment that they have read, understood, and will abide by the Compliance Program.

PLEASE NOTE: See AdvisorCloud360® for Key Definitions of terms utilized throughout the Compliance Program and AdvisorCloud360® for applicable Rule References.

PLEASE NOTE: The Advisor is a single-person firm. The Advisor shall follow the intent of the Compliance Program, but certain policies result in self-checking.

B. Role of the Chief Compliance Officer

The CCO of the Advisor is Christopher A. Bracco. The CCO administers the Advisor’s overall Compliance Program.

Accuracy of the Compliance Program
The CCO is responsible for ensuring that the Compliance Program is, at all times, accurate in its reflections of the Advisor’s business practices and any applicable Securities Laws and for distributing the most current Compliance Program to Supervised Persons.

Training Supervised Persons

The CCO is responsible for ensuring that Supervised Persons receive initial training and undertake any necessary continuing education to understand and meet applicable requirements of the Compliance Program. The CCO will arrange to meet (in person or by phone) with each new Supervised Person. At that time, the CCO will discuss with the new Supervised Person the Advisor's compliance requirements and specifically highlight those policies and procedures that relate to the Supervised Person's area of responsibility. At least annually, the CCO will also arrange a meeting with all Supervised Persons to discuss any additional or modified policies and procedures.

Forensic Testing and Risk Assessments

The CCO is also responsible for performing an annual review of the Compliance Program to determine the adequacy and the effectiveness of the program. Each of the ***CCO Testing*** items will indicate the testing action item required of the CCO. The CCO or Delegate documents all ***CCO Testing*** findings as it relates to the various functions of the Compliance Program***. The CCO Testing*** serves as the source of the CCO's annual review of the Compliance Program.

Delegation

The CCO may delegate a portion of their responsibilities to appropriate designees ("Delegate[s]") as long as the CCO remains primarily responsible for Compliance Program oversight and administration. Additionally, in the event that the CCO will be absent from the office, he or she will notify Supervised Persons of an appropriate Delegate to fulfill the CCO's responsibilities.

C. Fiduciary Duty

As a fiduciary, it is the Advisor's responsibility to act in the best interest of its Clients at all times. The Advisor will not place its own interests ahead of its Clients' interests. The Advisor's fiduciary duty represents the core of the Advisor's Compliance Program.

Specific obligations associated with the Advisor include:

- Having a reasonable, independent basis for investment advice.
- Obtaining best execution when implementing any Client's transactions where an Advisory Person has the ability to direct brokerage transactions for the Client.
- Ensuring that investment advice is suited to each individual Client's objectives, needs, and personal circumstances.
- Maintaining the confidentiality of Client information.
- Exercising reasonable care to avoid misleading Clients.
- Making full and fair disclosure to the Client of all material facts and when a conflict of interest or potential conflict of interest exists.
- Placing Client interests first and always acting in good faith.

In addition, it is unlawful for the Advisor:

- To employ any device, scheme, or artifice to defraud a Client or prospective client.
- To engage in any transaction, practice, or course of business which defrauds or deceives a Client or prospective client.
- To knowingly sell any security to, or purchase any security, from a Client when acting as a principal for his or her own account, or knowingly execute a purchase or sale of a security for a Client's account when also acting as a broker for the person on the other side of the transaction, without disclosing to the Client in writing before the completion of the transaction the capacity in which the Advisor is acting and obtaining the Client's consent to the transaction.
- To engage in fraudulent, deceptive, or manipulative practices.

D. Regulatory Inquiries

Because the Advisor operates in a highly regulated industry, the Advisor may receive inquiries and exam requests from regulators. If a Supervised Person is contacted by a regulator, whether by telephone, letter, or office visit, he or she may not, under any circumstances, engage in discussions with the contacting party, or take any other action in response to such contact, other than (i) advising the contacting party that all Supervised Persons are under instructions to refer all such inquiries to the CCO and (ii) promptly notifying the CCO.

If interviewed as part of an inquiry or exam, all Supervised Persons should treat the regulators with courtesy and respond fully, promptly, and honestly to all requests and questions. If a Supervised Person has a question as to the propriety of a request or question, the Supervised Person may respond by politely stating that the Supervised Person will consult with the CCO before providing the information.

Regulators will typically provide feedback on an exam in the form of a deficiency letter. Deficiency letters point out minor violations or perceived weaknesses in an advisor's compliance controls. Regulators typically request a response to a deficiency letter, including a description of remedial actions taken by the Advisor, within thirty (30) days from date of the letter. The CCO is responsible for coordinating the Advisor's response. In the unlikely event that a compliance inquiry or exam leads to an enforcement referral, the CCO will contact outside counsel immediately.

2. Supervision and Compliance Oversight

A. Supervisory Functions

The Advisor is required to reasonably supervise Supervised Persons with a view to preventing violations of Securities Laws. In meeting this requirement, the Advisor and its Supervised Persons will not be deemed to have failed reasonably to supervise any person, provided that:

- The Advisor has established procedures, and a system for applying the procedures, which would reasonably be expected to prevent and detect, insofar as practicable, any such violation by a person subject to the Advisor's supervision; and
- The Advisor and any Supervised Person acting in a supervisory capacity has reasonably discharged the duties and obligations incumbent upon the Advisor or supervisor and has no reasonable cause to believe that there is no non-compliance with the supervisory procedures and system.

The Compliance Program is intended to establish a system for preventing and detecting, insofar as practicable, violations of Securities Laws by Supervised Persons. The Advisor expects each Supervised Person acting in a supervisory capacity to oversee any other Supervised Person under their supervision in a manner consistent with the policies and procedures contained in the Compliance Program.

B. Hiring Supervised Persons

Initial Due Diligence

Prior to any new Supervised Person joining the Advisor, the CCO will conduct reasonable due diligence to review the background of the individual and determine if they have been the subject of any legal, financial and disciplinary history and whether the individual is a good fit for the Advisor.

Due diligence may include reviews of the following:

- background checks (e.g., confirming employment histories, disciplinary records, financial background, and credit information);
- conducting internet and social media searches; including a review of BrokerCheck (https://brokercheck.finra.org) or the Investment Adviser Public Disclosure website ("IAPD" – https://adviserinfo.sec.gov);
- requesting copies of their Form U5 from their prior employer, if applicable;
- utilizing third parties to research potential new hires;
- contacting personal references, and/or
- verifying educational claims.

If the individual has been subject to any legal, regulatory or financial events, the CCO will ensure that the individual remains a good fit for the Advisor and ensure that any events are adequately disclosed. Should the Advisor move forward with the new hire, the CCO will make a determination as to whether or not that individual requires heightened supervision.

Ongoing Due Diligence

For existing Supervised Persons the CCO considers a number of factors in determining whether an existing Supervised Persons needs to be placed on heightened supervision. These factors may include but are not limited to:

- new disclosures;
- patterns of violating firm policies and procedures;
- ongoing background reviews; and/or
- annual background attestations.

Heightened Supervision

Whether or not to impose heightened supervision is at the sole discretion of the CCO. If the CCO determines that heightened supervision is warranted the CCO will create a plan ("Heightened Supervision Plan") based on the nature of the event[s] CCO's should pay particular attention to patterns or the significance of a single event when deciding whether or not to place an individual on heightened supervision.

When developing the specific Heightened Supervision Plan the CCO will document the following items:

- Background regarding why the individual is being placed on heightened supervision
- Duration of heightened supervision e.g. 1 year, 2 years
- The specific supervisory procedures that will take place during the defined heightened supervision period e.g. increased review of email, increased review of trading activity, financial record review
- That the individual being placed on heightened supervision attests to the plan by signing off on the conditions.

C. Code of Ethics

The Advisor has adopted a Code of Ethics (the "Code") as a separate policy and procedure document. The Code establishes the standard of business conduct that all Supervised Persons must follow and also addresses potential conflicts of interest and disclosure requirements surrounding:

- Insider trading and material nonpublic information
- Confidentiality of nonpublic information
- Outside business activities of Supervised Persons
- Gifts and entertainment given or received by the Advisor and/or its Supervised Persons
- Political contributions to politically connected individuals and/or government entities
- Personal securities trading of Supervised Persons with Access to Nonpublic Information regarding the purchase or sale of securities for Clients ("Access Persons")
- Receipt and acknowledgment of adherence to the Code

CCO Testing: The CCO or Delegate conducts a quarterly review of personal securities trading and documents the findings in the Advisor's books and records. The CCO or Delegate is also responsible for reviewing outside business activities, political contributions, and gifts and entertainments.

PLEASE NOTE: See AdvisorCloud360® for the Outside Business Activity, Gifts and Entertainment, and Political Contributions Logs.

D. Insider Trading and Material Non-Public Information

The Insider Trading and Securities Fraud Enforcement Act of 1988 and securities laws requires advisors to establish, maintain and enforce written policies and procedures reasonably designed to prevent the misuse of Material Non-Public Information ("MNPI") by advisors and its Supervised Persons. Frequent litigation in the area of insider trading continues to shape the definitions of what is inside information and what constitutes appropriate handling of such information.

PLEASE NOTE: As referenced within the Code, it is the Advisor's policy that all Supervised Persons are prohibited from acting upon, misusing or disclosing any MNPI, also known as inside information. Any instances of, or questions regarding possible MNPI inside information must be brought to the CCO or Delegate's attention immediately brought to the attention of the CCO or Delegate. Any violations of the Advisor's policy may result in disciplinary action and/or termination.

General Prohibition

In order to prevent even inadvertent violations of the ban on insider trading, all of the Advisor's Supervised Persons must adhere to the following guidelines;

- all information about the Advisor's Clients, including but not limited to the value of accounts; securities bought, sold or held; current or proposed business plans; acquisition targets; confidential financial reports or projections; borrowings, etc. must be held in strictest confidence;
- when obtaining material information about an issuer from insiders, determine whether the information learned has already been disseminated through "public" channels;
- in discussions with any third parties, it also may be appropriate to determine whether the information obtained from the third-party has been publicly disseminated;
- If any Supervised Person determines that they have learned MNPI or market information, notify the CCO or Delegate of this fact immediately and refrain from disclosing this information to anyone else (in or outside of the Advisor), unless specifically advised to the contrary. In this case, neither the Advisor nor its Supervised Persons may transact in the securities of the subject issuer, either for themselves or for any Client, until such information has been publicly disseminated; and
- On an annual basis and otherwise as requested by the CCO or Delegate, disclose complete information about all securities transactions in which you or members of your immediate family engage, and must otherwise comply with the Advisor's Code and disclose any related person who is an officer or director of a publicly traded company.

Compliance Administration

In order to help prevent insider trading from occurring, the CCO or Delegate shall:

- Design an appropriate educational program and provide educational materials to familiarize Supervised Persons with the Advisor's policy, both of which are addressed through ongoing training of Supervised Persons.
- Answer questions and inquiries regarding the Advisor's policy, provide guidance to Supervised Persons on any possible trading situation or question, and resolve issues as to whether information received by a Supervised Person constitutes MNPI.
- Review the Advisor's policy and procedures on a regular basis and update it as necessary to reflect regulatory and industry changes.
- Review and document on a quarterly basis all Access Persons' reports of personal securities transactions for compliance with the Advisor's policies, regulatory requirements and the Advisor's fiduciary duty to its clients, among other things.

Instances of the Possible Possession of Inside Information

If a Supervised Person suspects that they, or the Advisor, has been given or come across MNPI, they must immediately report such circumstances to the CCO or Delegate, who will contact legal counsel, if applicable, and refrain from disclosing the information to anyone else, unless specifically advised to the contrary. If they are not sure whether the information meets the definition of MNPI, they are responsible for reporting the information to the CCO or Delegate, who will make such determination.

Upon determination that a Supervised Person has possession of MNPI, the CCO or Delegate shall implement measures to prevent dissemination of such information and monitor Client and Access Person trades related to securities regarding the information for unusual activity. If any activity is detected that may indicate improper use of MNPI, the CCO or Delegate shall conduct an additional review, take further action as deemed appropriate under the circumstances and document the instance within the Advisor's books and records.

Possession of Inside Information

A Supervised Person of the Advisor will contact the CCO or Delegate if they become aware of an actual or potential insider trading violation or violation of the policies and procedures.

Insider Trading Examples

While securities laws concerning insider trading is evolving, it is generally understood that securities laws prohibit: (a) trading by an insider on the basis of MNPI; (b) trading by a non-insider also called a "temporary insider" on the basis of MNPI, where the information was either disclosed to the non-insider in violation of an insider's duty to keep the information confidential or was misappropriated; and (c) communicating MNPI to others.

It is Impossible for the Advisor to catalog every example of when it may come into possession of MNPI. The following examples are not all-inclusive:

- A pending or proposed merger, acquisition or tender offer involving a publicly held corporation;
- A change in management involving a publicly held corporation;
- Impending bankruptcy or the existence of severe liquidity problems involving a publicly held corporation; or
- A contemplated public offering involving a privately held corporation, prior to the filing of the registration statement (preliminary prospectus).

Investment Information Relating to Clients is Inside Information

In the course of employment, Supervised Persons may learn about the current or pending investment activities of the Advisor's Clients (e.g., actual or pending purchases or sales of assets). Using or sharing this information other than in connection with the investment of the Advisor's Client accounts is considered acting on inside information and is therefore prohibited. In addition, personal securities transactions of Access Persons must not be timed to precede orders placed for any Client accounts, which could be considered as "front-running" or insider trading.

E. Conflicts of Interest

In order for the Advisor to ensure that Clients' interests come before those of the Advisor and its Supervised Persons, any actual or perceived conflicts of interest must be identified, evaluated, managed, and disclosed. The Advisor is not permitted to mislead or engage in deceptive conduct and must, in all instances, act in the best interests of its Clients. Managing the Advisor's conflicts of interest minimizes the potential adverse impact of conflicts of interest on Clients, as well as promoting Client protection and maintaining the Advisor's reputation and integrity. Disclosure of material conflicts is necessary so that any Client can make an informed decision as to whether to enter into or continue an advisory relationship or whether to take some action to protect themselves against the particular conflict of interest involved.

PLEASE NOTE: The Advisor will maintain a log and along with supporting documentation of all conflicts of interest that exist. See AdvisorCloud360® for the Conflicts of Interest Log.

F. Consequences of Non-Compliance

If a Supervised Person fails to comply with the requirements of the Compliance Program and any Securities Laws applicable to the Advisor's business, he or she will be subject to disciplinary action by the Advisor, which may range from a letter of reprimand to termination of employment. Any non-compliance or violations of law may also result in severe civil and criminal penalties.

The Advisor reserves the right to take disciplinary action, including termination of employment, against any Supervised Person if they engage in conduct deemed to be immoral, unethical, or illegal, whether or not such conduct constitutes a violation of the Compliance Program or relates to the Advisor's business. The Advisor may take such action if the Advisor believes that a Supervised Person's conduct poses any risk to the reputation or business of the Advisor.

Finally, a Supervised Person must report to the CCO any known or suspected violations of the policies and procedures contained in the Compliance Program or other activities of any Supervised Person that could be construed as a violation of Securities Laws, including the policies described in the Advisor's Compliance Program. If a Supervised Person is unsure whether a violation has occurred, the incident should be discussed with the CCO. Failure to report a violation to the CCO could result in disciplinary action against any non-reporting Supervised Person, which may include termination of employment.

PLEASE NOTE: The Advisor will maintain a log along with relevant supporting documentation of any violations to the Compliance Program. See AdvisorCloud360® for the Violations Log.

G. Whistleblower Policy

The Advisor has adopted a "Whistleblower Policy" to establish procedures for the receipt, review, and retention of complaints relating to violations of Securities Laws or any other provision of law, rule, order, standard, or

prohibition prescribed by a securities authority. While the Advisor does not encourage frivolous complaints, the Advisor does expect its Supervised Persons to report any suspected violations of Securities Laws, including the policies described in the Advisor's Compliance Program.

Reporting Persons Protected
Complaints reported in good faith will not be subject to any retaliation.

Scope of Complaints
Supervised Persons and external vendors, consultants, etc. are all encouraged to report all suspected wrongdoings.

Confidentiality of Complaints
All complaints submitted by Supervised Persons that are reported in good faith will be kept confidential and privileged to the fullest extent permitted by law.

Submitting Complaints
Complaints must be submitted in writing, by submitting an anonymous concern form, addressed to the CCO. Persons submitting complaints may request to discuss the complaint with the CCO.

PLEASE NOTE: See AdvisorCloud360® for the Anonymous Concern Form

OR

PLEASE NOTE: Click here for the Anonymous Concern Form.

In addition to directly reaching out to the CCO, Supervised Persons and external vendors, consultants, etc. may also call the SEC's Office of the Whistleblower at (202) 551-4790 to log a complaint. External vendors, consultants, etc. are not permitted to submit complaints anonymously.

Investigation of Complaints
The CCO will confirm the complaint pertains to a violation by investigating the complaint promptly and documenting the results.

Retention of Complaints
The CCO will keep records of all submitted complaints and the results of the corresponding investigations.

Unsubstantiated Allegations
If the investigation of the complaint submitted in good faith finds no violation, the reporting individual will not be subject to retaliation.

Reporting and Annual Review
The CCO will include all complaints and any remedial actions taken in the Annual CCO Report.

H. Business Continuity Plan

The Business Continuity Plan (the "BCP") is a separate policy and procedure document of the Advisor's Compliance Program. The Advisor recognizes the importance of ensuring continuity of operations in the event of an interruption of services that may result from terrorism, natural disaster, or otherwise. As a result, the Advisor has adopted the BCP to enable the continuation of operations and access to necessary information within a reasonable period of time. The Advisor has addressed the following important concepts in well-defined terms within the BCP:

- Business interruption scenarios
- Critical business functions
- Alternate work sites, data backup, and restoration
- Key person risk and succession planning
- Receipt and acknowledgment of adherence to the BCP

CCO Testing: The CCO or Delegate conducts an at least annual test of the Advisor's business continuity plan and documents the findings in the Advisor's books and records.

I. Operational Errors

It is the Advisor's responsibility to ensure appropriate and accurate management of Client relationships. An "operational error" is generally any error resulting in a relationship risk or loss resulting from inadequate or failed internal processes, actions of Supervised Persons and/or system issues.

This includes all aspects of the Advisor's operations, including, but not limited to:

- an error with Client billing and/or fee calculations;
- inaccurate security and/or portfolio valuations;
- failure to properly execute an agreement;
- inaccurate use of standard agreement templates;
- improper classification of Client types; and
- transposed language in Client communications.

PLEASE NOTE: The Advisor will determine the cause of each operational error, the impact (if any) on the Client, steps to rectify the error, and a strategy to ensure that the error does not happen again. The Advisor maintains a log of all operational errors along with any relevant and supporting documentation such as communications with the Client and steps taken to remediate the issue. See AdvisorCloud360® for the Operational Error Log.

J. Books and Records

The Advisor is required to make and keep certain books and records relating to its business-to-document aspects of compliance and supervision of the Advisor's Compliance Program. This includes, but is not limited to, financial and accounting records, Client account information, advertisements, and etc. The Advisor enforces the following requirements with regard to recordkeeping and communication:

- Financial statements and all books and records on which they are based must reflect all applicable transactions accurately and on a timely basis;
- All disbursements of funds and all receipts must be properly and promptly recorded;
- No false or artificial statements or entries may be made for any purpose in the Advisor's books and records or in any internal or external correspondence, memoranda, or communication of any type, including telephone, wire, or electronic communications;
- Retention of information and data must be timely and free from unauthorized alteration or use in accordance with legal requirements and operational policies and procedures; and
- Falsification of business documentation, whether it results in personal gain or not, is never permissible.

The Advisor's required books and records generally must be maintained for a period of five (5) years from the end of the fiscal year in which the last entry was made on the record. They must be maintained for the first two (2) years at an appropriate office of the Advisor. For the remaining period, they may be maintained in an easily accessible place, which can include an off-site location or a third-party storage provider. Notwithstanding the time frames established by Securities Laws, the Advisor may be required to maintain records for a longer period of time if there is a "pending legal matter."

Regulators have the authority to examine all books and records held by the Advisor. Thus, during a regulatory exam, the Advisor is expected to produce any requested records that are maintained - either in hard copy or electronic format.

CCO Testing: The CCO or Delegate conducts an at least annual review of the Advisor's document retention capability and documents the findings in the Advisor's books and records.

PLEASE NOTE: The CCO will have overall responsibility for ensuring that all required books and records are identified and properly maintained. Any question as to whether a particular document must be maintained by the Advisor should be directed to the CCO. See AdvisorCloud360® for the Books and Records Matrix.

K. Financial Statements

The Advisor shall maintain true and accurate financial records at all times. Financial records shall be maintained pursuant to Rule 204-2 (the "Books and Records Rule") as noted above. Financial records shall be reconciled throughout the year (generally quarterly) and maintained in appropriate form or technology to enable the CCO to monitor the financial health of the Advisor.

The Advisor shall periodically produce a balance sheet, income statement and general ledger, pursuant to Generally Accepted Accounting Principles ("GAAP").

CCO Testing: The CCO or Delegate shall review financial records and statements periodically to ensure the continued health and viability of the Advisor. It is the CCO's responsibility to ensure any financial situation that may impair the Advisor's ability to perform its duties and meet its obligations to Clients be immediately addressed and corrective action taken. If the Advisor finds itself in a precarious financial position, whereby it may not be able to meet such obligations, the Advisor must amend its Form ADV 2A, Item 18 disclosures accordingly.

3. Client Relationship Management

A. Client Prospecting

There are many ways for the Advisor to obtain new Clients, either through general marketing (see Client Communication Policy), word of mouth, use of solicitors, and/or other referral arrangements.

All Supervised Persons actively soliciting prospective clients of the Advisor are considered to be Advisory Persons of the firm and as such are required to register as Investment Advisor Representative ("IARs"). When an Advisory Person engages with a prospective client, the Advisory Person will gather sufficient information about the prospective client to determine whether the Advisor's services are suitable for the prospective client. The Advisory Person may provide the Disclosure Brochure to the prospective client. In such instances, the Advisory Person will maintain a list of prospective clients that received the Disclosure Brochure to determine whether a new Disclosure Brochure is required to be delivered at the time of engagement.

<u>Use of Solicitors</u>
An advisor may also utilize solicitors as a means of garnering clients. It is unlawful for an advisor to pay a cash fee to a solicitor for solicitation activities unless:

- The advisor is registered under Securities Laws; and
- The solicitor meets certain requirements and is not subject to a statutory disqualification

PLEASE NOTE: As a matter of policy, the Advisor does not engage paid solicitors for Client referrals. While the Advisor does not engage solicitors, payment of referral fees by the Advisor to persons who solicit advisory Clients is permitted only in accordance with the "Cash Solicitation Rule". If the Advisor does intend to engage a solicitor, appropriate disclosures will be made in advance of the inception of the relationship.

B. Client Onboarding

Building relationships with Clients is an important part of the Client onboarding process. Setting expectations for services and communications help drive Client satisfaction and lays the foundation for a successful relationship. As soon as the Advisor is notified of a new Client, the Advisor will review the opportunity and plan for the take on of the business. All new Client relationships follow established procedures to ensure that required documents are provided to the Client and adequate Client information and documents are received, reviewed for accuracy and completeness, and saved before funds are transferred. The Advisor will take the following action steps with each new Client:

<u>Initial Form ADV Delivery Requirements</u>
Prior to, or at the time of entering into an agreement, the Advisor delivers to the Client the most current version of Form ADV Part 2A ("Disclosure Brochure"), Form ADV Part 2B ("Brochure Supplement[s]"). The Disclosure Brochure, and Brochure Supplement[s] are collectively referred to as the "Disclosure Documents".

The Advisor delivers these Disclosure Documents to Clients in an acceptable format that is easily accessible and readable (i.e., searchable PDF format). Electronic versions of the Disclosure Brochure and Brochure Supplement[s] can be delivered by email. For Clients that do not have an established email address for Advisor communications, a paper version must be mailed to the Client's mailing address. Delivery must be made without charge to the Client. Upon request, a hard copy must be sent by regular, first-class mail or overnight carrier, or hand delivered as requested.

PLEASE NOTE: If any Disclosure Document is delivered electronically, it will be presented prominently in the electronic medium, for example, as a direct link or in the body of an email or message, and will be easily accessible for retail investors

Prior to, or at the time of entering into an Advisory Agreement (as defined below), the Advisor is required to deliver to the Client the most current version of the Disclosure Documents (Form ADV 2A – Disclosure Brochure, and each applicable Form ADV Part 2B – Brochure Supplement.

Privacy Policy Delivery

Prior to, or at the time of entering into an agreement, the Advisor delivers to the Client the Privacy Policy. The Advisor understands that Clients have entrusted the Advisor with their private information, and the Advisor will do everything to maintain that trust. The Advisor protects the security and confidentiality of the personal Client information. The Advisor implements controls to ensure that such information is used for proper business purposes in connection with the management and servicing of the Client relationship.

Advisory Agreement

The Advisor requires a written advisory agreement for all Clients (the "Advisory Agreement"). Advisory services will not be offered or provided unless an Advisory Agreement is executed by both the Client and the Advisor and an executed copy delivered to the Client. Advisory Agreements provide the Advisor and the Client with a legal document stating the expectations of both parties for the engagement. Critical areas of the document include, but are not limited to, a definition of services to be provided to the Client, an explanation and listing of advisory fees to be charged to the Client, additional parties that may be involved in the relationship (i.e., custodian or broker/dealer), and an acknowledgment of the delivery and receipt of the Advisor's Disclosure Brochure, Brochure Supplement(s), and Privacy Policy.

Obtaining Client Suitability

The Advisor has a fiduciary duty to provide suitable investment advice to each Client. As a general policy, the Advisor is responsible for making reasonable inquiries into and assessments of each Client's investment objectives, financial situation, investment experience, tolerance for risk, and any other material information. Based on the information, the Advisor will determine whether the proposed investment advice rendered to the Client is suitable.

The Advisor must internally document the investment objectives and goals of the Client. The Advisor may request information/documents from the Client to assist in determining suitability. The Advisor will prepare and place in the Client's file a memorandum identifying any information requested, but not provided by the Client, as well as the person from whom such information was requested and the reason why the Client did not provide the information. The Advisor must obtain in writing, any restrictions as it relates to the management of Client investments. The Advisor will instruct its Clients to contact the Advisor any time their financial situation or personal/company information changes.

Internal Documentation

It is the Advisor's policy to document and maintain all items related to the Client onboarding process within the Client's file. The Client will be set-up in the Advisor's system[s] for portfolio management, accounting, suitability monitoring, and billing purposes.

Account Opening and Transfer of Assets

The Advisor will receive all of the required account opening documents and review them for accuracy and completeness and will then add them to the Client's file. The Advisor will forward account paperwork to the broker-dealer/custodian ("Custodian"). If there are any issues with incomplete information or there are any concerns, the Client will be contacted for clarification. Once the account is open the Client will be contacted to initiate the asset transfer.

C. Ongoing Client Management

The Advisor has a fiduciary duty to provide ongoing Client management through the following:

Maintaining Suitability

The Advisor contacts Clients on at least an annual basis in order to validate the stated investments, goals, and objectives of the Client to support the review and analysis of Client investment suitability. A record of such Client contact is maintained in the Client's files and/or updated in electronic records, specifying the mode of contact. The Advisor will update account information when the Advisor becomes aware of any new information. Any requested changes to investment guidelines and restrictions must be communicated and confirmed with the Advisor in writing and may require an amendment or side letter to the Advisory Agreement.

Ad-Hoc Form ADV Delivery Requirements

Form ADV Part 2A – Disclosure Brochure: Should any material change occur in the Advisor's business practice throughout the year including, but not limited to, investment process, fees charged, ownership structure, business address, contact information, disciplinary disclosure, or other notable aspects of the Advisor's business, the Advisor will deliver the updated Disclosure Brochure or communicate the material changes to Clients within thirty (30) days of the amended filing identifying the material change.

Form ADV Part 2B – Brochure Supplement[s]: Should any material change occur in an investment advisor representatives background information throughout the year including, but not limited to, outside business activities, disciplinary or disclosure items, or other notable background information, the Advisor will deliver the updated Brochure Supplement or communicate the material change to Clients within thirty (30) days of the material change.

Annual Form ADV Delivery Requirements

Annually, within 120 days following the Advisor's fiscal year-end, the Advisor "delivers" at no cost to the Client, an update of the Disclosure Brochure that either includes:

- The updated Disclosure Brochure that contains a summary of material changes since the last delivery to Clients; or
- A summary of material changes to the updated Disclosure Brochure that includes an offer to provide a copy of the updated Disclosure Brochure and information on how a Client may obtain the Disclosure Brochure.

Annual Privacy Policy Delivery

The Privacy Policy is required to be delivered annually to Clients of the Advisor and is typically provided at the same time as the Disclosure Brochure and Brochure Supplement delivery.

Internal Documentation

It is the Advisor's policy to document and maintain all items pertaining to the ongoing Client Management within the Client's file.

CCO Testing: The CCO or Delegate periodically reviews Client files, including, but not limited to Agreements to ensure accuracy and proper execution, suitability and account information. The CCO or Delegate and documents the findings in the Advisor's books and records.

D. Treatment of Retirement Account Rollovers

The Department of Labor ("DOL") adopted Prohibited Transaction Exemption 2020-02 ("PTE 2020-02") which expands the definition of advice covered under ERISA law to include recommendations about retirement plan rollovers and Individual Retirement Accounts ("IRAs"). A recommendation that a Client roll over their retirement plan assets into an account to be managed by the Advisor creates a conflict of interest, as the Advisor will earn more in advisory fees as a result of the rollover.

The DOL has established a Five-Part Test in order to assist advisors in determining whether a recommendation to roll over retirement plan assets into an IRA falls under ERISA. The regulation states that a person provides "investment advice" if he or she: (1) renders advice to a plan or participant as to the value of securities or other

property, or makes recommendations as to the advisability of investing in, purchasing, or selling securities or other property; (2) on a regular basis; (3) pursuant to a mutual agreement or understanding; (4) that such advice will be a primary basis for investment decisions; and that (5) the advice will be individualized to the plan or participant.

Under the DOL there are requirements to adhere to the following:

1. acknowledgment from the advisor of their fiduciary status under Title I of ERISA and the Internal Revenue Code;
2. due diligence and written documentation of the specific reasons that any recommendation to roll over assets (whether from an ERISA plan to an IRA, from one IRA to another IRA, or from one type of account to another (e.g. commission-based account to fee-based account) is in the best interest of the client.
3. written disclosure to clients that include (i) the scope of the relationship, (ii) all material conflicts of interest, and (iii) the reasons the rollover recommendation is in their best interest;
4. compliance with the Impartial Conduct Standards which includes (i) provide prudent investment advice, (ii) charge only reasonable compensation, and (iii) avoid misleading statements; and
5. an annual compliance review with the results in a written report to a Senior Executive Officer of the advisor.

Advisor Recommended Rollovers
As a result of the aforementioned requirements, in the event of a rollover recommendation, the Advisor will conduct due diligence on the Client's option to rollover assets versus retaining them in an ERISA sponsored plan, to ensure it meets the Clients best interest. Factors to be considered may include, but are not limited to:

- Investment options - Investment options may differ between an ERISA sponsored plan and those available within an IRA.
- Tax considerations - Account owners may be subject to income tax, early withdrawal penalties, or net unrealized appreciation.
- Fees and expenses – Fees and expenses may vary depending on the services offered and availability of underlying funds.
- Service offerings - ERISA plans may provide an array of services to the account owner, such as participant loans, planning tools, personalized advice, tax planning or estate planning.
- Legal considerations - ERISA plans typically have unlimited protection from creditors under federal law. However, IRA assets are protected in bankruptcy proceedings only.

Policy:
In the event investment advice is covered under ERISA, the Advisor abides by the aforementioned DOL requirements.

Procedures:
1. In order to abide by the aforementioned DOL requirements, the Advisor will conduct due diligence on the Client's options, to ensure its recommendation is in the Clients' best interest. Factors considered include, but are not limited to:
    a. Investment options
    b. Tax considerations
    c. Fees and expenses
    d. Service offerings
    e. Legal considerations
    f. Simplification and consolidation

2. The Advisor will provide Clients with a written acknowledgment of the Advisor's ERISA fiduciary status, a written disclosure of the material conflicts of interest, and the basis for why the investment advice is believed to be in the Client's interest for all investment advice covered under ERISA.

3. *Client Directed Rollovers* - In any instance where a Client directs the Advisor to initiate and execute a rollover of retirement assets, the Advisor will utilize a separate and distinct acknowledgment form where

the Client attests to, via signature, the fact that the Advisor did not solicit the rollover and that the rollover is being executed at the sole discretion of the Client.

4. All copies of (i) acknowledgment of the Advisor's ERISA fiduciary status, (ii) delivery of disclosures, (iii) client-directed rollover forms (if applicable), and (iv) due diligence, are retained in the Client's file.

CCO Testing: The CCO or Delegate will review annually all investment advice covered under ERISA to ensure that each recommendation made to a Client was properly documented and adherence to all regulatory guidelines stated above have been met. The CCO or Delegate documents the findings within the Advisor's books and records

E. Treatment of Vulnerable Clients

The Advisor has adopted the following procedures designed to identify, protect, and proactively address instances of diminished capacity and financial exploitation. The Advisor has determined that any Client over the age of 62, subject to a state-specific Adult Protective Services statute, or exhibiting diminished capacity behavior or being exploited financially to be considered a "Vulnerable Client."

The Advisor will contact Vulnerable Clients, by phone or in person, on a more frequent than annual basis to ensure the Advisor's records relating to the Client profile is updated based on the Vulnerable Client's current life circumstances, including, but not limited to, job status, retirement, changes to named trustees/beneficiaries, or death. The Advisor will leverage this communication to determine whether there are any instances of diminished capacity and/or risk of financial exploitation.

<u>Red Flags for Diminished Capacity</u>

- Confusion with simple concepts
- Repeating instructions or questions
- Memory loss or disorientation
- Difficulty performing familiar tasks

<u>Red Flags for Financial Exploitation</u>

- Unexpected addition of authorized persons or changes to beneficiaries, trustees, and/or powers of attorney
- Unknown individual becomes active in the Client relationship
- Discussion of unusual or unexpected investments

<u>Protecting Vulnerable Clients</u>

In order to protect Vulnerable Clients, the Advisor has implemented the following business practices:

- The Advisor should attempt to have Vulnerable Clients designate a trusted third-party ("Authorized Individual") and grant the Advisor permission to communicate with the Authorized Individual via phone, email, fax, or in person to obtain, and the Advisor to share, Client information including, but not limited to, account positions, transaction history, and personally identifiable Client information;
- Assist the Vulnerable Client in determining whether they should obtain durable power of attorney or engage with an estate attorney to establish estate documents;
- Update suitability guidelines as appropriate for the Vulnerable Client to continually follow and assist all parties with the ongoing management of the Vulnerable Client's assets and accounts;
- Remind the Vulnerable Client of the importance of compiling and safekeeping documents, including, but not limited to, wills, birth certificates, marriage and divorce certificates, Social Security information, life-insurance policies, financial documents, and a listing of the Client's possessions; and
- Obtain contact information for the Vulnerable Client's attorney, family members, and establish a line of communication with beneficiaries/trustees in the event of a Vulnerable Client's diminished capacity, financial abuse, and/or death.

PLEASE NOTE: Upon detection of suspected diminished capacity, the Supervised Person will notify the CCO promptly to document the instance, along with proper documentation of the findings and any actions taken. The CCO will work with the Authorized Individual, attorneys, and trustees/beneficiaries on taking appropriate measures with the Vulnerable Client.

Upon detection of suspected financial exploitation, the Supervised Person will notify the CCO promptly to document the instance, along with proper documentation of the findings and any actions taken. The CCO will present documentation and records that are relevant to the suspected or attempted financial exploitation to respective parties including, but not limited to, trusted third parties, state, or government authorities. Additionally, the Advisor, in its discretion based on the facts and circumstances surrounding the Vulnerable Client, can take necessary action, including, but not limited to, imposing a hold on asset transfers from an account of an eligible Vulnerable Client for up to 15 business days if financial exploitation is suspected. The hold can be extended for an additional ten (10) days at the request of either the state securities regulator or adult protective services.

F. Treatment of Client Termination

Whether the termination is Advisor-initiated, Client-initiated, or as a result of the passing of a Client, the Advisor maintains procedures for terminating the relationship. When a Supervised Person becomes aware of a Client termination, the Supervised Person will communicate the reason for termination to the COO. There may be instances where a Client moves all of their accounts away from the Advisor without communicating the termination to the Advisor. In such instances, the Advisor will send out a termination notice to the Client to effectively terminate the Advisory Agreement. Additionally, the COO will complete the following:

- add the terminated relationship to the Client Termination Log
- ensure appropriate documentation in the Client's file as to why the Client relationship was terminated;
- ensure the refund of any prepaid advisory fees if the Advisor billed the client in advance; and
- assist as appropriate with the outgoing asset transfers.

Client Death or Incapacitation

In the event of death or incapacitation of a Client, the Advisor will request a copy of the death certificate to maintain in the Client's file, review the Client's estate documents and contact respective custodians and applicable third parties to the Client's estate to determine next steps and what is in the best interest of the Client. Items to consider include, but are not limited to:

- Identification of beneficiaries;
- Timing and direction from the Executor of the Client's estate; and
- Management of the account[s], including:
    - Freezing and/or liquidating the accounts
    - Repapering of Account Information
    - Transfer of Assets

CCO Testing: The CCO or Delegate conducts quarterly reviews of all closed accounts to ensure there have been no oversights in Client terminations. Additionally, the CCO or Delegate will conduct an annual review of terminated Clients to ensure that the Advisor is compiling and maintaining sufficient information around the termination and refunding. The review will be maintained within *AdvisorCloud360®.*

G. Treatment of ERISA Clients

The Employee Retirement Income Security Act of 1974 ("ERISA") is a federal law that establishes legal guidelines for private pension plan administration and investment practices. ERISA was written to protect plan beneficiaries and participants from problems and abuses. ERISA contains a number of provisions that address individuals and firms that are engaged in managing ERISA accounts or provide advisory services to employee benefit plans. In cases where the Advisor or its representatives are unsure of these provisions and responsibilities, they should seek expert advice prior to contracting with an ERISA account.

PLEASE NOTE: As a matter of policy, the Advisor does not provide advisory services to ERISA accounts. Prior to taking on an ERISA plan as a Client, the Advisor will amend its policies and procedures so that they comply with ERISA.

H. Client Fees

The fiduciary duty of the Advisor to its Clients requires that careful attention is applied to the Advisor's fee methodology and billing practices. The methodology for Client fees is disclosed in the Disclosure Brochure, as well as in the Advisory Agreement.

The Advisor will ensure that at the onset of an engagement, the advisory fee is agreed upon between the Client and the Advisor and properly documented within the client's Advisor Agreement. If there is any exception to the advisory fees charged to a client (e.g., non-managed assets, accounts with different fees, bill to accounts, etc.), the Advisor will ensure proper and thorough documentation either within the Advisory Agreement or the respective Client's file.

The Advisor will ensure that any changes to advisory fees are properly documented. The Advisor has implemented the following policy regarding changes to advisory fees:

- If advisory fees are raised, the Advisor will be required to obtain a written acknowledgment from the Client regarding the increase in advisory fees.
- If advisory fees are being lowered, the Advisor will ensure that it creates a written memo within the Client's file addressing the lowered fee, the date it was lowered and any other pertinent information. If the Advisor decides to then raise the advisory fee, the Advisor will be required to obtain a written acknowledgment from the Client.

Fee Methodology

The Advisor's standard policy is to calculate fees as a percentage of assets under management. The Advisor may waive, modify, or reduce the fees for certain Clients. Any deviation from the standard fee assessment or calculation terms must be agreed to in writing by the Advisor and the Client in advance of any fee calculation. The Advisor should document any instances of deviation from the standard fee assessment.

Fee Billing

The Advisor will review fee calculations before billing Clients either via invoice or direct deduction in order to minimize any potential miscalculated fees being charged to Clients of the Advisor. The Advisor provides Clients with a quarterly report itemizing the fee, including the calculation period covered by the fee, the account value and the methodology used to calculate the fee. For certain alternative investments (e.g., private funds, limited partnerships etc.) the Advisor may not receive final valuations for the billing period prior to the fee billing calculation. In such instances, the Advisor will perform a reconciliation of billing once final valuations are received by the Advisor.

CCO Testing: The CCO or Delegate periodically reviews the Client's fee billing and methodology to ensure accurate billing and documents the findings in the Advisor's books and records.

I. Custody

An advisor is deemed to have custody of client accounts if it directly or indirectly holds client assets, has any authority to obtain possession of them, or has the ability to appropriate them. The following situations create a custody status:

- *Constructive Custody* (Annual surprise custody audit not required)
    - Deducting advisory fees from client accounts
    - Maintaining standing letters of authorization ("SLOA") to third parties

An advisor may allow the above activities and will not be subject to the implications of "Real Custody" as detailed below if certain safeguards are met. Please see Fee Deduction and Standing Letters of Authorization below.

- *Real Custody* (Annual surprise custody audit required)
    - Collecting more than $500 in advisory fees, six months or more in advance
    - Maintaining client login credentials
    - Serving as trustee for client accounts
    - Having power of attorney over client accounts

- Holding onto client checks for longer than 72 hours (3 business days)
- Receiving stock certificates from the client and forwarding them to the custodian
- Managing a private fund

PLEASE NOTE: As a matter of policy, the Advisor does not have real custody over Client funds or securities, however, the Advisor does have constructive custody due to the deduction of advisory fees from Client accounts.

Fee Deduction

The Advisor is considered to have custody of Client assets because they have the ability to have fees paid directly from Client accounts. The Advisor has adopted the following policies and procedures regarding assets in Client accounts. The Advisor will: (1) segregate Client funds and securities and maintain them with a "qualified Custodian" in an account in that Client's name, (2) promptly notify Clients in writing of any new or changes to a current qualified Custodian's name, address, and the manner in which the funds or securities are maintained, and (3) ensure that the qualified Custodian sends a quarterly account statement to each Client, identifying the amount of funds and each security in the Client account at the end of the period and setting forth all transactions during that period.

"Due Inquiry" Requirement - The Advisor conducts a "due inquiry" in order to establish a basis that the qualified Custodian sends account statements to each Client no less frequently than quarterly. To accomplish the "due inquiry" requirement, the CCO or Delegate receives written confirmations on their own personal accounts from the Custodian that the account statement was sent, giving the Advisor reasonable belief and assumption that Client statements were sent to Clients by the Custodian. Accessing the Client's account statements on the Custodian's website will not satisfy the "due inquiry" requirement because it does not confirm the account statement was actually delivered to the Client.

Standing Letters of Authorization to Third Parties

An advisor may have custody of assets if they have SLOAs to third parties, thereby requiring the advisor to disclose that they have custody of client funds. However, an advisor may not subject to the independent surprise examination requirement of the Custody Rule as long as they meet the seven (7) conditions below:

1. The client provides an instruction to the custodian, in writing, that includes the client's signature, the third-party's name, and either the third party's address or the third party's account number at a custodian to which the transfer should be directed.
2. The client authorizes the advisor, in writing, either on the custodian's form or separately, to direct transfers to the third party either on a specified schedule or from time to time.
3. The client's custodian performs appropriate verification of the instruction, such as a signature review or other method to verify the client's authorization, and provides a transfer of funds notice to the client promptly after each transfer.
4. The client has the ability to terminate or change the instruction to their chosen custodian.
5. The advisor has no authority or ability to designate or change the identity of the third-party, the address, or any other information about the third party contained in the client's instruction.
6. The client's custodian sends the client, in writing, an initial notice confirming the instruction and an annual notice confirming the instruction.
7. The advisor maintains records showing that the third party is not a related party to the advisor or located at the same address as the advisor.

PLEASE NOTE: As a matter of policy, the Advisor does not have SLOAs to third parties.

Advance Collection of Fees

As a matter of policy, the Advisor does not collect advance payments of $500 or more, six (6) months in advance of services rendered. In the event that more than $500 is collected, the Advisor will ensure services are completed within six (6) months.

Login Credentials

An advisor may be deemed to have custody of assets if they maintain client login credentials. The maintenance of login credentials creates a custody status for assets within those accounts because, with client login information, the Advisor will have the ability to change certain fields and/or presets within the Client's account including, but not limited to, mailing address, e-mail address, bank accounts, etc. Additionally, with login

credentials, an advisor has the ability to transfer funds out of the account without triggering approval from the Client.

PLEASE NOTE: As a matter of policy, the Advisor does not maintain Client login credentials.

Executor, Conservator, Trustee Relationships or Power of Attorney
An advisor may be deemed to have custody of assets if they are appointed as trustee on a Client's account or have power of attorney authority for a Client. Power of attorney is a written document in which one person (the principal) appoints another person to act as an agent on his or her behalf, giving authority to the agent to perform certain acts or functions on behalf of the principal.

PLEASE NOTE: As a matter of policy, the Advisor does not serve as trustee or have power of attorney over any Client accounts.

Client Checks and Security Certificates
An advisor who holds onto client checks for more than seventy-two (72) hours is deemed to have custody on the assets and securities held.

As a matter of policy, the Advisor does not have custody through the handling of Client checks or security certificates. The Advisor has implemented the following internal procedures to ensure the proper handling of all checks and securities.

- Checks:
    - The Advisor will either forward checks to the Custodian or utilize remote check deposit via the Custodian's software within three (3) business days. Checks that are deposited remotely are kept for at least ten (10) days to ensure proper settlement of the funds.
    - Third party checks made payable to the Client will be forwarded to the Custodian or returned to the Client within three (3) business days.
- Security Certificates:
    - The Advisor will not accept security certificates at the Advisor's office but may advise Clients on how to securely deliver certificates to their Custodian and will tell Clients not to send security certificates to the Advisor's office.
    - If the Advisor receives security certificates inadvertently, the Advisor will promptly return/forward the security certificate[s] to the Client with instructions on how to direct them to the Custodian to deposit in their account[s].

The Advisor documents all checks and security certificates received, whether forwarded to the Custodian or returned to the Client, within the Checks and Securities Log. See AdvisorCloud360® for the Checks Log.

J. Client Money Movement

It is the responsibility of every Supervised Person of the Advisor, who interacts with Clients to verify any and all outgoing money transfer instructions when standing instructions are not on file with the Custodian. Any Supervised Person who verifies transfer instructions with the Client must be able to identify the Client over the phone or via two pieces of identifying information, prior to executing the outgoing money transfers. The following procedures are designed to mitigate the fraud risk that is pervasive in the industry. For additional information related to information security and fraud, please see Section 7.

Before any requests for funds transfer may be acted upon, the Advisor must first verify the Client and the authenticity of instructions.

First Party Money Movement
The Advisor does not accept first-party money movement instructions via email, fax, or mail. Supervised Persons must be in direct verbal contact with the Client.

- Recognizing the insecure nature of email, Supervised Persons should make every effort to obtain instructions from Clients in advance.
- The Advisor must document the date, time, and contact reached while confirming instructions and log the event with the Client record in their CRM system

When there is any doubt as to the identity of the individual to whom you seek verbal verification, the person making the call should require that the Client successfully answer at least two (2) identifying questions for which the Advisor could cross-reference responses, which could include, for example:

- Primary account holder's date of birth
- Address associated with the account
- Primary account holder's mother's maiden name

Third Party Money Movement

If a standing letter of authorization is not on file for third party money movement, the Advisor is required to obtain one-time authorization forms executed by the Client.

K. Client Complaints

In the course of providing advisory services, the Advisor and/or its Supervised Persons may receive complaints from Clients regarding their services or other related matters. The Advisor will respond appropriately and promptly to Client complaints that it receives and, when appropriate, take corrective actions in an effort to prevent future complaints. Any statement alleging specific inappropriate conduct on the part of the Advisor constitutes a complaint. A Client complaint must be initiated by the Client and must involve a grievance expressed by the Client. In many instances, it is difficult to determine whether or not a communication constitutes a "complaint". A mere statement of dissatisfaction from a Client about an investment or investment performance in most cases does not constitute a complaint. Supervised Persons should report all communications that could be construed as a complaint to the CCO who will determine if the communication actually qualifies as a "complaint".

Supervised Persons understand the importance of handling and documenting Client complaints, including informing the CCO of any Client communications that may be construed as a complaint in a timely manner. The following policy applies to the handling of Client complaints:

- Notify the CCO promptly
- Do not respond to the Client complaint without prior approval of the CCO.

PLEASE NOTE: The CCO will investigate and document each Client complaint within the Client Complaint Log and ensure it is responded to in a timely manner. *See* AdvisorCloud360® for the Client Complaint Log.

L. Anti-Money Laundering / Customer Identification Program

The Advisor's AML policy is to endeavor to prevent, detect, and report the possibility of money laundering. "Money laundering" is understood to be the process by which individuals or entities attempt to conceal the true origin and ownership of the proceeds of internationally recognized criminal activity, such as organized crime, drug trafficking, or terrorism. Money laundering involves the use of the financial system to disguise the origin of assets, for example, by creating complex layers of financial transactions and by the integration of the laundered proceeds into the economy as "clean" money. There are various laws and regulatory standards that govern entities in the effort to deter money laundering, including: the Bank Secrecy Act of 1970; the Money Laundering Control Act of 1986; and the USA PATRIOT Act.

It's important to note that since the Advisor does not custody Client assets but rather has Clients open accounts with Custodians for custody and transaction execution services, the broker-dealers will have the primary responsibility to carry out the AML requirements for the Advisor's clients. As such, the Advisor primarily relies on Custodians to conduct Anti-Money Laundering ("AML") and Customer Identification Program ("CIP") reviews on its Clients.

CCO Testing: The CCO or Delegate conducts an annual review of the Custodians to confirm the effectiveness of their AML policy and document the findings in the Advisor's books and records.

4. Portfolio Management and Trading

A. Investment Research and Monitoring

Securities Oversight

The Advisor has a fiduciary duty to conduct reasonable due diligence with respect to any security (or other financial instrument) that the Advisor buys, sells, or holds in a Client's portfolio. The Advisor's duty to conduct

reasonable due diligence generally increases with the complexity and uniqueness of a security (or other financial instrument).

The Advisor's primary area of research for a security lies in fundamental analysis. This analysis focuses on individual issuers and their potential in light of their financial condition, and market, economic, political, and regulatory conditions. The Advisor may compile information from multiple industry sources for insights including, but not limited to:

- Management quality;
- Product and/or service quality;
- Business cycle[s] for the company's key products or services;
- Earnings and cash flow;
- New product or service offerings in the pipeline that could enhance future growth Industry characteristics; and
- Competitive position in the marketplace.

When researching mutual funds or ETFs, prior fund returns, portfolio management tenure/stability, and fund rankings are also factored into the research.

CCO Testing: The CCO or Delegate conducts an ongoing review to determine if securities should continue to be held, sold, or if additional amounts of the security should be purchased. Factors weighed in determining any action include, but are not limited to:

- Price fluctuations;
- Company/Issuer announcements;
- Market news; and
- Portfolio guidelines.

The CCO or Delegate documents its due diligence surrounding securities in the Advisor's books and records.

B. Portfolio Suitability and Monitoring

The Advisor must manage each portfolio according to the investment strategy/mandate, and, as necessary, provide an explanation to the Client for material deviations from the agreed-upon mandate. Additionally, the Advisor will monitor account[s] to ensure adherence to any specific guidelines and restrictions.

The Advisor tracks each Client's individual portfolio guidelines. At the inception of the account, the Advisor will input the Client's guidelines into the Client's file, which will be monitored manually. The Advisor refers to the Client's file ahead of conducting any trading to ensure that securities under consideration fall within the Client's stated guidelines.

The Client's guidelines are also used during portfolio reviews. As part of these reviews, the securities held by each account are reviewed to ensure that the account's positions are consistent with the investment guidelines contained in the Client's file. Any issues, or potential issues, with portfolio strategy or individual positions, are reviewed and discussed.

<u>Mutual Fund Share Class Selection</u>
When purchasing mutual fund shares for a Client's account, a Client is subject to various fees and charges, including, but not limited to, the cost of portfolio management, creating account statements, account services, recordkeeping, commissions, and legal services. The particular fees and charges the Client will pay are generally determined by the share class that the client purchases.

Some share classes are subject to either a front-end sales charge or a deferred sales charge and may be appropriate when implementing a pure buy and hold strategy. Other share classes impose a higher ongoing fee (12b-1 fee) which is retained by the custodian.

PLEASE NOTE: As a matter of policy, the Advisor seeks to use the lowest cost share class available while taking into account the Client's investment time horizon and preference. Transaction charges should not impact investment decisions either from a trade frequency or investment selection standpoint. The Advisor requires that

pre-approval be obtained from the CCO or Delegate for any mutual fund investments where the lowest cost expense ratio share class available is not used.

CCO Testing: The CCO or Delegate periodically reviews accounts for adherence to investment guidelines, for example, suitability and mutual fund share class selection to ensure lowest cost share class is selected and documents the findings in the Advisor's books and records.

C. Trading Practices and Conflicts

Advisors generally must trade in accordance with procedures developed to ensure that the Advisor seeks best execution of Client orders. While the Advisor has fairly broad discretion to tailor policies to their specific operations, the Advisor must disclose potential material conflicts of interest and any procedures implemented to prevent these conflicts.

Directed Brokerage

While the Advisor will recommend a specific Custodian based on its initial and ongoing due diligence, the Client may ultimately direct the Advisor to utilize a specific Custodian. The Advisor requires that such direction is provided by the Client in writing, either as part of the Advisory Agreement or by separate instruction. Clients will then establish an account with a specific Custodian and direct the Advisor to place trades with that Custodian. Under these circumstances, the direction by a Client to execute trades with a particular Custodian means that the Advisor does not have the ability to choose the price of the security traded or the commission paid. The result could be higher commissions, greater spreads or less favorable net prices, than if the Advisor was empowered to negotiate commission rates or spreads freely, or to select brokers or dealers based on best execution.

To address the conflicts with regards to the limitations of client-directed brokerage with respect to best execution, the Advisor will provide full and accurate disclosures within the Advisory Agreement and Disclosure Brochure. Additionally, the Advisor conducts ongoing best execution due diligence to ensure its Custodian recommendations are in the best interest of its Client. The Advisor also discloses that Client directed transactions may not be combined or "batched" for execution purposes with orders for the same securities for other accounts the Advisor manages.

PLEASE NOTE: This activity has the potential for creating counterparty risk that may impact Clients. Counterparty risk is measured by the loss that a Client would incur if the counterparty failed to perform pursuant to the terms of transactional or contractual commitment. Counterparty risk increases when the Custodian's solvency is undermined either due to systemic risk, financial loss, negligence, potential regulatory or legal claims, or operational failures. Therefore, the Advisor has a due diligence process for assessing the counterparties to their trading activity, among other things. As a part of that consideration, the Advisor analyzes and makes judgments regarding a Custodian's financial condition over time, realizing that financial strength is subject to many unpredictable factors and sudden shocks.

Firm Trading Policy

Trade Aggregation - When the purchase or sale of a security is deemed to be in the best interest of more than one Client account, it is the Advisor's policy to aggregate, or "batch", orders for the purchase or sale of securities for all such Client accounts to the extent consistent with best execution and the terms of the relevant Advisory Agreements. Such combined trades are used to facilitate best execution, including negotiating more favorable prices, obtaining more timely or equitable execution, and/or reducing overall commission charges.

PLEASE NOTE: The Advisor will ensure that aggregated securities transactions in participating Client accounts are carried out in a fair and equitable manner, by upholding the following conditions:

- Aggregation policies are fully disclosed to all Clients;
- The Advisor does not favor any advisory account over any other account;
- The Advisor gives individual investment advice to each account;
- Each participating Client account receives the average price for each trading day;
- Trades are combined only if consistent with the duty to seek best execution and with the terms of the relevant Clients' Advisory Agreements;
- Aggregated trades are documented in the Advisor's books and records archive, including securities bought, sold and held by each participating account; and

- For each aggregated order, the books and records of the Advisor will separately reflect the securities bought, sold, and held by each account.

Trade Allocation - Generally, aggregated transactions are averaged as to price and transaction costs and will be allocated among participating accounts in proportion to the purchase and sale orders placed for each account on any given day (*i.e. pro rata*). While the Advisor will always try to allocate *pro rata* in the first instance, the Advisor may use other methods of allocation – provided that such methods are fair and equitable. The Advisor may use a random allocation method if limited availability or thinly traded securities (partial fills). In such instances, the Advisor will not include individual accounts and collective investment vehicles in which the Advisor, or its Supervised Persons, might have an interest.

PLEASE NOTE: The Advisor will ensure that allocation methods are fair and equitable, by upholding the following conditions:

- Allocation policies are fully disclosed to all Clients;
- The Advisor does not favor any advisory account over any other account; and
- The participating accounts and the relevant allocation method are specified in the Advisor's books and records before entering an aggregated order.

Trade Rotation - When all transactions for a particular security cannot be aggregated, the Advisor may be required to trade on a partial aggregated basis or account by account. The Advisor has developed procedures to ensure changes in the order of which accounts are traded first.

PLEASE NOTE: The Advisor will ensure that trade rotation policies are fair and equitable, by upholding the following conditions:

- The Advisor does not favor any advisory account over any other account;
- The Advisor gives individual investment advice to each account;
- For each trade, books and records of the Advisor will separately reflect the rotation process used.
- Methods for trade rotation used may include, but are not limited to:
    - Numerical by account number (ascending then descending)
    - Alphabetical by client last name (A-Z then Z-A)
    - Random allocation

Trading Away - Trading away is defined as a trading procedure that gives an advisor the opportunity to execute security trades at another custodian and having the trades settle at the advisor's current custodian.

PLEASE NOTE: As a matter of policy, the Advisor generally does not trade away from the Custodian. However, in certain instances, trade away transactions may be warranted when the Advisor's existing Custodian does not have access to markets that are suitable for certain Clients. As data regarding execution becomes more tangible through technology, best execution gains more transparency and may create obligations for Advisors to select other custodians to uphold their fiduciary duties.

Principal Transactions

Principal transactions involve securities transactions in which an advisor has a proprietary interest in the securities being traded. Principal transactions must be disclosed to clients in writing prior to the completion of the transaction and written client consent must also be obtained. Consent may be obtained after execution but prior to settlement of the transaction.

PLEASE NOTE: As a matter of policy, the Advisor does not engage in principal transactions and does not anticipate in doing so. In the event that a situation develops that might involve a principal transaction, appropriate disclosures will be made in advance of the transaction.

Agency Cross Transactions

Agency cross transactions involve securities transactions in which an advisor acts directly (or through an affiliate) as a client's advisor and as broker for the person on the other side of the transaction.

PLEASE NOTE: As a matter of policy, the Advisor does not engage in agency cross transactions and does not anticipate doing so. In the event that a situation develops that might involve an agency cross transaction, legal counsel will be consulted prior to the transaction.

Soft Dollars
Among the factors an advisor may consider in seeking best execution is the value of a custodian's execution and research services, including third-party research provided by the custodian (*i.e.*, "soft dollar" services), provided these services fall within the safe harbor of Section 28(e) of the 1934 Act.

PLEASE NOTE: As a matter of policy, the Advisor does not engage in soft dollar transactions and does not anticipate doing so. In the event that a situation develops that might involve the use of soft dollars, the Advisor will make all appropriate disclosures prior to entering into a soft dollar arrangement and ensure that the appropriate policies and procedures are in place.

Broker-Dealer Affiliation
Certain advisors may have an affiliated broker-dealer or supervised persons who are registered representatives of a broker-dealer. Client trades may be placed through an affiliated broker-dealer where an advisor, and/or its supervised persons, may receive commissions and/or other economic benefit from the trades. In such instances, there needs to be a higher level of care to be exercised when placing trades with affiliated broker-dealers to ensure the advisor is acting in the best interest of its clients.

PLEASE NOTE: As a matter of policy, the Advisor and its Supervised Persons do not have any broker-dealer affiliations. In the event that a situation develops that might involve a broker-dealer affiliation, the Advisor will make all appropriate disclosures and ensure that the appropriate policies and procedures are in place.

D. Trading Errors

It is the Advisor's policy to manage portfolios and place securities trades with a Custodian with accuracy, efficiency, and pursuant to sufficient legal authority. A "trade error" is generally any transaction resulting in Client funds being committed to unintentional transactions. Trade errors can result from a variety of situations involving portfolio management, trading, and settlements. Types of trading errors include, but are not limited to:

- Transposing an order (e.g., buying instead of selling);
- Purchasing or selling unintended securities or unintended amounts of securities;
- Allocating a transaction to the wrong account;
- Purchasing or selling securities that are not appropriate for an account;
- Selling a security a client does not own;
- Entering an order at the wrong price;
- Operational errors in calculating price/commission information or in arranging for settlement; and
- An error in the software used to conduct the trade.

Because a trade error generally results in Client money being at risk, the following trade review process and trade error correction policy generally apply:

Trade Review:
The CCO or Delegate reviews a sample of securities transactions in an attempt to verify accurate and proper reconciliation of trades with the Advisor's data, consistency of the securities transactions within the client's Investment Parameters for suitability; and the absence of any improper trading in the account.

Trade Error Identification:
Upon identification of a trade error, It is the Advisor's responsibility to evaluate the error and ensure that the appropriate party corrects the error.

Trade Error Correction:
The Advisor's policy is to identify and correct trading errors, over a de minimis amount, affecting any account as expeditiously as possible.

- Any error that results in a gain will accrue to the benefit of the account in which the error was made; and
- Any error that results in a direct loss will be reimbursed to the account in which the error was made. In no case will the Advisor use soft dollars to correct trade errors.

PLEASE NOTE: The Advisor maintains a log of all trading errors along with any relevant and supporting documentation such as communications with the Client and steps taken to remediate the issue. See AdvisorCloud360® for the Trade Error Log.

E. Best Execution

The duty to "seek best execution" (either at the security level or through the evaluation of the custodians the Advisor recommends) is not necessarily a directive to capture the best price or to minimize transaction costs. Both are difficult to achieve and even more difficult to prove. Best execution is viewed as a process, whereby the Advisor has established procedures to ensure that Clients are serviced by competitive vendors. The Advisor defines best execution in the context of the firm, taking into account the nature of the Advisor's business and trading procedures.

CCO Testing: The CCO or Delegate periodically reviews best execution quantitative and qualitative statistics and compares the Advisor's recommended Custodian to other competitive custodians to demonstrate the rationale for the recommended Custodian[s]. The findings of the best execution reviews are documented in the Advisor's books and records.

F. Proxy Voting

The right to cast votes on certain corporate matters is an important power given to shareholders of publicly traded companies and mutual funds. Since most shareholders do not attend annual meetings in person, their right to express their opinion on these matters are done by casting a ballot either electronically or via mail. An advisor is expected to address its role with respect to voting proxies on behalf of clients in an agreement and in the disclosure brochure. Clients may agree to take on the responsibility to vote proxies on securities they own, or they may elect to not vote their proxies at all. In any case, regulators expect an advisor to have clearly defined (and communicated) policies and procedures related to this vital aspect of corporate governance.

As a matter of policy, the Advisor will not vote, nor advise Clients on how to vote, proxies for securities held in Client accounts. The Client retains the authority and responsibility for the voting of proxies. The Advisor will not provide any advice or take any action with respect to the voting of proxies as agreed to in the Advisory Agreement and disclosed in the Disclosure Brochure. Should a Client have questions on a particular proxy, the Advisor may assist the Client in understanding the background and intent of the proxy, but shall not make any attempt to influence the Client in their voting decision.

G. Valuation

Advisors have a fiduciary duty to place its Client's interests first and foremost. This duty includes the securities valuation process which seeks to provide current, fair, and accurate valuations of investments. Conducting proper valuations of securities is important because it affects, among other things: (i) financial reporting; (ii) the calculation of advisory fees; (iii) performance reporting and presentations; and (iv) risk profiles. The Advisor relies on the Custodian for valuation for all securities, except for private investments [Custodian is solely the conduit for information].

Exchange-listed investments - If the Advisor identifies a security that is not priced, has a stale price or does not appear to be accurate, the CCO should be contacted immediately. The CCO will work with the Custodian to obtain an accurate price. The Advisor does not fair value securities.

CCO Testing: All securities held in accounts managed by the Advisor will be independently valued by the Custodian. The Advisor will not have the authority or responsibility to value portfolio securities. However, for exchange-listed investments, the CCO or Delegate periodically conducts a spot check to confirm the accuracy of the securities valuation provided by the Custodian and documents the findings within the Advisor's books and records.

5. Client Communications: Advertising & Sales Marketing

A. Client Communications

Any form of communication to Clients that is designed to solicit or maintain advisory service ("Client Communications") is covered by regulations under Securities Laws. The Advisor has developed the following policies and procedures to ensure compliance with these Securities Laws.

Securities Laws generally define the term "advertisement" to include any notice, circular, letter or other written communication addressed to more than one person, or any notice or other written announcement in any publication or by radio or television, which offers, among other things, "any investment advisory service with regard to securities". This definition includes all communications that the Advisor may use to solicit new Clients as well as maintain existing ones.

Additionally, written communications on a one-to-one basis to existing, or prospective, advisory Clients designed to offer advisory services, or maintain the existing Client, are deemed to be an advertisement. **However**, if the written communications to existing advisory Clients are solely designed to present the performance of their accounts, they are generally not considered advertisements.

B. Advertising Rule Content Standards

Securities Laws further provides that it shall find a violation has been committed when an investment advisor acts to publish, circulate, or distribute any advertisement which, among other things:

- Refers, directly or indirectly, to any testimonial;
- Refers, directly or indirectly, to past specific recommendations;
- Represents, directly or indirectly, that any graph, chart, formula, or other device being offered can, in and of itself, be used to determine which securities to buy or sell, or when to buy or sell them (unless sufficiently qualified);
- Contains any statement to the effect that any report, analysis, or other service will be furnished for free or without charge, unless such report, analysis or other service actually is or will be furnished entirely for free and without any condition or obligation, directly or indirectly; or
- Contains any untrue statement of a material fact, or which is otherwise false or misleading.

Past Specific Recommendations

Unless certain specific conditions are met, as noted above, the Advisor may not advertise its "past specific recommendations". To ensure compliance with this requirement, the Advisor will not name any specific issuer in any advertisement unless the Advisor complies with the requirements of Securities Laws: i.e. either lists, or offers to furnish a list of, each recommendation made during the immediately prior one-year period together with detailed information about each recommendation; or:

- The Advisor complies with relevant Securities Laws.
- The Advisor may provide a partial list of recommendations if: (1) securities are selected for inclusion based on objective, non-performance related criteria; (2) the same selection process is used in subsequent periods; (3) profits or losses attributable to any specific security listed are not discussed; and (4) appropriate supporting records are maintained.
- The Advisor may include information about past specific recommendations (in addition to testimonials) in certain types of materials not deemed advertisements for purposes of those sections of the Securities Laws that limit the use of past specific recommendations and testimonials. These materials include:
    - Oral communications other than those in radio or television broadcasts;
    - Written communications in response to unsolicited requests by a Client, prospective client, or consultant for specific information about the Advisor's past specific recommendations provided to: (1) the requesting Client, prospective Client, or consultant; (2) a single consultant on behalf of multiple Clients; or (3) several consultants; and
    - Written communications to the Advisor's existing Clients, provided that the purpose of the communication is not to offer advisory services.

Use of Performance Calculations

The recordkeeping rule requires Advisors to keep all of their advertisements and any document necessary to form the basis for performance information in advertisements ("supporting records"). The Advisor must keep advertisements and supporting records for five (5) years from the end of the fiscal year in which the advertisement was last published or otherwise disseminated. All documents necessary to form the basis for performance calculation should be kept for all years since inception.

Regulators will not review or approve Advisor advertisements prior to use. Whether any particular advertisement is false or misleading will depend upon the particular facts and circumstances surrounding its use. The burden of determining what is "false or misleading" is on the Advisor, and is an aspect of the Advisor's advertising review process.

Performance Presentation Standards

A performance communication is deemed fraudulent if it does any of the following:

- Fails to disclose the effect of material market or economic conditions on the results portrayed. For example, an advertisement stating that the accounts of the Advisor's Clients appreciated 25% in value without disclosing that the market generally appreciated 40% during the same period.
- Includes some model or actual results that do not reflect the deduction of advisory fees, brokerage or other commissions, and any other expenses that a Client would have paid or actually paid. In certain one-on-one presentations, performance results may be presented on a gross basis if at the same time the Client receives in writing:
    - Disclosure that the performance figures do not reflect the deduction of investment advisory fees;
    - Disclosure that the Client's return will be reduced by the advisory fees and any other expenses it may incur in the management of its investment advisory account;
    - Disclosure that the investment advisory fees are described in the Advisor's Disclosure Brochure; and
    - A representative example (table, chart, graph, or narrative) that shows the effect on performance that investment advisory fees, compounded over a period of years, could have on the total value of a Client's portfolio.
- Fails to disclose whether and to what extent the results portrayed reflect the reinvestment of dividends and other earnings.
- Suggests or makes claims about the potential for profit without disclosing the possibility of loss.
- Compares model or actual results to an index without disclosing all material facts relevant to the comparison.
- Fails to disclose any material conditions, objectives, or investment strategies used to obtain the results portrayed.
- Fails to disclose prominently, if applicable, that the results portrayed relate only to a select group of the Advisor's Clients, the basis on which the selection was made, and the effect of this practice on the results portrayed, if material.

Use of Articles from News Media

Regulators take the position that certain articles from the news media are not prohibited by Securities Laws, which prohibits the use of testimonials by an Advisor. Distribution by an Advisor of a *bona fide* news article, written by an unbiased third party, is not subject to the requirements of the rule governing advertisements; articles that refer to prior recommendations of advisors may be distributed if the prior recommendations are solely contained within the article. However, using such reprints is subject to Securities Laws, which makes it a violation for the Advisor to publish an advertisement that contains any untrue statement of a material fact or is otherwise misleading.

C. Interactive Media Communications

Advisor Use of Social Media

The Advisor may utilize various interactive media communications ("Social Media") to communicate the Advisor's services with Clients, prospective clients, and others. The Advisor is required to supervise all Social Media activities that communicated the Advisor's services or information, which includes business accounts operated by Supervised Persons. These permitted business Social Media activities may include the use of the following media outlets:

- Company website[s];

- LinkedIn;
- Facebook;
- Twitter;
- Blogs; and
- Any other communication medium that is considered social media.

Supervised Person Use of Social Media
Unless permitted and pre-approved by the CCO or Delegate, Social Media activity from a Supervised Person's personal account is prohibited from referencing the Advisor's services or information on their personal accounts. In addition to the Advisor's Code, generally, all permitted Social Media activities on behalf of the Advisor or Supervised Persons, must adhere to the Advisor's Client Communications guidelines, as defined above and highlighted below:

- Must not contain any false or misleading statements or omission of material facts;
- Must not contain any specific securities recommendations;
- Must not contain any testimonials; and
- Must not contain any confidential Client or employer information.

CCO Testing: The CCO or Delegate conducts an at least annual review of social media profiles to ensure adherence to the standards of the Advertising Rule. The review is documented in the Advisor's books and records.

D. Review and Approval Process

The Advisor is required to keep records of Client Communications and to reasonably guard against fraud and misrepresentation. All Supervised Persons creating and delivering Client Communications will be subject to post-use review by the CCO.

CCO Testing: The CCO or Delegate conducts a post sample review of advertising materials to ensure adherence to the standards of the Advertising Rule. The review is documented in the Advisor's books and records.

6. Regulatory Filings

A. Form ADV Filings and Amendments

The Advisor may be required to file various forms and reports on both an annual and ongoing basis to maintain their status and provide updates to various states and/or regulators.

Form ADV
Form ADV is a uniform form used by registered investment advisors for registration. Form ADV is broken into two parts.

Form ADV Part 1*:* Form ADV Part 1 is an online form filed through the IARD system.

Annually, within ninety (90) days following fiscal year-end, the Advisor reviews, updates as necessary, and files its Form ADV Part 1 via FINRA's IARD system.

Additionally, Form ADV Part 1 will be amended and filed if the Advisor adds or removes a relying adviser as part of an umbrella registration, the information provided in response to Items 1, Item 3, Item 9, or Item 11 of Part 1A or Sections 1 or 3 of Schedule R becomes inaccurate in any way. The Advisor will file an amendment to the Disclosure Brochure through IARD within 30 days of the change.

Form ADV Part 2A - Disclosure Brochure*:* The Disclosure Brochure is a narrative of the Advisor with a primary purpose of providing Clients with a clearly written and meaningful disclosure, in plain English, about the Advisor's services, fees, business practices, conflicts of interest, and material business relationships with affiliates. The Disclosure Brochure must also be kept current and made available during regulatory examinations. It must be provided to prospective clients prior to or at the time of the signing of an Advisory Agreement and becoming a

client of the Advisor. The Disclosure Brochure is required to be filed through the FINRA IARD system for review by both federal and state regulators.

Annually, within ninety (90) days following fiscal year-end, the Advisor must review, update, and file its Form ADV Part 2A – Disclosure Brochure and Appendix 1 – Wrap Fee Program Brochure (if applicable) via FINRA's IARD system.

Additionally, the Disclosure Brochure Wrap Fee Program Brochure (if applicable) must be amended and filed should any material change occur in the Advisor's business practice throughout the year including, but not limited to, investment process, fees charged, ownership structure, business address, contact information, disciplinary disclosure, conflicts of interest, and/or other notable aspects of the Advisor's business. The Advisor will file an amendment to the Disclosure Brochure through IARD within thirty (30) days of the change.

Form ADV2B - Brochure Supplement(s)*:* The Brochure Supplement(s) contains information about the Advisor's Advisory Persons. The Brochure Supplement is required to be filed through the FINRA IARD system.

There is no annual update or filing requirement for the Brochure Supplement. However, the Brochure Supplement must be amended whenever there is a material change to an investment adviser representative's disclosure information, employment, education and/or outside business activities.

The Advisor maintains a copy of each Disclosure Brochure and Brochure Supplement and each amendment or revision.

Form ADV-W - Withdrawal
In the event that the Advisor has ended its Client relationships in a particular jurisdiction and intends to no longer operate in that jurisdiction, the Advisor is required to notify the respective regulatory agency of that change. To notify current regulators, the Advisor will submit a timely filing of Form ADV-W, which is the form used to withdraw registration from a jurisdiction or when transitioning to a different regulator.

Additional State Filings
In addition to the standard filing requirements of the Form ADV there may be further filings required by certain States/Jurisdictions. The Advisor keeps itself appraised of changes to State Securities Laws where they conduct business and submit any required State filings as applicable.

CCO Testing: The CCO or Delegate periodically reviews Client geography to determine which states, if any, require the Advisor to register in that State. The Advisor will promptly begin a State registration and provide corresponding fees and documents to the State.

B. IAR Registrations, Disclosures, and Amendments

Advisory Persons are required to register as IARs with states in which the Advisor conducts business unless exempted from registration in a particular state. The states may require registration and/or licensing of IARs who: (i) provide advice to "retail" Clients, meaning natural persons other than "qualified clients"; (ii) have more than five (5) clients in the respective state[s] with the exception of Louisiana, Nebraska, New Hampshire, and Texas, and (iii) have a "place of business" within a state. The CCO or Delegate will review IAR registration requirements prior to soliciting business in any state in which its IARs have a "place of business" because the definition and requirements for an IAR vary from state to state.

Form U4
The U4 Filing is used by IARs to enable their individual registration with applicable regulators and jurisdictions. Advisors should amend an IAR's Form U4 to address state registrations, changes in residential address, disclosure items, and/or changes to outside business activities.

Form U5
The U5 Filing is submitted to withdraw an individual's registration as an IAR. A partial U5 can either remove IAR registrations in specific jurisdictions or, if they have fully resigned from the Advisor, a full U5 can be submitted to remove all registrations of that IAR with the Advisor.

Form ADV2B - Brochure Supplement
As noted above, the Brochure Supplement is not required to be filed through the FINRA IARD system, but the Advisor must keep copies and all amendments in their books and records. Advisors should update the Brochure Supplement to address material changes, such as, outside business activities, additional compensation received and financial, and/or disciplinary matters.

Financial & Disciplinary Disclosures
Securities laws require the Advisor to disclose any instances where the Advisor and/or its Supervised Persons have been found liable in a legal, regulatory, civil, or arbitration matter that alleges violation of securities and other statutes; fraud; false statements or omissions; theft, embezzlement or wrongful taking of property; bribery, forgery, counterfeiting, or extortion; and/or dishonest, unfair or unethical practices. The ability to view the Advisor's IARs backgrounds is on the Investment Adviser Public Disclosure website at www.adviserinfo.sec.gov by using their name or CRD# to search.

C. Exchange Act Filings

Certain Clients may hold significant positions in publicly traded equity securities and as such the Advisor may need to make certain filings with the SEC under the Securities Exchange Act of 1934 ("Exchange Act"). The various filings and our procedures for ensuring the timely submission of these filings are described in this section of the Compliance Manual. The Advisor monitors, on an ongoing basis, any matters that may require amendments or additional filings.

Schedule 13F
If an advisor acts as an institutional investment manager with investment discretion with respect to accounts of $100 million or more of exchange-traded or NASDAQ securities, based upon the list of designated securities published quarterly by the SEC, the advisor must file a Form 13F, reporting: (1) the name of the issuer; (2) the number of shares held; and (3) the aggregate fair market value of each security held. For a list of all 13F Securities, please go to www.sec.gov/divisions/investments/13flists.htm.

PLEASE NOTE: To date, Schedule 13F filing has not been triggered. Should the Advisor exceed the $100 million discretionary threshold, the Advisor will implement the following procedures for 13F Filings:

- The Advisor will make its first 13(f) filing within 45 days after the calendar year-end, or by February 14.
- The Advisor will continue to make quarterly filings prior to the filing deadline for each of the successive three calendar quarters. For specific dates, please refer to the SEC website.
- The Advisor will make these filings as described in the rule and will retain the filing records.

CCO Testing: The CCO or Delegate periodically compares the Advisor's assets to the SEC's most current quarterly 13F securities list using data query to determine if the Advisor has exceeded the $100 million threshold and document the findings in the Advisor's books and records.

Schedule 13D
Schedule 13D must be filed if any person who acquires beneficial ownership of more than five (5) percent of a class of any U.S. registered equity security with more than an investment return purpose in owning the security. Schedule 13D must be filed with the SEC and sent to the issuer of the security and to each exchange on which the security is traded. Advisors are required to file Schedule 13D electronically on EDGAR.

PLEASE NOTE: To date, Schedule 13D filing has not been triggered. Should the Advisor exceed the threshold, the Advisor will timely and accurate 13D Filing.

Schedule 13G
Schedule 13G may be filed in lieu of Schedule 13D if an advisor's holdings were acquired in the ordinary course of business and not with the purpose of changing or influencing control of the issuer. If the Advisor's ownership intent changes to an intent or effect of causing a change in control of the issuer, a Schedule 13D must be promptly filed.

PLEASE NOTE: To date, Schedule 13G filing has not been triggered. Should the Advisor exceed the threshold, the Advisor will timely and accurate 13G Filing.

Schedule 13H

Schedule 13H require large traders, whose transactions in non-marketable securities equal or exceed two (2) million shares or $20 million during any calendar day, or twenty (20) million shares or $200 million during any calendar month, to identify itself to the SEC and make certain disclosures to the SEC on Form 13H within EDGAR.

PLEASE NOTE: To date, Schedule 13H filing has not been triggered. Should the Advisor exceed the threshold, the Advisor will timely and accurate 13H Filing.

7. Privacy, Information Security and Technology Use

A. Cybersecurity

Cybersecurity is a separate policy and procedure document of the Advisor's Compliance Program ("Cybersecurity Policy"). The Advisor has adopted the Cybersecurity Policy to provide guidance to the Advisor's Supervised Persons on the storage and/or transmission of confidential digital information. The Advisor has addressed the following important concepts and controls in well-defined terms within the Cybersecurity Policy:

- Storage of confidential digital information
- Transmission of confidential digital information
- Receipt and acknowledgment of adherence to the Cybersecurity Policy

CCO Testing: The CCO or Delegate periodically tests for adherence to the policies stipulated in the Cybersecurity Policy. The CCO or Delegate documents these reviews within the Advisor's books and records.

B. Regulation S-P: Safeguard and Disposal Rule

The SEC has adopted amendments to the rule under Regulation S-P requiring advisors to adopt policies and procedures to address administrative, technical, and physical safeguards (the "Safeguard Rule") for the data security, integrity, and confidentiality of customer records and information. The SEC has further required that policies and procedures take reasonable measures to protect against unauthorized access or use of the information in connection with its collection, storage, transmission, and disposal (the "Disposal Rule").

To meet the standards of both the Safeguard and Disposal Rules, the Advisor has developed policies and procedures to apply security measures to reasonably safeguard its private Client information during its course of ownership and through its disposal, such as shredding physical documents and coordinating with their technology service provider to destroy digital storage devices, as noted in the Advisor's Privacy Policy. The Advisor will also apply firewalls, anti-virus, and other information security tools as needed to safeguard client information. Should the Advisor become aware that unauthorized parties have accessed client information, the Advisor will take additional steps to stop and prevent further unauthorized access and contact any Clients impacted to notify them of potential fraudulent activity in their name or accounts.

C. Regulation S-ID: Identity Theft Red Flag Program

Regulation S-ID requires certain financial institutions to establish an identity theft red flags program designed to detect, prevent, and mitigate identity theft. There are four key elements that advisors must address in their Identity Theft Prevention Program (ITPP), including:

- Identifying relevant red flags
- Detecting red flags
- Responding appropriately to red flags
- Maintaining the ITPP

Advisors must determine which red flags are relevant to their businesses and the covered accounts they manage over time. There is no specific list of red flags that are mandatory and no specific policies and procedures are required. However, a list of factors that the entity should consider (with examples) is included in the guidelines from the SEC along with an expectation that entities will respond and adapt to new forms of identity theft and the related risks as they arise.

Identifying Relevant Red Flags

The CCO or Delegate will periodically determine whether it offers or maintains covered accounts by conducting a risk assessment of their ITPP, including the risk factors, sources, and categories of Red Flags.

Risk factors include the types of covered accounts the advisor offers or maintains, the methods it provides to open or access its covered accounts, and its previous experiences with identity theft.

Sources of Red Flags include incidents of identity theft that the Advisor has experienced, methods of identity theft that have been identified as a result of changes in identity theft risks, and applicable regulatory guidance.

Categories of Red Flags include alerts, notifications, or other warnings received from consumer reporting agencies or service providers (such as fraud detection services) as well as suspicious documents and other customer unusual conduct or requests.

A red flag is a transaction that a Supervised Person knows or suspects to:

- Involve proceeds from an illegal activity;
- Evade currency transaction reporting requirements;
- Vary significantly from the Client's normal investment activities; or
- Have no business or apparent lawful purpose and the Advisor knows of no reasonable explanation for the transaction after examining the available facts, including the background and possible purpose of the transaction.

The Advisor utilizes various Custodians to supplement its own efforts to identity and manage identity theft red flags. The Advisor considers the following risk factors when identifying relevant red flags for covered accounts:

- the types of covered accounts offered;
- the methods provided to open or access these accounts; and
- previous experiences with identity theft.

In addition, Red Flags from the following five categories and the "Red Flag Identification & Detection Grid" ("Grid") have been considered:

- alerts, notifications, or warnings from a credit reporting agency or service providers;
- presentation of suspicious documents;
- presentation of suspicious personal identifying information;
- unusual use of, or other suspicious activity related to a covered account; and
- notice from other clients, victims of identity theft, law enforcement authorities, or other
- persons regarding possible identity theft in connection with covered accounts.

It should be noted that the examples listed in the "Red Flag Identification & Detection Grid" are not exhaustive, nor do they constitute a mandatory checklist, but should be utilized as a resource of relevant red flags in the context of the business. Additionally, the Advisor will rely on its custodian/broker dealer and investment management platforms for certain detections of red flags as noted below.

Red Flag	Detecting the Red Flag
Category: Alerts, Notifications or Warnings from a Consumer Credit Reporting Agency **Category: Suspicious Documents**	
1. Identification presented looks altered or forged.	The Advisor or its Custodian 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.	The Advisor or its Custodian will ensure that the photograph and the physical description on the identification match the person presenting it.
3. Information on the identification differs from what the identification presenter is saying.	The Advisor or its Custodian will ensure that the identification and the statements of the person presenting it are consistent.

4. Information on the identification does not match other information The Advisor has on file for the presenter, like the original account application, or copy of the client's signature -	The Advisor or its Custodian will ensure that the identification presented and other information we have on file from the account, such as the address on their driver's license are consistent.
5. The application looks like it has been altered, forged or torn up and reassembled.	The Advisor or its Custodian will scrutinize each application to make sure it is not altered, forged, or torn up and reassembled.
Category: Suspicious Personal Identifying Information	
6. Inconsistencies exist between the information presented and other things known or can find out about the presenter by checking readily available external sources.	The Advisor or its Custodian will review any flagged items including addresses, social security numbers, or other CIP information that has multiple client matches or other problems and take appropriate steps
7. Personal identifying information presented has been used on an account The Advisor knows was fraudulent.	The Advisor or its Custodian will compare the information presented with addresses and phone numbers on accounts or applications found or were reported to be fraudulent.
8. Personal identifying information presented suggests fraud, such as an address that is fictitious, a mail drop, or a prison; or a phone number is invalid, or is for a pager or answering service.	Custodians will send communications to all address changes (to the old address and the new one). The Advisor will review any returned mail to verify its accuracy.
9. The SSN presented was used by someone else opening an account or other clients.	The Advisor or its Custodian will compare the SSNs presented to see if they were given by others opening accounts or other clients.
10. The address or telephone number presented has been used by many other people opening accounts or other clients.	The Advisor or its Custodian will compare address and telephone number information to see if they were used by other Client and clients.
11. A person who omits required information on an application or other form does not provide it when told it is incomplete.	The Advisor or its Custodian will track when Clients or clients have not responded to requests for required information and will follow up with the Clients or clients to determine why they have not responded.
12. Inconsistencies exist between what is presented and on The Advisor's file.	The Advisor or its Custodian will verify key items from the data presented with information they have on file.
13. A person making an account application or seeking access cannot provide authenticating information beyond what would be found in a wallet or consumer credit report, or cannot answer a challenge question.	The Advisor or its Custodian will authenticate identities for existing clients by asking challenge questions that have been prearranged with the client and for Clients or clients by asking questions that require information beyond what is readily available from a wallet or a consumer credit report.
Category: Suspicious Account Activity	
14. Soon after The Advisor gets a change of address request for an account, they are asked to add additional access means (such as - checks) or authorized users for the account.	Custodians 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 Advisor.
15. An account develops new patterns of activity, such as - distribution request frequency, an increase in trading, instructions sent via email, or transactions not typical of the client	The Advisor or its Custodian will contact the client at the phone number on file to discuss
16. Mail The Advisor sends to a client is returned repeatedly as undeliverable even though the account remains active.	The Advisor or its Custodian will note any returned mail for an account and immediately check the account's activity and attempt to contact the client at the phone number on file to discuss
17. The Advisor learns that a client is not getting his or her paper account statements.	The Advisor or its Custodian will record on the account any report that the client is not receiving paper statements and immediately investigate them.

18. The Advisor is notified that there are unauthorized - transactions to the account.	The Advisor or its Custodian will verify if the notification is legitimate and involves a firm account, and then investigate the report.
Category: Notice from Other Sources	
19. The Advisor is told that an account has been opened or used fraudulently by a client, an identity theft victim, or law enforcement.	The Advisor or its Custodian will verify that the notification is legitimate and involves a firm account, and then investigate the report.
20. The Advisor 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 Advisor or its Custodian will contact the client to learn the details of the unauthorized access to determine if other steps are warranted.

Detecting Red Flags

The ITPP should address the detection of Red Flags in connection with the opening of covered accounts and existing covered accounts by: (i) obtaining identifying information about, and verifying the identity of, a person opening a covered account and (ii) authenticating customers, monitoring transactions, and verifying the validity of change of address requests for existing covered accounts.

The Advisor will review the opening and maintenance procedures for covered accounts in order to detect Red Flags. For opening covered accounts, which can include obtaining identifying information, the Advisor will verify the identity of the person opening the account and request relevant supporting documentation. For existing covered accounts, the Advisor will verify client's identity, monitor transactions, and verify the validity of changes that are requested.

Responding Appropriately to Red Flags

Based on the Red Flags that have been detected and the suggested responses for mitigating identity theft, the following procedures have been developed to respond to detected identity theft Red Flags. When the Advisor has been notified of a Red Flag or detection procedures show evidence of a Red Flag, the following steps will be taken, as appropriate to the type and seriousness of the threat:

I. Client (*Red Flags raised by someone applying for an account*)

Review the Application. The Advisor will review the Client's information collected for opening an account (e.g., name, date of birth, address, and an identification number such as a Social Security Number or Taxpayer Identification Number).

Request Government Identification. If the Client is applying in person, a current government-issued identification card, such as a driver's license or passport will be checked.

Seek Additional Verification. If the risk of identity theft is probable or large in impact, the Advisor may also verify the person's identity through non-documentary methods, including:

- Contacting the Clientthrough the contact information provided;
- Independently verifying the client's information by comparing it with information from a credit reporting agency, public database or other source such as a data broker or the Social Security Number Death Master File;
- Checking references with other affiliated financial institutions (Clearing firm does this), or
- Obtaining a financial statement.

Deny the Application. If the Client is found using an identity other than his or her own, the account will be denied.

Report. If the Client is found using an identity other than his or her own, The Advisor will report it to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. It may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," be reported to the appropriate FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and the Advisor's clearing firm.

Notification. If determined that personal identifiable information has been accessed, The Advisor will prepare any specific notice or any other required notice under state law to clients.

II. Access Seekers (*Red Flags raised by someone seeking access to an existing client's account*)

Watch. The Advisor will monitor, limit, or temporarily suspend activity in the account until the situation is resolved. This may involve working in conjunction with its Custodians where applicable.

Check with the Client. The Advisor will contact the client, describe what was found and verify with them that there has been an attempt at identify theft.

Heightened Risk. The Advisor 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's giving account information to an imposter pretending to represent the firm or to a fraudulent web site.

Check Similar Accounts. The Advisor will review similar accounts under management to see if there have been attempts to access them without authorization.

Collect Incident Information. For a serious threat of unauthorized account access The Advisor may, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," collect if available:

- Firm information (both introducing and clearing firms): Firm name, CRD number, contact name & telephone number
- Dates and times of activity
- Securities involved (name and symbol)
- Details of trades or unexecuted orders
- Details of any wire transfer activity
- Client accounts affected by the activity, including name and account number, and
- Whether the client will be reimbursed and by whom.

Report. If unauthorized account access is found, The Advisor will report it to the Custodian and work in conjunction with the Custodian to report as appropriate to appropriate local and state law enforcement; where organized or wide spread crime is suspected, the FBI or Secret Service; and if mail is involved, the US Postal Inspector. The Advisor may also, as recommended by FINRA's Customer Information Protection web page's "Firm Checklist for Compromised Accounts," report it to their FINRA coordinator; the SEC; State regulatory authorities, such as the state securities commission; and their clearing firm.

Notification. If determined that personal identifiable information has been accessed that results in a foreseeable risk for identity theft, The Advisor will prepare any specific notice to clients or other required under state law.

Review of Insurance Policy. Since insurance policies may require timely notice or prior consent for any settlement, we will review our insurance policy to ensure that their response to a data breach does not limit or eliminate our insurance coverage.

Assist the Client. We will work with our clients to minimize the impact of identity theft by taking the following actions, as applicable:

- Offering to change the password, security codes or other ways to access the threatened account;
- Offering to close the account;
- Offering to reopen the account with a new account number;
- Instructing the client to go to the FTC Identity Theft Web Site 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.

The Advisor follows the procedures of custodial Identity Theft Programs to notify appropriate compliance and operational personnel to implement procedures to prevent and respond to identity theft red flags and circumstances.

Maintaining the ITPP
The Advisor will update the ITPP (including the relevant Red Flags) periodically, to reflect changes in risks to Clients or to the safety and soundness of the Advisor from identity theft, based on factors such as the Advisor's experiences with identity theft, changes in methods of identity theft, and changes in the Advisor's business.

CCO Testing: The CCO or Delegate will determine which identity theft red flags are relevant to the business and ensure there are reasonable controls in place to detect those red flags. The CCO or Delegate will document their response to any red flags detected and incorporate those experiences when considering updates to the way they detect and respond to red flags.

D. Email Use

All email communications must abide by the Client Communications section noted above and must be archived in the Advisor's books and records. Supervised Persons of the Advisor must conduct all business communications via the email account assigned by the Advisor. Using an email domain not approved by the Advisor will not be archived and is strictly prohibited. Unless approved by the CCO or Delegate, Supervised Persons should refrain from using the Advisor's email system for personal use. Should there be a need for personal use of the Advisor's email system, it should be kept to a minimum.

CCO Testing: The CCO or Delegate periodically reviews a sample of email communications to ensure adherence to the Client Communication Policy defined above, identification of any Client complaints, insider trading, and/or failure to adhere to privacy policies. The CCO or Delegate documents the findings within the Advisor's books and records.

E. Mobile Devices

Access to Emails
With approval from the CCO or Delegate, Supervised Persons may access their business email accounts on their personal mobile devices.

Texting
Supervised Persons are not permitted to use text messages on any personal electronic device unless the communication is for administrative purposes only (i.e., confirming address for meeting, relaying location information for a meeting, etc.). All communications with Clients must be done via systems/accounts that can be archived and monitored.

8. Vendor Management

A. Background

As a fiduciary to its Clients, the Advisor manages vendors across the lifecycle of the relationship using a risk-based approach. The Advisor conducts initial and ongoing due diligence and retains documentation of vendors who are: (i) vital to the firm's operations; and (ii) may maintain sensitive Client and firm information. To determine criticality and therefore the required level of due diligence, the Advisor conducts an internal assessment of the service and data to be shared. In light of this information, the Advisor will determine what level of due diligence the firm requires and at what frequency.

The Advisor recognizes that, while processes can be outsourced, responsibility for performing due diligence of vendors and their practices lies with the Advisor. Varying degrees of due diligence are achievable with different vendors, and information is aggregated in line with this policy guideline as feasible.

B. Due Diligence

The Advisor engages new and potential vendors depending upon their risk profile and a determination of whether they meet the criteria of a Critical Vendor. As part of the Advisor's Vendor Management Program, all vendors have some degree of due diligence performed on both an initial and ongoing basis.

Initial Due Diligence

This process begins when the CCO is alerted to a new vendor by the firm personnel. In the event that the CCO determines comprehensive due diligence is required, he or she will send the vendor a formal due diligence request form ("DDQ"). In the event the CCO determines that there is little to no risk to the Advisor and its Clients as a result of its relationship with a vendor due to a lack of transference of data, or of low criticality, he or she may determine that ongoing due diligence is not necessary.

Efforts of due-diligence may include, but are not limited to:

- An in-depth interview with an authorized representative of the Vendor
- A review of the adequacy of the written agreement governing the terms of the outsourcing arrangement which must clearly define material terms and detail corrective and exit strategy or transition provisions
- If the Vendor is a regulated entity, the Advisor will require its reasonably available record of regulatory compliance
- A review of the Vendor's reputation and financial status
- A review of the Vendor's business continuity plan and the ability to resume services in the event of a disaster.
- A review of the effectiveness of the Vendor's privacy and confidentiality controls in regard to the information provided to the Advisor.

Ongoing Due Diligence

Once initial due diligence has been conducted, the Advisor will implement the following steps annually:

- Review criticality and performance. This process involves direct communication with personnel responsible and utilizing vendor services. This process assists the CCO in determining priorities for vendor management activities.
- Review existing Service Level Agreements for terms of privacy, confidentiality, and data management. For vendors who retain firm information, the CCO examines terms of data ownership, transference, destruction, and termination.
- Aggregate updated control reporting, such as SSAE-16 and SOC1 & 2 documentation, as available.
- Review Information Security Policies and Business Continuity Plans, as feasible.
- Verify contact information, representatives, customer support, and business continuity contacts.
- Issue a DDQ for updating or review relevant details depending on the accessibility of the vendor where feasible.
- Consider the appropriate steps for termination and transition.

C. Additional Considerations and Limitations

The Advisor recognizes that business requirements may change as may the ownership and operational methods of vendors. Such changes may trigger an as-needed review of a vendor's capabilities and the procedures mentioned above. The Advisor may also reissue its DDQ or attempt to validate detailed information on an as-needed basis.

The Advisor understands that not every vendor will respond to its DDQ or that a specific vendor may not meet the Advisor's security requirements. In these instances, the CCO will work with the data or process owner to perform a risk/reward analysis with respect to the specific vendor. Such an analysis may include:

- Business Need/Criticality;
- Minimum Standards of Care;
- The difficulty of Sourcing an Alternate Vendor; and
- Breach Risk.

The Advisor will make a reasonable effort to obtain an understanding of the business and its practices and will document its rationale for maintaining a relationship with a non-conforming vendor and will make reasonable efforts to include such a vendor in its ongoing due-diligence process.