Motiv8 Investments LLC

Written Policies and Procedures

Effective Date: August 2023

Table of Contents

Record of Changes

Effective Date	Section	Modification
August 2023	Political Contributions ("Pay to Play Rules")	Added new section

Policy Statement

MOTIV8 INVESTMENTS LLC ("MIL") is a registered investment adviser. This document describes its policies and procedures.

At a minimum, MIL will annually review and update these policies and procedures. MIL may conduct interim reviews in response to significant compliance events, changes in business arrangements, and regulatory developments.

MIL will maintain copies of all policies and procedures that are in effect or were in effect at any time during the last five years.

MIL's goal is to maintain the highest ethical and professional standards for employee conduct. This manual is only a guide and cannot cover employee and/or supervised person's conduct in every conceivable situation that may arise in the course of MIL's business. In the event of any uncertainty, an officer, director, affiliate, supervised person, or employee of the firm should ask a supervisor or the Chief Compliance Officer ("CCO") for advice on compliance with this manual and/or the applicable securities laws.

Definitions of italicized terms, where not otherwise defined, may be found in the Definitions section of this manual (see table of contents under "Code of Ethics").

Throughout this document, the term "CCO" is understood to mean the CCO or designated representative, as the CCO may delegate the performance of certain compliance responsibilities to other individuals at the firm. The CCO has ultimate responsibility for the compliance program of the firm.

Policies in this manual apply to every employee, supervised person, member and officer of MIL. Each of these persons is required to read the contents of this manual and conform to the policies contained therein. MIL's Annual Attestation Acknowledgement Form (see Sample 1) of this manual contains an acknowledgement that MIL members, supervised persons, officers and employees must sign setting forth that they have read and understood the compliance policies and procedures applicable to them.

Fiduciary Statement

An investment adviser has a duty to always act in the best interest of its clients. It should not engage in any activity in conflict with the interest of any client and it should take steps to eliminate all conflicts of interest that might incline it to provide advice that is not impartial. If it cannot eliminate such a conflict, then it must fully disclose the conflict. It should also take care to avoid misleading statements and it should provide full and fair disclosure of all material facts. Generally, facts are "material" if a reasonable investor would consider them to be important in determining to do business with the adviser. The duty of addressing and disclosing conflicts of interest is an ongoing process and as the nature of an adviser's business changes, so may the relationship with its clients.

Firm Statement

As an investment adviser, MIL owes its clients specific duties as a fiduciary:

- Maintain suitability and investment profile information
- Provide advice that is suitable, appropriate, and in the client's best interest;
- Give full disclosure of material facts and any potential or actual conflicts of interest to clients and prospective clients;
- Serve with loyalty and in utmost good faith; and
- Exercise reasonable care to avoid misleading a client

MIL seeks to protect the interest of each client and to consistently place the client's interests first and foremost in all situations. It is the belief of this investment adviser that its policies and procedures are sufficient to prevent and detect any violations of regulatory requirements as well as of the firm's own policies and procedures.

Use of MyRIACompliance™

MIL intends to use MyRIACompliance™ software to assist with certain of its recordkeeping and reporting obligations. Specifically, MIL will utilize the software to track, review and approve attestations, certifications, prior approval requests, and reports; this will take the place of certain sample documents attached to this Policies and Procedures Manual.

Client Accounts

The firm's CCO shall review all new accounts to ensure compliance with applicable laws and MIL policies.

Opening New Accounts

Prior to engaging in investment advisory services offered by MIL, each potential client shall receive at a minimum the following:

- Firm Brochure (Form ADV Part)
- Brochure Supplement (Form ADV Part 2B) for the Investment Adviser Representative(s) ("IAR") who will be servicing the account
- Form CRS Customer Relationship Summary (Form ADV Part 3)
- Privacy Policy

Client Agreements

Prior to providing advisory services to a client, MIL and the client shall complete and execute a contract outlining the services to be provided, the terms of the services as well as an investment policy statement or other document that provides suitability information such as investment objectives, risk tolerance and financial condition of the client. The firm will only use an advisory contract that has been reviewed and approved by the CCO. The firm will not typically accept clients who refuse to provide suitability information, but may make exceptions on a case-by-case basis.

The firm will not open suspicious accounts or accounts for minors unless properly set up through a guardian.

Updating Client Account Information

The firm will periodically, but at a minimum annually, verify and update the information it receives from its clients during client meetings and reviews.

Additionally, the firm's CCO shall conduct quarterly transaction reviews of client account activity and transactions to ensure that transactions:

- Comply with the best execution policies of MIL;
- Comply with the trade allocation and block trading policies of MIL; and
- Reflect the objectives and requests as outlined in the client's investment policy statement.

Recordkeeping Requirements

MIL will keep and maintain client account files and records including signed client agreements.

Terminated Accounts

MIL will maintain client files for terminated accounts for a minimum of five years from the end of the calendar year in which the client terminates the relationship. A list of terminated accounts will also be kept on file (see Sample 2).

Death of a Client

The death of a client can be a challenging circumstance for an investment adviser. During this time, the firm must still adhere to its fiduciary duty and act in the client's best interest. This will involve a review of the investment advisory contract to determine if the contract remains in effect in the event of the client's death. If the firm has been granted discretionary authority, and the contract does not terminate upon client death, then the adviser will continue to manage the assets in fulfilling its fiduciary obligation to the client until instructed otherwise by the executor of the client's estate.

Once the firm has received notification of the client's death, it should:

- Notify the custodian and any other applicable third parties.
- Obtain a copy of the client's death certificate.
- Identify the executor and obtain copies of documents to evidence the executor's authority.
- Determine any other authorized representatives for communication (e.g., attorneys, CPAs, etc.).
- If instructed by the executor, re-paper and transfer accounts to the new owners.
- Document all communication with the executor and any other authorizes representative of the estate.

Additionally, if instructed by the executor, the firm should work with the custodian to provide any additional documentation required by the custodian to liquidate and/or transfer assets, which may include the following:

- Court Letter of Appointment, which names the executor (current in its date and with a visible or original court seal).
- A type of power of attorney called "stock power," which allows for the transfer of ownership of stock.
- State tax inheritance waiver, if applicable.
- Affidavit of domicile.
- For accounts held in trust, the trustee certification showing successor trustee.
- For joint accounts, a Letter of Authorization signed by the survivor if the assets are moving anywhere other than his or her own account. Alternatively, if there is no surviving tenant and the assets are moving anywhere other than the last decedent's estate account, the firm will require a Letter of Authorization signed by the executor.

All documents obtained to complete the liquidation and/or transfer process will be maintained as a part of MIL's books and records.

Outside Business Activities

Supervised persons shall not engage in any outside business activity without prior firm approval.

Definition

An outside business activity (OBA) is any employment or compensation from any other person or entity as a result of a business activity, other than a passive investment, outside the scope of a supervised person's relationship to MIL.

Review and Approval by the CCO

Supervised persons of MIL are required to report outside business activities to the CCO for review and approval prior to engaging in these activities (see Sample 3). The CCO will review these activities to determine if they create a conflict of interest with the supervised persons' ability to act in the best interest of the firm's customers. If it is determined that a conflict does exist, the CCO will determine if the conflict can be appropriately mitigated by disclosure or other means.

The supervised person shall provide at least the following information to the CCO regarding the activity:

- Name, address, contact information for the person or entity paying the compensation;
- Complete description of the activity;
- Amount of compensation or formula; and
- Duration of the activity.

Disclosure on Appropriate Documents

Individual Form U4s and Form ADV Part 2Bs will be updated as needed for outside business activities. It is the responsibility of the individual supervised person and the CCO to make sure these documents are updated promptly in the event disclosure is required.

Certain outside business activities of supervised persons may require firm documents to be updated as well. If updates are required for Form ADV Part 1A, Part 1B, Part 2A, and / or Part 3, then the CCO will be responsible for updating these documents when needed.

Record Keeping Requirements

CCO will keep and maintain records of all OBA requests and any relevant supporting documentation that helped in the decision to approve or deny the OBA.

Marketing

Advertising Under SEC Rule 206(4) – 1

History

The SEC has adopted an amended rule, Rule 206(4)-1, under the Advisers Act, which addresses investment advisers marketing their services to clients and investors ("Marketing Rule"). This Marketing Rule amends the existing Rule 206(4)-1 ("Advertising Rule") and also replaces Rule 206(4)-3 ("Solicitation Rule").

Firm Policy

The firm's CCO shall be responsible for reviewing and approving company marketing and ensuring it is in compliance with jurisdictional regulations. No advertisement shall be distributed without the CCO's prior approval.

Definition

The definition "advertising" under the Marketing Rule has two prongs. The first prong is designed to capture traditional advertising, while the second prong addresses compensated testimonials and endorsements.

(1) The definition of advertisement includes any **direct or indirect communication** an investment adviser makes that:

> (a) offers the investment adviser's investment advisory services with regard to securities to prospective clients (retail and institutional) or investors in a private fund advised by the investment adviser ("private fund investors"), or
>
> (b) offers new investment advisory services with regard to securities to current clients or private fund investors.
>
> Notably, the definition does not include the following:
>
> (a) one-on-one communications, unless the communication includes hypothetical performance information that is not provided: (i) in response to an unsolicited investor request or (ii) to a private fund investor
>
> (b) extemporaneous, live, oral communications
>
> (c) information contained in a statutory or regulatory notices and filings (or other similarly required communication), provided that such information is reasonably designed to satisfy the requirements of such notice or filing

(2) The definition of advertisement includes any **compensated testimonials and endorsements**. (This includes a similar scope of activity as traditional solicitations under the current solicitation rule.) This second prong includes oral communications and one-on-one communications to capture traditional one-on-one solicitation activity, in addition to solicitations for non-cash compensation. It will exclude certain information contained in a statutory or regulatory notice, filing, or other required communication.

General Prohibitions and Compliance Requirements:

An advertisement is not permitted to:

1. Include any untrue statement of a material fact, or omit to state a material fact necessary in order to make the statement made, in the light of the circumstances under which it was made, not misleading
2. Include a material statement of fact that the adviser does not have a reasonable basis for believing it will be able to substantiate upon demand by the SEC
3. Include information that would reasonably be likely to cause an untrue or misleading implication or inference to be drawn concerning a material fact relating to the investment adviser
4. Discuss any potential benefits to clients or investors connected with or resulting from the investment adviser's services or methods of operation without providing fair and balanced treatment of any material risks or material limitations associated with the potential benefits
5. Include a reference to specific investment advice provided by the investment adviser where such investment advice is not presented in a manner that is fair and balanced
6. Include or exclude performance results, or present performance time periods, in a manner that is not fair and balanced; or
7. Otherwise be materially misleading.

Accordingly, MIL will ensure that any advertisements comply with the foregoing.

Promoters/Solicitors Offering Testimonials and/or Endorsements

History

As noted above, the Advertising Rule historically did not incorporate solicitor activity as advertising, whereas the current Marketing Rule integrates traditional solicitor activity making promoters/solicitors subject to Rule 206(4)-1. The current Marketing Rule 206(4)-1 contains the following notable changes:

- Expand the Marketing Rule to cover promoter/solicitor arrangements involving all forms of compensation, rather than only cash compensation
- Include exceptions for de minimis payments and certain non-profits programs
- Eliminate requirements to deliver the investment adviser's ADV Part 2A
- Expand the Marketing Rule to apply to solicitation of "investors" in any private fund,

rather than only to "clients" of the investment adviser
- Expand the types of disciplinary events that would trigger disqualification provisions

Definitions

A "testimonial" is defined as "any statement by a current client or investor in a private fund advised by the investment adviser: (i) About the client or investor's experience with the investment adviser or its supervised persons; (ii) That directly or indirectly solicits any current or prospective client or investor to be a client of, or an investor in a private fund advised by, the investment adviser; or (iii) That refers any current or prospective client or investor to be a client of, or an investor in a private fund advised by, the investment adviser."

An "endorsement" is defined as "any statement by a person other than a current client or investor in a private fund advised by the investment adviser that: (i) Indicates approval, support, or recommendation of the investment adviser or its supervised persons or describes that person's experience with the investment adviser or its supervised persons; (ii) Directly or indirectly solicits any current or prospective client or investor to be a client of, or an investor in a private fund advised by, the investment adviser; or (iii) Refers any current or prospective client or investor to be a client of, or an investor in a private fund advised by, the investment adviser."

General Prohibitions and Compliance Requirements:

An advertisement may not include any testimonial or endorsement, and MIL may not provide compensation, directly or indirectly, to a promoter/solicitor for a testimonial or endorsement, unless MIL complies with the following conditions:

- MIL will create proper, clear, and detailed disclosure including the following:
  - Clear and prominent disclosure that the testimonial was given by a current client or private fund investor, and the endorsement was given by a person other than a current client or private fund investor, as applicable
  - Clear and prominent disclosure that cash or non-cash compensation was provided for the testimonial or endorsement, as applicable
  - Clear and prominent statement of any material conflicts of interest on the part of the person giving the testimonial or endorsement resulting from MIL's relationship with such person
  - Disclosure of the material terms of any compensation arrangement, including a description of the compensation provided or to be provided, directly or indirectly, to the person for the testimonial or endorsement
  - A description of any material conflicts of interest on the part of the person giving the testimonial or endorsement resulting from MIL's relationship with such person and/or any compensation arrangement
- *MIL will create an agreement between MIL and the promoter providing the testimonial or endorsement detailing term, payments, and marketing activities

- *MIL will conduct due diligence to make sure the promoter is not disqualified
- MIL will ensure ADV filings reflect the use of solicitors; and
- MIL will provide oversight and compliance consisting of the following:
    - MIL will conduct initial and no less than annual due diligence on promoters
    - MIL will provide the promoter/solicitor with the required disclosures to present to potential clients or investors
        - The required disclosures can be disseminated either orally, or in writing, as agreed upon within the promoter agreement
    - MIL must have a reasonable belief that the promoter/solicitor is providing the required disclosures to the potential client or investor at the time of the solicitation
    - MIL will typically rely on asking potential clients if they received such disclosures, but may utilize other means
    - MIL will annually review the content of the disclosures being provided to new clients or investors.

** If there are no benefits or the benefits have a value of less than a $1,000 de minimis value, then the written agreement and disqualification conditions do not apply.*

For the sake of clarity, the foregoing restrictions will apply to all compensated "refer-a-friend" type programs, under which clients can "refer" their friends in exchange for some type of benefit (i.e., cash, gift cards, discounts on advisory fees, or other benefits with a financial value).

MIL further recognizes that promoters/solicitors must comply with the provisions of not only the current Marketing Rule but also, but any state laws or FINRA rules, which may require certain registration(s) for promoters/solicitors.

Finally, MIL will maintain records of any testimonials, endorsements, and promoters/solicitors (past and present) as part of its ongoing books and records requirements.

Third Party Ratings

The use of a third party rating in advertising is allowable, but only if the advertisement complies with the Marketing Rule's general prohibitions and additional conditions.

Overview

A third party may rank or rate an investment adviser provided that the person (i) is not a related person and (ii) provides such ratings or rankings in the ordinary course of its business. (The "ordinary course of business" requirement would largely correspond to persons with the experience to develop and promote ratings based on relevant criteria.)

The use of a third party rating/ranking also requires the following conditions:

1) **Due diligence requirement:** MIL must have a reasonable basis to believe that any questionnaire or survey used in the preparation of the third-party rating is structured to

make it equally easy for a participant to provide favorable and unfavorable responses, and is not designed or prepared to produce any predetermined result.
2) **Disclosure requirement:** MIL must clearly and prominently disclose (or have a reasonable belief that the third-party rating clearly and prominently discloses): (i) the date on which the rating was given and the period of time upon which the rating was based; (ii) the identity of the third-party that created and tabulated the rating; and (iii) if applicable, that compensation has been provided directly or indirectly by the adviser in connection with obtaining or using the third-party rating.

Moreover, at no time can a rating be false or misleading under the general prohibitions or under the general anti-fraud provisions of the securities laws.

Due Diligence Requirement

Accordingly, if utilizing third-party ratings/rankings, MIL will access the questionnaire or survey that was used in preparation of the rating/ranking and ensure it understands the underlying methodology and structure of the third party's process of determination;

Disclosure Requirement

In order to meet the clear and prominent disclosure requirement, MIL will ensure that the disclosure is at least as prominent as the third-party rating and includes the following:

- The date on which the rating was given;
- The period of time upon which the rating was based;
- The identity of the third party that created and tabulated the rating; and
- If applicable, the compensation provided, whether direct or indirect, cash or non-cash, by MIL in connection with obtaining the third party rating.

Performance Advertising

Overview

According to the Marketing Rule, the following types of performance advertising are generally prohibited (with certain exemptions) and thus MIL will not utilize the following:

1. **Gross performance**, unless the advertisement presents net performance as well, with equal prominence to and in the format designed to facilitate comparison with the gross performance
2. **Any performance** results, unless they are provided for specific time periods in most circumstances
3. **Statements of approval** indicating that the SEC approved or reviewed any calculation or presentation of performance results

4. **Performance results from fewer than all portfolios** with substantially similar investment policies, objectives, and strategies as those being offered in the advertisement, with limited exceptions
5. **Performance results of a subset of investments** extracted from a portfolio, unless the advertisement provides, or offers to provide promptly, the performance results of the total portfolio
6. **Hypothetical performance** (which does not include performance generated by interactive analysis tools), unless MIL (i) adopts and implements policies and procedures reasonably designed to ensure that the performance is relevant to the likely financial situation and investment objectives of the intended audience and (ii) provides certain information underlying the hypothetical performance
7. **Predecessor performance**, unless there is appropriate similarity with regard to the personnel and accounts at the predecessor adviser and the personnel and accounts at MIL.
In addition, MIL will include all relevant disclosures clearly and prominently in the advertisement.

Firm Policy

Firm policy dictates that if and when MIL decides to use performance advertising, extreme care and caution will be taken.

Performance advertising encompasses several styles of presentations: past specific performance of individual securities, performance of one or more model accounts managed by the firm, performance of actual client accounts managed by the firm, performance of a composite of actual client accounts, and back tested models generated by research of the adviser.

It is beyond the scope of this Policies and Procedures Manual to detail all of the complex compliance issues associated with each style of performance advertising. Final approval rests with the CCO although he or she may be assisted by outside resources as needed or requested.

Regulators will apply a "facts and circumstances" standard in the review of each style of previously mentioned performance advertising. MIL will follow the rules, statutes, guidance and any applicable "No Action" letters that apply to each style of performance advertising.

Performance advertising requires special and specific disclosure to ensure the viewer is not misled concerning the content of the advertisement. Certain examples of disclosure required for different types of performance advertising are summarized below.

Past specific advertising

- Presented in a fair and balanced manner;
- Disclosures with appropriate contextual information for investors to evaluate recommendations;
- Presentation of performance figures "net" of management fees and transaction charges, if applicable; and
- Disclosure that past performance is not indicative of future performance.

Performance reporting of models, actual client accounts, or composites of actual client accounts

- Disclosure of the effect of material (significant) market or economic conditions on the results portrayed;
- Disclosure of the deduction of investment advisory fees so the results presented are "net of fees" (management and transaction fees);
- Disclosure of whether and to what extent the results portrayed reflect the reinvestment of dividends and other earnings;
- Disclosure of the possibility of loss along with any discussion of the possibility for gain;
- If the results are compared to an index, disclosure of all material factors relevant to the comparison (e.g., an advertisement that compares model results to an index without disclosing that the volatility of the index is materially different from that of the model portfolio);
- Disclosure of any material conditions, objectives, or investment strategies used to obtain the performance advertised;
- Disclosure of the limitations inherent in model results;
- Disclosure, if applicable, of material changes in the conditions, objectives, or investment strategies of the model portfolio during the period portrayed and the effect of those changes;
- Disclosure, if applicable, that some of the securities or strategies reflected in the model portfolio do not relate, or relate only partially, to the services currently offered by the investment adviser; and
- Disclosure, if applicable, that the investment adviser's clients actually had investment results that were materially different from those portrayed in the model.

Back tested models

- Disclosure that the performance obtained through hypothetical or back-tested strategies does not result from actual trading and there is no market risk involved in the results;

- Disclosure that the "results" are hypothetical and often created with the benefit of hindsight and that it may be difficult, if not impossible, to account for all of the factors that might have affected a manager's decision making process;
- Disclosure that hypothetical or back-tested performance often involves certain material assumptions in applying investment decisions that might have been made, based on the investment theory espoused, during the relevant historical period and the data set chosen may not be indicative of present or future market conditions;
- Disclosure that there are often sharp differences between hypothetical performance results and actual returns subsequently achieved. Due to the benefit of hindsight, hypothetical performance almost invariably will show attractive returns, while actual results going forward may not be as attractive;
- Disclosure that past results are not indicative of future performance; and
- Disclosure that results are net of management and transaction fees.

Predecessor Performance Requirements

- The person or persons who are primarily responsible for achieving the prior performance results manage accounts at MIL,
- The accounts managed at the predecessor adviser are sufficiently similar to the accounts managed at MIL that the performance results would provide relevant information to clients and investors,
- All accounts that were managed in a substantially similar manner are advertised unless the exclusion of any such account would not result in materially higher performance and the exclusion of any account does not alter the presentation of any applicable time periods required by the Marketing Rule, and
- The advertisement includes, clearly and prominently, all relevant disclosures, including that the performance results were from accounts managed at another entity.

Social Media

Social networks connect people via online communities such as Facebook, LinkedIn, Twitter, and others. As with other technology, social networks have proper and improper uses. This policy is designed to help firm employees who use social networking understand what is recommended and required of them.

Use for Business Purposes

MIL permits the usage of social media websites by its supervised persons for business purposes on the following outlets: Facebook, Twitter, LinkedIn, Friendster and YouTube

MIL has adopted the following policies and procedures concerning this usage for business purposes:

- Social media site usage is considered correspondence and/or advertising by MIL;
- Supervised persons are required to notify the CCO of their intention to utilize social media sites prior to usage;
- Usage and posting to these sites must be monitored and approved by the firm's CCO; and
- MIL's books and records policies on correspondence and advertising require that, as correspondence and/or advertising, social media usage and posts must be retained and archived.

Use for Personal Purposes

Supervised persons of MIL using social media for personal purposes should follow the following procedures:

- Notify the CCO of the social media outlets being used;
- Follow MIL's guidelines for personal use of Social Media in reference to any mention of MIL:
  - Limit any reference to MIL to title, location, contact information, and/or years of service;
  - Do not hold themselves out as representing MIL views in any way;
  - Do not post or otherwise comment regarding MIL business, clients, employees, policies or any other potentially confidential information;
  - Do not "chat" or otherwise communicate with clients or potential clients regarding any actual or potential investment advice; and
  - Prepare any posts or communications with care and professionalism and ensure they are appropriate in tone and content.

In addition, staff members should never disclose personal information on any social media website that could allow a third party to gain access to MIL's systems and passwords used for work equipment should not be drawn from any publicly posted information.

Use of Third Party Content

All MIL employees must consider communications that are "direct" and "indirect" and the concept of "adoption" and "entanglement." An example would be if an employee's use of social media includes a hyperlink to third party content, then this would be attributed to the employee and would therefore be considered advertisement.

MIL employees must abide by the guidelines when considering the use of a hyperlink from a third party since the content of the link will be attributed to the employee. If the employee has reason to believe that the content provided by a third party is an untrue statement of material fact or materially misleading information or otherwise violates the Marketing Rule, then it cannot be used.

MIL typically allows for third party comments on employees' social media (e.g., "like," "share," "endorse," etc.) and such comments will not be attributed to the employee so long as the following is adhered to:

- MIL cannot prepare the comments for the third party
- MIL cannot sort the comments
- MIL cannot selectively delete or alter the comments or their presentation

This policy applies to all social networking sites currently in use, as well as any future such sites that may develop during the existence of MIL. This policy also covers any other chat rooms, blogs, video sites (e.g., YouTube) or online bulletin boards in which MIL employees may be involved.

Ongoing Monitoring

MIL will periodically monitor the internet, and specifically social networking sites, for references to the firm by employees. Any violations of this policy will be handled accordingly.

This policy will continue to evolve as new technologies and tools become available and as regulatory requirements change. Where no policy or guidance exists, or if uncertain, MIL employees should consult with their supervisor in order to avoid any potential violation.

Written Correspondence

Correspondence

MIL is involved in communicating with its clients in various formats: written letters, email, fax, phone, firm website, Twitter, blog and client portal.

In all cases, these communications will either be classified as advertising or correspondence and will follow the appropriate rules and regulations.

Correspondence generally refers to both incoming and outgoing written communications between the firm and one client or potential client. Communications to more than one individual are typically defined as advertising and are subject to the advertising rules and regulations. Correspondence includes both hard copy forms as well as electronic (e.g., email, text message, instant message, and facsimile).

It is the firm's policy that communications with the public be truthful, not misleading, and not contain any exaggerated or unwarranted statements. Everything is to be presented in a fair and balanced manner.

Some of the additional steps to be taken include:

- The CCO will review client correspondence for complaints and respond to them promptly as they are made by clients;
- The CCO will take the necessary steps to ensure incoming and outgoing correspondence is archived;
- The CCO will randomly spot check written correspondence to verify the communications are not misleading, fraudulent, exaggerated and do not violate applicable rules and regulations in any way (see Sample 4 and Sample 5);
- The CCO will verify that the firm is maintaining copies of all correspondence in accordance with applicable rules and regulations;
- The CCO will approve methods of delivery prior to use;
- Items marked "internal use only" will not be disseminated outside of firm personnel;
- Use of third party prepared material will only be used with the approval of the CCO; and
- Any incoming correspondence that could possibly be deemed a complaint will be immediately forwarded to the CCO.

Electronic Communications

It is firm policy that only approved methods of electronic communication will be used with clients. Firm personnel should consult with the CCO if there is any question on what methods are available to be used.

It is important to note, electronic communications with clients are subject to retention and periodic review by the CCO at any time.

If electronic communications are used to comply with the annual delivery of MIL's ADV filing and/or Privacy Policy requirement, MIL will either attach these documents to an email communication or will inform its clients in an email with an embedded hyperlink to MIL's website, where the most current ADV filing and Privacy Policy can be viewed. Prior to distributing materials in this manner, MIL will obtain prior authorization from its clients. MIL will use an electronic authorization form or will obtain electronic authorization via its investment advisory contract. MIL will retain this authorization as part of its required books and records.

Anti-Money Laundering (AML) Policy

It is the policy of the firm to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities.

Anti-Money Laundering Program

The CCO shall:

- Monitor the firm's compliance with this policy;
- Monitor changes in applicable laws and regulations relating to money laundering and implement further controls as may be required by such changes in laws and regulations;
- Ensure the firm keeps the records required by this policy;
- Ensure Suspicious Activity Reports (SAR-SFs) are filed when required by applicable law and regulations; and
- Train employees of the firm to ensure compliance with this policy.

Ongoing Transaction Review

The CCO will also review transactions by investors and determine whether to engage legal counsel if a particular investor engages in an abnormal series of transactions, such as (but not limited to):

- excessive frequency of contributions and redemptions;
- transactions in cash or money orders;
- transactions with foreign shell banks, banks with P.O. Boxes or banks located in jurisdictions without anti-money laundering laws;
- transactions in which subscription monies are received from a non-subscribing third party;
- transactions by or for the benefit of senior political figures, their immediate family members and close associates;
- reluctance to answer compliance-related questions about ultimate beneficial ownership; and
- distribution of redemption proceeds to an account other than the original wiring account used by the investor.

Client Identification and Verification

Prior to establishing a new client relationship, the firm will obtain and review the following information to verify the identity of the client:

- The client's legal name;
- The client's date of birth (if the client is an individual);
- The client's physical address (not a P.O. Box or email address);

- The client's telephone number;
- The client's government identification number (e.g., tax identification number, social security number, or passport number with country of issuance);
- A short description of the client's primary business, if any; and
- A short description of the client's primary source of funds (e.g., business listed above, inheritance, pension).

Clients Who Refuse to Provide Information

If a potential or existing client either refuses to provide the information described above or appears to have intentionally provided misleading information, MIL will not open a new account and, after considering the risks involved, consider closing any existing account. In either case, MIL's CCO will be notified so that MIL can determine whether it should file a Form SAR-SF.

Verifying Information

MIL will ensure that it has a reasonable belief that it knows the true identity of its clients by using risk-based procedures to verify and document the accuracy of the information it receives about its clients. In verifying client identity, MIL will analyze any logical inconsistencies in the information it obtains.

MIL will verify its client's identity through documentary evidence or non-documentary evidence, as necessary. In analyzing the verification information, MIL will consider whether there is a logical consistency among the identifying information provided, such as the client's name, street address, zip code, telephone number (if provided), date of birth, and social security number.

If MIL detects any red flags that indicate possible money laundering or terrorist financing activity, it will, after internal consultation with the firm's CCO, file a SAR-SF in accordance with applicable law and regulation.

Lack of Verification

When MIL cannot form a reasonable belief that it knows the true identity of a client, it will do the following: (1) not open an account; (2) impose terms under which a client may conduct transactions while it attempts to verify the client's identity; (3) close an account after attempts to verify client's identity fail; or (4) file a SAR-SF if required by applicable law and regulation.

Recordkeeping

MIL will document its verification, including identifying information provided by a client, the methods used and results of verification, and the resolution of any discrepancy in the identifying information. MIL will keep records containing a description of any document that it relied on to verify a client's identity, noting the type of document, any identification number

contained in the document, the place of issuance, and if any, the date of issuance and expiration date. With respect to non-documentary verification, MIL will retain documents that describe the methods and the results of any measures it took to verify the identity of a client. MIL will maintain records of identification information for five years after the account has been closed; it will retain records made about verification of the client's identity for five years after the record is made.

Responding to Red Flags

When a member of the firm detects a red flag with respect to a client account, he or she will investigate further under the direction of the CCO. This may include gathering additional information internally or from third-party sources, contacting the government or filing a Form SAR-SF.

Money laundering "red flags" include:

- The client exhibits unusual concern about the firm's compliance with government reporting requirements and the firm's AML policies (particularly concerning his or her identity, type of business and assets), or is reluctant or refuses to reveal any information concerning business activities, or furnishes unusual or suspicious identification or business documents;
- The client wishes to engage in transactions that lack business sense or apparent investment strategy, or are inconsistent with the client's stated business or investment strategy;
- The information provided by the client that identifies a legitimate source for funds is false, misleading, or substantially incorrect;
- Upon request, the client refuses to identify or fails to indicate any legitimate source for his or her funds and other assets;
- The client has a questionable background or is the subject of news reports indicating possible criminal, civil, or regulatory violations;
- The client exhibits a lack of concern regarding risks, commissions, or other transaction costs;
- The client appears to be acting as an agent for an undisclosed principal, but declines or is reluctant, without legitimate commercial reasons, to provide information or is otherwise evasive regarding that person or entity;
- The client has difficulty describing the nature of his or her business or lacks general knowledge of his or her industry;
- The client attempts to make frequent or large deposits of currency, insists on dealing only in cash, or asks for exemptions from the firm's policies relating to the deposit of cash;
- The client engages in transactions involving cash or cash equivalents or other monetary instruments that appear to be structured to avoid the $10,000 government reporting requirements, especially if the cash or monetary instruments are in an amount just below reporting or recording thresholds;
- For no apparent reason, the client has multiple accounts under a single name or multiple names, with a large number of inter-account or third-party transfers;

- The client's account has unexplained or sudden extensive wire activity, especially in accounts that had little or no previous activity;
- The client's account shows numerous currency or cashier's check transactions aggregating to significant sums;
- The client's account has a large number of wire transfers to unrelated third parties inconsistent with the client's legitimate business purpose;
- The client's account indicates large or frequent wire transfers, immediately withdrawn by check or debit card without any apparent business purpose;
- The client makes a funds deposit followed by an immediate request that the money be wired out or transferred to a third party, or to another firm, without any apparent business purpose;
- The client makes a funds deposit for the purpose of purchasing a long-term investment followed shortly thereafter by a request to liquidate the position and transfer of the proceeds out of the account;
- The client requests that a transaction be processed to avoid the firm's normal documentation requirements;
- The client, for no apparent reason or in conjunction with other red flags, engages in transactions involving certain types of securities, such as penny stocks, Regulation S stocks, and bearer bonds, which although legitimate, have been used in connection with fraudulent schemes and money laundering activity (such transactions may warrant further due diligence to ensure the legitimacy of the client's activity);
- The client's account shows an unexplained high level of account activity with very low levels of securities transactions;
- The client maintains multiple accounts, or maintains accounts in the names of family members or corporate entities, for no apparent purpose; or
- The client's account has inflows of funds or other assets well beyond the known income or resources of the client.

Responsibility for AML Records and SAR Filing

MIL's CCO will be responsible for ensuring that AML records are maintained properly and that SARs are filed as required. MIL will maintain AML records and their accompanying documentation for at least five years. MIL will keep other documents according to existing Bank Secrecy Act and other record keeping requirements.

Training Programs

The CCO will develop and conduct ongoing employee training. MIL's training will occur on at least an annual basis or when material changes occur to the AML policy and procedures. MIL will maintain records to show the persons trained, the dates of training, and the subject matter of their training.

Portfolio Management Processes

Allocation of Investment Opportunities among Clients

It is MIL's policy, to the extent practical, to allocate investment opportunities to clients over a period of time on a fair and equitable basis relative to other clients. MIL's CCO reviews client accounts quarterly for equitable treatment and reviews its allocation practices annually.

Consistency of Portfolios with Client Investment Objective

MIL provides account management on a continuous basis. Subject to a grant of discretionary authority, MIL, through its IARs or any recommended subadvisers, shall invest and reinvest the securities, cash or other property held in the client's account in accordance with the client's investment objectives, including tax planning strategies if/as applicable, as identified by the client during initial interviews and information gathering sessions. Such suitability information is reviewed and updated by the CCO at least annually.

Mutual Fund Share Class Selection

When recommending the purchase of mutual funds to clients, MIL's policy is to recommend that clients purchase the least expensive mutual fund share class available and to disclose material conflicts of interest including the receipt of compensation for recommending mutual funds.

MIL will assess what mutual fund share classes are available to its clients to determine the least expensive share class taking into consideration the client's needs and anticipated activity in the account. Anytime MIL recommends a higher cost share class to a client, particularly if the higher cost share class pays 12b-1 fees, the firm will disclose to the client the availability of the lower cost share class and will document the basis for the recommendation in the client file.

Periodically, MIL will assess whether previously recommended share classes continue to be the least expensive. This assessment shall take into account whether new share class options are available, whether a client now meets any minimum investment thresholds for a lower cost share class, and whether a client's situation has changed since the previous mutual fund investment. If the previously recommended share class is no longer the least expensive, MIL will determine whether it is in the best interest of its clients to convert clients to the lower cost share class. MIL will also evaluate all mutual funds share classes held in its client accounts, whether recommended by the firm or not, to determine if clients are invested in the lowest cost share class available given each client's time horizon, preferences, and investment objectives.

MIL will document its initial and on-going evaluation of its mutual fund share class selection process. Additionally, MIL will communicate and train its investment advisory representatives

on its initial and periodic mutual fund share class evaluation processes. The CCO will periodically review client records to ensure MIL and its investment advisory representatives are properly following the firm's mutual fund share class selection policy.

MIL will disclose in its ADV Part 2 whether the firm or its supervised persons receive asset-based sales charges or service fees (i.e., 12b-1 fees) from the sale of mutual funds. This disclosure will explain the conflict of interest this compensation creates, how MIL addresses the conflict, and how the firm will disclose conflicts to clients when they arise.

Account Statements

The custodian or other qualified third party holding the client's funds and securities will send the client a confirmation of every securities transaction and a custodial statement at least quarterly. MIL also provides periodic statements to clients which state account holdings and value of portfolio holdings.

Additional information related to MIL's portfolio management and trading procedures is detailed in the executed agreement for services located in the specific client file, and in MIL's Form ADV 2A.

Subadviser/Money Manager Review

MIL utilizes or recommends the services of subadvisers or money managers for account/portfolio management services. Prior to referring clients to any such entity, MIL will conduct a due diligence review of the adviser or money manager. The review may consist of a presentation by the subadviser to MIL, additional gathering of material regarding the subadviser or money manager, including its Form ADV, registration status of firm, etc. Once all information has been collected, MIL will review the materials and determine if the subadviser or manager should be utilized for account management services. Records of the review and final decision will be maintained in MIL's compliance files.

Department of Labor Prohibited Transaction Exemption 2020-02

Rule Background

On February 16, 2021, a new U.S. Department of Labor ("DOL") "Prohibited Transaction Exemption" rule commonly referred to as the "Improving Investment Advice for Workers and Retirees" exemption went into effect. The DOL describes this new exemption as follows:

> *Title I of the Employee Retirement Income Security Act of 1974, as amended (the Act) codified a prohibited transaction provision in title 29 of the U.S. Code (referred to in this document as Title I). Title II of the Act codified a parallel provision now found in the Internal Revenue Code of 1986, as amended (the Code). These prohibited transaction provisions of Title I and the Code generally prohibit fiduciaries with respect to "plans," including workplace retirement plans (Plans) and individual retirement accounts and annuities (IRAs), from engaging in self-dealing and receiving compensation from third parties in connection with transactions involving the Plans and IRAs. The provisions also prohibit purchasing and selling investments with the Plans and IRAs when the fiduciaries are acting on behalf of their own accounts (principal transactions). This exemption allows investment advice fiduciaries to plans under both Title I and the Code to receive compensation, including as a result of advice to roll over assets from a Plan to an IRA, and to engage in principal transactions, that would otherwise violate the prohibited transaction provisions of Title I and the Code. The exemption applies to Securities and Exchange Commission- and state-registered investment advisers, broker-dealers, banks, insurance companies, and their employees, agents, and representatives that are investment advice fiduciaries. The exemption includes protective conditions designed to safeguard the interests of Plans, participants and beneficiaries, and IRA owners. The class exemption affects participants and beneficiaries of Plans, IRA owners, and fiduciaries with respect to such Plans and IRAs. This notice also sets forth the DOL's final interpretation of when advice to roll over Plan assets to an IRA will be considered fiduciary investment advice under Title I and the Code.*

Of particular note, this new rule exemption generally applies to non-discretionary investment advisers per ERISA section 3(21)(A)(ii). Such investment advisory firms are considered to be a Financial Institution when providing investment recommendations related to an IRA rollover from a qualified retirement plan, an IRA rollover from another IRA, a switch from a commission-based to a fee-based IRA, or other similar scenarios.

The exemption's definition of a *Financial Institution* includes an entity such as MIL that is:

> *Registered as an investment adviser under the Investment Advisers Act of 1940 (15 U.S.C. 80b-1 et seq.) or under the laws of the state in which the adviser maintains its principal office and place of business.*

Impartial Conduct Standards

MIL will adhere to the Impartial Conduct Standards which are:

- Give advice that is in the Retirement Investor's Best Interest;
- Charge no more than reasonable compensation and seek to obtain best execution; and

- Make no materially misleading statements about the recommended transaction and other relevant matters

In regard to *Best Interest* advice, the exemption notes the following:

Advice is in a Retirement Investor's "Best Interest" if such advice reflects the care, skill, prudence, and diligence under the circumstances then prevailing that a prudent person acting in a like capacity and familiar with such matters would use in the conduct of an enterprise of a like character and with like aims, based on the investment objectives, risk tolerance, financial circumstances, and needs of the Retirement Investor, and does not place the financial or other interests of the Investment Professional, Financial Institution or any Affiliate, Related Entity, or other party ahead of the interests of the Retirement Investor, or subordinate the Retirement Investor's interests to their own.

Furthermore, the exemption defines a number of key terms referenced above regarding *Best Interest* advice.

The definition of a *Retirement Investor* includes:

The beneficial owner of an IRA acting on behalf of the IRA or a fiduciary of… an IRA.

The definition of an *Investment Professional* means an individual who:

(1) Is a fiduciary of… an IRA by reason of the provision of investment advice described in ERISA section 3(21)(A)(ii) or Code section 4975(e)(3)(B), or both, and the applicable regulations, with respect to the assets of the… IRA involved in the recommended transaction;

(2) Is an employee, independent contractor, agent, or representative of a Financial Institution; and

(3) Satisfies the federal and state regulatory and licensing requirements of insurance, banking, and securities laws (including self-regulatory organizations) with respect to the covered transaction, as applicable, and is not disqualified or barred from making investment recommendations by any insurance, banking, or securities law or regulatory authority (including any self-regulatory organization).

The definition of an *Affiliate* means:

(1) Any person directly or indirectly through one or more intermediaries, controlling, controlled by, or under common control with the Investment Professional or Financial Institution. (For this purpose, "control" would mean the power to exercise a controlling influence over the management or policies of a person other than an individual);

(2) Any officer, director, partner, employee, or relative (as defined in ERISA section 3(15)), of the Investment Professional or Financial Institution; and

(3) Any corporation or partnership of which the Investment Professional or Financial Institution is an officer, director, or partner.

The definition of a *Related Entity* is:

Any party that is not an Affiliate, but in which the Investment Professional or Financial Institution has an interest that may affect the exercise of its best judgment as a fiduciary.

Disclosure

The following disclosures are required to be provided to the Retirement Investor recipient of a rollover recommendation prior to engaging in any transaction:

- A written acknowledgment that MIL and its investment professionals are fiduciaries under Title I of ERISA and the Code, as applicable, with respect to any fiduciary investment advice provided by MIL and its investment professionals to the Retirement Investor.
    - MIL will typically satisfy this requirement through delivery of its Form ADV Part 2A or a separate written disclosure (see Sample 12).
- A written description of the services to be provided by MIL and its material conflicts of interest.
    - MIL will typically satisfy this requirement through delivery of its Form ADV Part 2A and advisory agreement.
- Documentation of the specific reasons that any recommendation for an applicable roll over is in the Retirement Investor's best interest.
    - MIL will typically satisfy this requirement via an IRA investment recommendation checklist.

Once disclosure has been provided, MIL will not be obligated to provide it again, except at the Retirement Investor's request or if the information has materially changed.

IRA Investment Recommendation Checklist

MIL will only make an investment recommendation to a prospect or client related to an IRA rollover from qualified retirement plan, an IRA rollover from another IRA, or a switch from a commission-based to a fee-based IRA account if the recommendation is in the Best Interest of the Retirement Investor.

Accordingly, MIL has implemented a checklist to be completed for all such relevant investment recommendation scenarios. The purpose of the checklist is to document whether the investment advice provided is in the Best Interest of the Retirement Investor and meets the Impartial Conduct Standards.

Level Fees

MIL intends to only charge a *Level Fee* with respect to any such relevant investment recommendation scenarios as described above. A *Level Fee* is a fee or compensation that is provided based on a fixed percentage of the value of the assets or a set fee that does not vary with the particular investment recommended, rather than a commission or other transaction-based fee.

If an IRA rollover recommendation is executed, then due to the *Level Fee* arrangement any future IRA investment recommendations (such as a recommended asset allocation modification) should not result in an increase in compensation paid to MIL.

Retention of Recommendation Documentation

MIL will retain all records related to documenting why the investment recommendation is in the Best Interest of the Retirement Investor. This documentation, including the relevant investment recommendation checklist along with all other relevant supporting documentation, will be retained in the relevant client file(s).

Annual Review

MIL is required to conduct an annual retrospective review that is reasonably designed to assist the firm with achieving compliance with the Impartial Conduct Standards and the policies and procedures regarding the Prohibited Transaction Exemption rule. Specifically, the methodology and results of this annual retrospective review must be documented in a written report that is provided to MIL's CCO, who in turn will certify annually that:

- The CCO has reviewed the report;
- MIL has in place policies and procedures reasonably designed to achieve compliance with the Prohibited Transaction Exemption rule; and
- MIL has in place a prudent process to (i) modify its policies and procedures as events dictate and (ii) test the effectiveness of these policies and procedures on a periodic basis.

This retrospective review, report and certification must be completed no later than six (6) months following the end of the period covered by the review.

Self-Correction

The Prohibited Transaction Exemption rule also provides self-correction procedures, which state that a non-exempt prohibited transaction will not have occurred due to a violation of the rule provided that:

- Either the violation did not result in investment losses to the Retirement Investor or the investment adviser made the Retirement Investor whole for any resulting losses;
- The investment adviser corrects the violation and notifies the DOL via email at IIAWR@dol.gov within thirty (30) days of the correction;
- The correction occurs no later than ninety (90) days after the investment adviser learned of the violation or reasonably should have learned of the violation; and
- The investment adviser notifies the persons responsible for conducting the retrospective review during the applicable review cycle, and the violation correction is specifically set forth in the written report of the retrospective review.

Recordkeeping

MIL is required to maintain records for six (6) years demonstrating compliance with the Prohibited Transaction Exemption rule. This includes a requirement that the retrospective report, certification, and supporting data be retained for a period of six (6) years from compilation.

Proxy Voting Policy

Proxy Voting Policy Statement

MIL will not ask for, nor accept voting authority for client securities. Clients will receive proxies directly from the issuer of the security or the custodian. Clients should direct proxy questions to the issuer of the security.

Handling of Customer Funds – Custody Issues

Definition

An adviser has custody if it holds, directly or indirectly, client funds or securities, or has any authority to obtain possession of them. An adviser would also have custody if a related person holds, directly or indirectly, client funds or securities, or had any authority to obtain possession of them in connection with advisory services provided to clients. Custody generally includes:

- Having possession of client funds or securities unless the adviser returns them to the client within three days;
- Any arrangement under which the adviser is authorized or permitted to withdraw client funds or securities based on its instructions, including but not limited to direct fee deduction and certain arrangements under a standing letter of authorization or other disbursement authority (SLOA); or
- Any capacity that gives the adviser legal ownership or access to client funds or securities.

Policy

MIL will not have physical custody of any client funds or securities. MIL will maintain client assets with a qualified custodian. MIL may have other forms of custody as defined by the appropriate rule. The CCO will determine whether or not the firm has custody and will ensure compliance with relevant custody rules, including disclosure of custody on Form ADV if/as required.

Direct Fee Deduction

MIL currently has custody via direct fee deduction. When MIL deducts advisory fees directly from client accounts, the following additional steps will be taken:

- Client will provide written authorization permitting the fees to be deducted from his or her account;
- MIL will maintain client assets at a qualified custodian and ensure that the custodian segregates and identifies each client's securities;
- MIL will notify the client in writing of the custodian's name, address, and the manner in which the client assets are maintained;
- MIL will make a reasonable effort to ensure that the qualified custodian being used will deliver quarterly account statements to the client showing transactions for that time period;
- When required by rule, MIL will send an itemized invoice to the client showing the formula used to calculate the fee, the amount of assets under management the fee is based on, and the time period covered by the fee.

The CCO will periodically review and test the management fee calculations to ensure they are accurate based on the advisory contract.

Disbursement Authority via SLOA

Certain clients may grant MIL standing authority via a SLOA to make disbursements to third parties from the client's account at a qualified custodian. Accordingly, MIL would be deemed to have custody of these client accounts.

For any accounts with a SLOA in place, MIL will either (a) follow the custody rules for the relevant jurisdiction, including submitting to a surprise audit as applicable, or (b) follow the conditions set forth immediately below so that no surprise audit will be required for these accounts.

1. The client will be required to provide a written instruction to the qualified custodian 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 will authorize MIL in writing, either on the qualified 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 qualified custodian will perform appropriate verification of the instruction, such as a signature review or other method to verify the client's authorization, and will provide a transfer of funds notice to the client promptly after each transfer.
4. The client will have the ability to terminate or change the instruction to the client's qualified custodian.
5. MIL will have 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. MIL will maintain records showing that the third party is not a related party of MIL or located at the same address as MIL.
7. The client's qualified custodian will send the client, in writing, an initial notice confirming the instruction and an annual notice reconfirming the instruction.

The CCO will periodically review the arrangement to ensure it meets these conditions and document MIL's compliance with the conditions.

Trustee/Executor/Power of Attorney for Advisory Client

Certain clients of MIL may establish MIL or one of its related persons with a power of attorney, as trustee, or as executor for the client. If this occurs, then MIL will be deemed to have custody of client assets. In these cases, MIL will engage an independent account to perform an annual surprise audit of the client's funds and securities with the first audit to occur within six (6) months after becoming trustee or executor for the client. The CCO will periodically review the arrangement to ensure it meets these conditions and document MIL's compliance with the

conditions. In addition, MIL will update its Form ADV to disclose that is has custody of client assets.

However, the SEC does not consider an appointment as trustee or executor to result in custody when the appointment is a result of a family or personal relationship with the client. In this instance, MIL will not be required to follow the custody safeguards immediately above.

Qualified Custodian

Qualified custodian may include a bank, or savings association that has deposits insured by the Federal Deposit Insurance Corporation under the Federal Deposit Insurance and registered broker-dealers.

Receipt of Funds or Securities

If MIL receives a check made payable to a third party (such as a custodian), MIL will make a copy of the check, record the receipt and delivery of the check, and will try to forward the check within 24 hours but always within three (3) business days. An appropriate "check log" (see Sample 6) will be maintained to document receipt and subsequent delivery of the check to the third party.

If MIL inadvertently receives client funds or securities (such as checks made payable to MIL for investment but not for payment of advisory fees), MIL will return to the client the funds or securities within three (3) business days with instructions for the client on where they should send or take the funds or securities.

Safeguarding of Client Assets from Conversion or Inappropriate Use by Advisory Personnel

In an effort to detect unauthorized or inappropriate activity in client accounts, the CCO will request reports that are available to MIL from each custodian and/or clearing firm holding client assets. Such reports may include:

- Client change of address requests;
- Requests to send documents (statements or reports) to addresses other than the home addresses listed on clients' account documents;
- Trading activity reports, including redemption and repurchase requests (most custodians have reports classified or named as exception reports to identify activities in clients' accounts that are "exceptions" to the normal activities);
- Comparisons of IARs' personal trading activity and IARs' clients' trading activity (most regulators will do a review of IARs' personal accounts and do a partial comparison of clients' account activity and holdings and IARs' holdings and activity).

In addition to outside reports, MIL's CCO will institute practices and procedures to monitor the firm's IARs and personnel to look for such items as:

- Unapproved custom reports or statements produced by IARs or support staff;
- Unapproved outside business activities;
- Unapproved seminars or invitations sent to clients, or unapproved changes made to approved seminars or invitations;
- Calls or emails from clients with questions about unapproved products or offerings;
- Calls or emails from unapproved product sponsors (more than just the occasional contact to solicit business);
- "Abnormal" or "suspicious" activities by firm personnel (e.g., frequent "closed door" meetings or calls not due to client privacy).

Account Valuation and Billing

Overview

In computing the market value of any investment of a client's account, each security listed on any national securities exchange or otherwise subject to current last-sale reporting shall be valued at the value reported on the statement that clients receive from the custodian. Such securities which are not traded nor subject to last-sale reporting shall be valued at the latest available bid price reflected by quotations furnished to MIL by such sources as it may deem appropriate.

The firm's billing procedures are disclosed and updated in the Form ADV 2A and the client contracts.

Advisory Fee Review

The CCO will periodically review and test the advisory fee calculations to ensure they are accurate based on the advisory contract.

- MIL will periodically review a sample of client accounts to verify that:
  1) The fee is calculated using the agreed upon rate
  2) The fee is calculated in the manner specified in the client contract (i.e., based on the average daily balance vs. value at end or beginning of billing period)
  3) Assets are valued in the manner specified in the client contract
  4) Household accounts are aggregated for fee billing purposes unless the client contract provides otherwise
  5) Assets that are excluded from billing by the advisory contract are not included in the fee calculation
  6) Fees are billed at the frequency stated in the advisory contract
  7) Fees for new clients are prorated when advisory services began mid-billing period
  8) Fees paid in advance are refunded when a client contract is terminated mid-billing period
  9) A performance fee is not charged to a client who does not meet the proper criteria
  10) The billing rate is reduced when prearranged breakpoints are reached
  11) Wrap fee accounts, if any, are not charged additional fees (such as transaction fees) when the transactions qualify for the wrap fee program's bundled fee
  12) Actual billing practices are consistent with Form ADV disclosures

- MIL will periodically reconcile total advisory fees billed to its clients with fees actually received from its clients.

If a third party (including but not limited to a third party adviser) calculates the advisory fee, then MIL will confirm that the third party has policies and procedures to ensure the accuracy of the fee and will periodically confirm that the third party is following its policies and

procedures. MIL may sample client accounts to confirm the accuracy of the fee calculation by the third party.

Customer Complaint Policy

Definition

A customer complaint will be defined as any written or oral statement of a customer or any person acting on behalf of a customer alleging a grievance involving the activities of persons under the control of MIL in connection with providing investment advice or placing orders on behalf of customers.

Handling of complaints

The firm's CCO shall be responsible for handling complaint reviews. Complaints should be immediately forwarded to the CCO for appropriate handling. No supervisory personnel should attempt to resolve a complaint without the involvement of the CCO.

CCO's Compliance Requirements:

- Review complaints and the facts surrounding the complaints immediately as they are made by customers or reported by supervisory personnel;
- Communicate with customers via telephone, mail, face-to-face meetings, and/or email to resolve complaints and customer issues;
- Maintain a complaint log of complaints. The log will at a minimum contain the following information: customer's name, date complaint received, type of complaint (oral versus written), brief description of complaint, date review started, supervisory personnel involved, date complaint resolved, and a brief description of the resolution;
- Maintain a complete complaint file. This file will contain each customer complaint, including, but not limited to: any letter, email, or document from a customer who has filed a complaint; any letter, email, or document from any agency regarding the complaint; any communication sent from MIL to any customer, agent, agency, or third party regarding each complaint; and documentation of how each complaint was resolved;
- Assure that complaints are settled or resolved and that no complaints are left "dangling" or incomplete. No complaint should be left unresolved and the date the complaint is "closed" should be noted on the complaint log and in the complaint file; and
- Examine the cause of the complaint and determine if changes are needed in policies and procedures or any disciplinary action is warranted to prevent future complaints; and Ensure that relevant disclosure forms and documents are updated, filed and delivered where and when appropriate.

Recordkeeping

Books and Records

The firm's CCO is responsible for keeping the firm's records in accordance with Section 204 of the *Advisers Act* and Rule 204-2.

Record Retention Requirements

The firm's CCO shall ensure that all records are kept readily accessible for at least two years and kept at least five years either on-site or at alternative location.

Financial Condition

MIL will periodically review its financial condition to ensure it is not subject to any financial condition that is reasonably likely to impair its ability to meet its contractual commitments to its clients. If MIL's financial condition is impaired, then it will determine whether it should disclose its financial condition to its clients in its ADV Part 2A.

Minimum Net Worth Computation

If required by the jurisdiction(s) in which it is registered, MIL shall prepare and maintain a balance sheet in conformity with GAAP each month. The balance sheet shall be dated as of the last day of the month and shall be prepared within ten (10) business days after the end of the month. MIL shall at all times maintain a net worth in compliance with the applicable requirements of the jurisdiction(s) in which it is registered. Should MIL fail to maintain a sufficient net worth, then it will provide notification of the deficient net worth to the applicable regulator by the close of business on the next business day, together with a balance sheet dated as of the date such deficiency occurred.

Registration, Hiring, and Training of Supervised Persons

Firm Policy

The firm's CCO shall be responsible for handling the hiring, registration if required, and training of IARs and unregistered employees. IARs that are independent contractors will be considered employees for purposes of this discussion.

A list of employees, both registered and unregistered will be maintained.

Hiring

The firm's CCO will:

- Conduct background checks and due diligence to ensure new hires will not pose compliance or regulatory problems;
- Verify whether or not the activities of new hires will require registration as "IARs" in any jurisdiction;
- Verify whether or not the activities of new hires will require them to be considered access persons for compliance with personal securities transactions requirements;
- Review outside business activities of new hires; and
- Collect attestations from new hires that they have read and will abide by MIL's Policies and Procedures Manual, Code of Ethics, Privacy Policy and any applicable corporate policies.

Registration

If the CCO determines that IAR registration is required, the following steps will be taken:

- Determine the submission requirements for registration, which may include depending on jurisdiction:
    - Reviewing the Form U4 and submitting it to the IARD system in order to request registration;
    - Reviewing the NY-IAQ and submitting it to the state in order to request registration in New York; and/or
    - Submitting additional paperwork, such as fingerprints or affidavits.
- Create a Form ADV Part 2B for the IAR; and
- Ensure the new hire does not engage in activity that would require registration until such time that the individual's IAR registration is approved.

The CCO will continually monitor the activities of unregistered employees to ensure they do not engage in any activity that would require registration as an IAR.

Training

Ongoing training for unregistered employees and IARs may be provided by the CCO. Ongoing training may include but is not limited to topics relating to: MIL's Policies and Procedures and Code of Ethics, privacy issues, services offered by the firm or general compliance topics.

At least annually, staff will be required to attend annual meetings and complete annual attestations. Topics from any annual meetings along with the annual attestations will be maintained.

Professional Designations

Representatives of MIL may use professional designations/certifications if they are specific accredited designations/certifications. Allowed designations may be used in the representative's Form ADV Part 2B, on his or her business cards, and/or on approved advertisements. The following policies govern the use of these designations:

- Representatives desiring to use professional designations must request approval by MIL prior to the use of any designation.
- The CCO will be responsible for approving any designation requested to be used by a representative of MIL.
- If a requested designation is not on MIL's approved list, the representative must provide all support documentation to ensure that the designation is a valid designation by an accredited organization. Such documentation should include the organization's reasonable standards or procedures for assuring the competency of its certificants; reasonable standards or procedures for monitoring and disciplining its certificants for improper or unethical conduct; and any continuing education requirements for its certificants in order to maintain the designation or certification.
- The CCO may approve or deny a representative's request to use designations.
- Those holding these designations will be responsible for keeping in good standing, or will notify the CCO immediately if the organization has taken adverse action against the representative or there is any lapse in the certification.
- When a supervised person is using a professional designation for registration or marketing purposes, the CCO will confirm annually that the supervised person using the designation has completed all annual requirements in order to be in good standing with the professional designation.

Firm Registration

MIL is a registered investment adviser, registered pursuant to the Investment Advisers Act of 1940.

Policy

It is the firm's policy to maintain compliant registration status at all times. This may require additional "notice" filings in other appropriate jurisdictions as required.

Unless otherwise permitted, MIL will not conduct investment advisory activity in any jurisdiction unless the firm is first notice filed in that jurisdiction. While most jurisdictions will allow for a "de minimis" number of clients before requiring firm notice filing, some jurisdictions may require notice filing upon taking on the first client in that jurisdiction. Having a "place of business" in a state, as defined by applicable regulatory statutes, in a state will require notice filing regardless of the number of clients in that jurisdiction.

It is the CCO's responsibility to ensure that the firm is appropriately registered and notice filed at all times.

Procedure

The firm's CCO will:

- Monitor the state of residence of the firm's clients to ensure the firm does not exceed the de minimis threshold for any jurisdiction;
- File updated applications to request additional state notice filings when needed.

Renewal

The firm's CCO will ensure that:

- The firm's annual renewal fees are timely paid through the IARD system every calendar year as required;
- The firm files its Form ADV Annual Amendment within 90 days of its fiscal year end; and
- The firm provides any additional paperwork or other information required on an annual basis in connection with the firm's annual renewal filings.

Other-than-Annual Amendments

The firm's CCO will ensure that the firm files material changes to its Form ADV and any Form U4 documents promptly, usually within 30 days, if the following occurs:

- Information in Items 1, 3, 9 (except 9A(2), 9B(2), 9E, and 9F), or 11 of Part 1A becomes inaccurate
- Information in Items 4, 8, or 10 of Part 1A becomes materially inaccurate
- Information provided in MIL's firm brochure becomes materially inaccurate
- Information provided in the Form CRS becomes materially inaccurate (the firm must file updates to the Form CRS within 30 days)

Form ADV Part 2A Firm Brochure

MIL will update the firm brochure each year at the time it files its annual updating amendment and promptly whenever any information in the brochure becomes materially inaccurate. All updates to a firm brochure will be filed through the IARD system and maintained in the firm's files.

Form ADV Part 2B Brochure Supplement

Brochure supplements are required for each supervised person who formulates investment advice for a client and has direct client contact and any supervised person who has discretionary authority over a client's assets, even if the supervised person has no direct client contact. MIL is not required to file its brochure supplements, but it is required to maintain copies of all supplements and amendments to supplements in its files. MIL will update brochure supplements promptly whenever any information in them becomes materially inaccurate.

Distribution of Disclosure Documents

Form ADV Part 2A Firm Brochure

MIL delivers the applicable firm brochure to each client before or at the time it enters into an advisory agreement with that client. Additionally, each year within 120 days of the end of the firm's fiscal year, MIL delivers to each client either (i) an updated firm brochure accompanied by a summary of material changes or (ii) a summary of material changes with an offer to provide the entire firm brochure.

As a fiduciary, MIL has an ongoing obligation to inform its clients of any material information that could affect the advisory relationship. MIL will deliver to clients any update to the firm brochure that amends information in response to Item 9 of Part 2A (disciplinary information and will also disclose other material changes to clients, even if those changes do not trigger delivery of an interim amendment.

Form ADV Part 2B Brochure Supplement

MIL prepares a brochure supplement for any supervised person who formulates investment advice for a client and has direct client contact and any supervised person who has

discretionary authority over a client's assets, even if the supervised person has no direct client contact. The firm delivers the brochure supplement for each supervised person who provides advisory services to a client before or at the time the supervised person begins to provide advisory services to the client.

No supplement is required for a supervised person who has no direct client contact and has discretionary authority over a client's assets only as part of a team.

As a fiduciary, the firm has a continuing obligation to inform its clients of any material information that could affect the advisory relationship. MIL will deliver to clients any update to the supplement that amends information in response to Item 3 of Part 2B (disciplinary information) and will also disclose other material changes to clients, even if those changes do not trigger delivery of an updated supplement.

Electronic Delivery

When consent is not explicitly granted in the client contract, MIL obtains client consent for electronic delivery of its brochures using an electronic delivery consent form. Evidence of annual delivery is maintained.

Form ADV Part 3 Client Relationship Summary (Form CRS)

If MIL has clients who are retail investors, then MIL files a Form CRS through the IARD system that briefly describes its types of client relationships and services; fees, costs, conflicts of interest, and standard of conduct; disciplinary history, and other information relevant to the client relationship. A client is a retail investor if the client is a natural person and receives advisory services primarily for personal, family, household purposes.

Initial Delivery

MIL delivers its Form CRS to each retail investor client before or at the time it enters into an advisory agreement with that client. In addition, MIL will deliver its Form CRS to an existing retail investor client.

Ongoing Delivery

In addition to the initial delivery, MIL will deliver its Form CRS to an existing retail investor client before or at the time that it:

- Opens a new account that is different from the retail investor's existing account(s);
- Recommends that the retail investor roll over assets from a retirement account into a new or existing account or investment; or
- Recommends or provides a new investment advisory service or investment that does not necessarily involve the opening of a new account and would not be held in an existing account.

As a fiduciary, MIL has a continuing obligation to inform its clients of any material information that could affect the advisory relationship. Accordingly, MIL updates its Form CRS and files the amended Form through the IARD system within 30 days after any information in the Form becomes materially inaccurate. Within 60 days after a Form CRS is required to be updated, MIL delivers to each retail investor client the amended Form CRS or communicates the updated information to such client by other means.

Upon request from a retail investor client, MIL delivers its current Form CRS to the client within 30 days.

Method of Delivery

MIL may deliver its Form CRS electronically if the retail investor client consents to electronic delivery. The client may grant consent to electronic delivery in the client contract or through other means.

MIL maintains evidence of each delivery of its Form CRS to a retail investor client whether delivered electronically or by other means.

If MIL has a public website, it prominently posts its current Form CRS in an easily accessible location and format.

Other Regulatory Filings

Some firms may be required to make additional filings pursuant to the Securities Exchange Act of 1934.

Firm Policy

It is the firm's policy to make the necessary filings. It is the CCO's responsibility to be familiar with the various filings and to ensure that the firm has made the appropriate filings in a timely manner.

Specific Filings

Some of these filings with a brief description include:

- Section 13(d) – Requires a Schedule 13D to be filed by the beneficial owner of more than five (5) percent of a publicly traded equity security (Section 12). It is important to understand the broad definition of "beneficial owner" and the timing of the report, which has to be filed within 10 days of the purchase.
- Section 13(f) – Requires advisers to file a Form 13F if they exercise investment discretion with respect to $100 million or more in certain identified 13F securities. Form 13F usually has to be filed within 45 days of the end of the quarter.
- Section 13(g) – Requires a filing similar to a Schedule 13D, but with less information. May be allowed if the investor is strictly a passive investor and does not intend to exert control.
- Section 13(h) – Requires an adviser that is defined as a "large trader" to file its first Form 13H within 10 days of meeting the threshold. Large traders are also required to amend Form 13H annually within 45 days of the end of the year and make quarterly update filings. A large trader is a person or entity whose trades exceed either (i) two million shares or $20 million in a day or (ii) 20 million shares or $200 million during any calendar month.
- Section 16 – Requires directors, officers, and shareholders of more than ten (10) percent of a publicly traded company to file various reports based on activity, specifically: Forms 3, 4 and 5.

If the CCO at any time determines that the firm needs to make one of these regulatory filings, it may be helpful at that time to consult with a qualified attorney or third party to help with the filing.

Solicitors

If MIL compensates a person for client referrals, MIL will follow the procedures set forth below.

A solicitor is any person who refers a potential client to an investment adviser. MIL will only compensate a solicitor for client referrals if the solicitor is registered either as an investment adviser or as an investment adviser representative; or in compliance with SEC Rule 275.206(4)-3 or applicable state law. Whether or not registration is required to solicit business on behalf of MIL, the solicitor MUST comply with the provisions of SEC Rule 275.206(4)-3 and/or applicable state law.

MIL will do the following when engaging a solicitor:

- MIL will create a solicitor's agreement between MIL and the solicitor detailing term, payments, marketing activities, and disclosures. The solicitor will not act in the capacity of investment adviser representative of MIL unless so registered;
- MIL will create a solicitor's disclosure document. The solicitor will provide the disclosure document to prospects at or around the time of solicitation and no later than the time of contracting by MIL. The disclosure document must identify the solicitor and his or her activities, detail his or her compensation, acknowledge the delivery of MIL's firm brochure (ADV 2A), and be signed by the prospect with a copy delivered back to MIL;
- MIL will maintain records of solicitation as well as a list of solicitors past and present for five years as part of its ongoing books and records requirements;
- MIL will ensure its ADV filings reflect that it has solicitors associated with the firm.
- MIL will not engage a solicitor who is disqualified under SEC Rule 275.206(4)-3.

Trading

MIL uses the electronic order entry system provided by its custodian or another third party to enter trading activity and transactions. If electronic means are not available, MIL may place orders by fax or telephone, in which case order tickets will be maintained. If MIL uses multiple custodians the order entry priority will be alternated between custodians so that clients will not be disadvantaged on an ongoing basis.

Directed Brokerage

MIL does not allow its clients to direct brokerage. MIL recommends one or more custodians or broker-dealers to effect securities transactions for its clients. The custodians or broker-dealers were chosen based on MIL's fiduciary responsibilities to provide best execution.

Soft Dollar and Additional Economic Benefit Practices

Background

The SEC has interpreted "soft dollar" practices as arrangements under which products or services, other than execution of securities transactions, are obtained by an investment adviser from or through a broker-dealer in exchange for the direction by the adviser of client brokerage transactions to the broker-dealer. MIL has an affirmative duty of full and fair disclosure of material facts in relation to soft dollar practices to its clients, as well as an obligation to act in the best interests of its clients and to place client interests before its own as part of any soft dollar arrangements. The SEC, through its interpretive release of Section 28(e) of the Securities Exchange Act of 1934 effective July 24, 2006, defined acceptable brokerage and research services that fall under the safe harbor of Section 28(e). An adviser that determines in good faith that the brokerage and research services received in exchange for sending transaction business to a broker-dealer are reasonable compared to the commissions paid by the clients will not have breached its fiduciary duty.

Firm Policy

While MIL has no formal soft dollar program in which soft dollars are used to pay for third party services, MIL may receive research, products, or other services from custodians and broker-dealers ("economic benefits"). Our receipt of these benefits is not tied directly to client transactions, but we may be required to maintain a certain level of client assets at the broker-dealer or custodian in order to receive the benefits. This results in a conflict of interest. There can be no assurance that any particular client will benefit from additional benefits, whether or not the client's transactions paid for it, and MIL does not seek to allocate benefits to client accounts. MIL benefits by not having to produce or pay for the research, products or services, and MIL will have an incentive to recommend a broker-dealer based on receiving additional economic benefits. Clients will be made aware through disclosure that MIL receives these

economic benefits and its recommendation of the broker-dealer may result in higher commissions charged to the client. MIL will evaluate whether our receipt of any economic benefits is in the best interest of our clients.

Compliance Requirements

MIL's CCO is responsible for the following:

- Ensuring that this policy is followed and, if any new arrangements are subsequently created, that the policy as well as MIL's firm brochure are promptly updated to properly reflect this;
- Ensuring the best execution of securities transactions if/when MIL executes or arranges for trades on behalf of clients.

Review Process

Reviews of the firm's soft dollar and additional economic benefits practices are conducted by the CCO no less than annually. Interim reviews may be conducted in response to changes in the firm's practices.

Block Trading

Should MIL decide that aggregating client orders (block trading) for more than one client is in the best interests of those clients, then MIL will effect the transaction and allocate shares from the block trade in a fair and equitable manner.

MIL will follow custodial or broker-dealer instructions for a block trade, including but not limited to:

- Indicating the number of shares to be allocated to each account;
- Having shares allocated on a pro-rata basis based upon the size of the client's account;
- Distributing custodian or broker-dealer charges for the block trade on a pro-rata basis to each client account; and
- Ensuring each account receives the average execution price of the trade(s).
- There may be certain circumstances associated with a block trade that may prevent a pro-rata distribution to client accounts and require the CCO to make a determination in the best interests of the clients involved in the transaction.

In cases where the entire block trade cannot be effected:

- Some clients may be excluded from the allocation process if their allocation would result in a de minimis allocation;
- Clients with low cash positions could be considered first in the allocation process;
- Client accounts requiring the smallest number of shares could be allocated shares over accounts with larger requirements;
- The CCO may devise a system that does not favor one client account or household over

another; and/or
- Allocations will be made each day should the block trade take more than one day and best efforts will be made by MIL to ensure one account is not favored over another.

While block trading may benefit clients by purchasing or selling larger blocks in groups, MIL does not feel that the clients are at a disadvantage due to the best execution practices of its custodian. Under certain circumstances even though MIL maintains the ability to block trade MIL may not choose this method of transaction.

Circumstances when block trading will not be used:

- The size of the order in dollars may affect the market in the security;
- The volume of the order in shares may affect the market in the security;
- The number of client accounts of MIL involved in the order;
- Models and strategies of the firm affect the custom component of a client's account.

Under certain circumstances, employees of MIL may participate in the aggregated trade of securities alongside clients of MIL. This will be covered in the Code of Ethics section of the manual. Employees of MIL will not be favored as far as price or allocations in this type of transaction are concerned.

Records associated with block trades will be kept by MIL as part of its books and records requirements.

MIL will make the appropriate ADV filings and disclosures in reference to block trades.

Trade Errors

A trade error occurs when there is a deviation from the general trading practices involving transactions and settlements of trades for a client's account. Part of MIL's fiduciary obligation is to identify and correct these errors as soon as discovered.

In general, the following may be viewed as trade errors:

- An incorrect type of transaction (e.g., buy, sell, limit, market);
- A purchase or sale of the wrong security or the wrong amount;
- A trade taking place in an incorrect account number;
- An inaccurately allocated block trade;
- The purchase or sale of securities in violation of the client's investment profile or guidelines; and
- The purchase or sale of securities for non-discretionary clients prior to or without receiving client consent, or without proper documented authorization.

The following types of errors will not be deemed a trade error:

- An incorrect trade that was caught prior to settlement thereby not having a negative

impact on the client;
- A trade that was improperly documented;
- The rewriting of a ticket that describes or corrects an improperly executed transaction;
- An error made by an unaffiliated third party (broker-dealer, custodian, etc.). However, MIL is responsible for reviewing these trades and ensuring that third party errors are favorably resolved; and
- A good faith transaction for the client, based on MIL's evaluation and assessment, which may not be in line with client's objective.

Trade errors must be brought to the CCO in a timely manner once discovered. The CCO should document when the trade error occurred and whether MIL is responsible (see Sample 7). If responsible, MIL will look to correct the error immediately, on the same day if possible, following fiduciary standards and acting in the client's best interest. If a third party is responsible, MIL will oversee the resolution. Any loss will be reimbursed to the client for the full amount of the loss, including the reimbursement of transaction fees, in the form of a statement credit or check written by MIL, if the custodian or broker-dealer does not cover it under the de minimis. MIL may also contact its E&O carrier if needed.

If there is a profit resulting from the error:

- MIL may hold the profit in a firm trade error account in accordance with its accounting standards and donate them to charity annually.

Payments made to clients will be properly documented. MIL will maintain a trade error file for a period of at least five years.

Trading Practices

Broker Selection

The following steps will be taken when selecting broker-dealers to execute client trades:

- The CCO will create a list of broker-dealers approved to execute client trades. This list will set forth guidelines for the percentage of trades the firm will allocate to particular broker-dealers and other execution facilities;
- Periodically the CCO will review this list and compare it with actual allocations made over the past quarter or some other period;
- If significant deviations should occur, the CCO will investigate such deviations and the Company should consider revising the list;
- The CCO will periodically and systematically monitor and evaluate the execution and performance capabilities of the broker-dealers MIL uses. Monitoring methods will include, among other things, encouraging traders to obtain multiple price quotations for a trade from multiple sources and indicate them on the trade ticket, reviews of trade tickets, confirmations and other documentation incidental to trades, and periodic meetings to solicit and review input from MIL's traders, portfolio managers and others;
- From time-to-time, quantitative performance data about broker-dealers will be acquired

from the broker-dealers or third party evaluation services to assist the review process;
- The CCO will request periodically and review some or all of each broker-dealer(s) reports on order execution (SEC Rule 11Ac1-5) and order routing (SEC Rule 11Ac1-6) to ascertain whether the executing broker-dealer is routing client trades to market centers that execute orders at prices equal to or superior to those available at other market centers. Evidence of such reviews shall be appropriately documented.

Best Execution

Under applicable law, MIL owes a fiduciary duty to clients to obtain best execution of their brokerage transactions. MIL also has a fiduciary duty to its clients to achieve best execution when it places trades with broker-dealers. Failure by MIL to fulfill its duty to clients to obtain best execution may have significant regulatory consequences. MIL policies are modeled after the guidelines articulated by the regulators; specifically, it believes that, to a significant degree, best execution is a qualitative concept. In deciding what constitutes best execution, the determinative factor is not the lowest possible commission cost, but whether the transaction represents the best qualitative execution. In making this determination, MIL's policy is to consider the full range of the broker's services, including without limitation the value of research provided, execution capabilities, commission rate, financial responsibility, administrative resources and responsiveness. MIL periodically and systematically, but no less than annually, will evaluate the quality of brokerage services provided by broker-dealers executing its transactions.

Factors that will be considered will include:

- Quality of overall execution services provided by the broker-dealer;
- Promptness of execution;
- Liquidity of the market for the security in question;
- Provision of dedicated telephone lines;
- Creditworthiness, business reputation and reliability of the broker-dealer;
- Research (if any) provided by the broker-dealer;
- Promptness and accuracy of oral, hard copy or electronic reports of execution and confirmation statements;
- Ability and willingness to correct trade errors;
- Ability to access various market centers, including the market where the security trades;
- The broker-dealer's facilities, including any software or hardware provided to the adviser;
- Any specialized expertise the broker-dealer may have in executing trades for the particular type of security;
- Commission rates;
- Access to a specific IPO or IPOs generally.

Anti-Insider Trading Policy

Background

An investment adviser should establish, maintain and enforce written policies and procedures reasonably designed, taking into consideration the nature of such investment adviser's business, to prevent the misuse of material, non-public information by such investment adviser or any person associated with such investment adviser.

Compliance Requirements

The CCO is responsible for:

- Ensuring employees and associated persons sign a statement acknowledging and agreeing to abide by the firm's prohibition on insider trading;
- Maintaining a list for each access person listing securities owned ("Holdings report" – see Sample 8);
- Maintaining copies of transaction confirmations or monthly or quarterly securities account statement summaries from each of these persons ("Transactions report" – see Sample 9);
- Reviewing these confirmations and statements for inappropriate transactions and reporting them to CCO for action;
- Maintaining records of CCO reviews and results.

The employee acknowledgement statement and Holdings report should be provided to the CCO on the date of association and annually thereafter. Other record-keeping requirements should be done on a quarterly basis, no more than 10 days after the end of the calendar quarter. Reviews of this policy are to be conducted by the CCO on an annual basis at a minimum.

Material Interest of the Investment Adviser and Personal Trading Activities of Supervised Persons

Material Interest

MIL will not recommend to clients, or buy or sell for client accounts, securities in which the firm or a related person has a material financial interest. (Examples of a material financial interest would include: acting as a principal, general partner of a partnership/fund where clients are solicited to invest, or acting as an investment adviser to an investment company that the firm recommends to clients.)

Investing Personal Money in the Same Securities as Clients

From time to time, representatives of MIL may buy or sell securities for themselves that they also recommend to clients. The CCO will always document any transactions that could be construed as conflicts of interest and MIL will always transact client business before its own when similar securities are being bought or sold.

Supervision and Compliance

CCO Responsibility

The CCO is primarily responsible for supervising the activities of all supervised persons for compliance with both applicable rules/regulations and MIL's internal policies and procedures.

The CCO may delegate certain supervisory tasks to other responsible persons with the knowledge and expertise to effectively administer those activities. It is ultimately the CCO's responsibility to ensure that delegated supervisory tasks are being completed. Delegated duties, if any, are listed below:

Description of task/responsibility	Name of Delegate	Title of Delegate
Employee Hiring	Cassie Ottofaro	Operations

Firm Policy

The firm has implemented a system to prevent and detect prohibited activity and to ensure compliance with the firm's policies and procedures. The CCO will review reports, ask and answer questions, conduct investigations when appropriate and document the supervisory activity.

Risk Assessment

The CCO will at a minimum annually conduct a risk assessment to identify and analyze potential risks associated with the firm. This may be accomplished throughout the year or at a specific time chosen by the CCO. The risk assessment will be used to identify potential weaknesses in this manual, the supervisory practices of the firm or the compliance program as a whole.

Annual Review

The CCO will conduct an annual review of the firm's entire compliance program as specified in Rule 206(4)-7. Different elements of the review may include:

- Meetings with executive staff on current policies;
- Risk assessment;
- Testing and verifying that current procedures are reasonably designed to achieve compliance with security rules and regulations;
- Updating procedures where necessary; and/or
- Notifying staff of changes in firm policies and procedures.

Remote Office Supervision

For the purpose of this section, a remote office is an office location from which the RIA conducts advisory business regardless of distance from the adviser's main office (the location where the CCO is located and the majority of supervisory activities is conducted), that is not visited at least monthly by the adviser's CCO.

MIL understands that the remote office locations present their own unique compliance challenges and has implemented the following additional "remote office" compliance policies and procedures:

- Remote office personnel are required to submit new client account applications and applicable paperwork to the adviser's CCO for review and submission to the custodian or other appropriate entity;
- Remote offices are required to submit advertising and correspondence material for approval prior to using or sending these items to their clients. This requirement includes items such as, but not limited to: letterhead, business cards, seminars, websites, flyers, brochures, slide presentations, radio and print advertising;
- Remote offices are required to submit for approval any d/b/a name used by any person or firm located at the office;
- Since emails are considered correspondence, remote office IARs are required to use a pre-approved email address monitored by the firm's CCO;
- Remote offices are required to immediately report customer complaints – both verbal and written – to the CCO. This notification will be followed by further communication including a detailed explanation of the matter from the involved representative;
- Since the adviser's main office is required to maintain books and records for the firm, remote offices are required to submit copies of "hard copy" items to the main office in a timely manner. An example of a hard copy item would include any client applications or other client paperwork done on paper rather than electronically. Most hard copy items should be scanned and submitted via email attachment or via file upload whenever possible;
- IARs and supervised personnel are required to sign annual attestation statements acknowledging that they have read, understood, and agreed to abide by the policies, procedures, and ethical business standards of MIL; additionally, remote office supervised personnel may be required to sign a more robust statement with additional items unique to remote office locations;
- MIL conducts periodic reviews of remote office client files (maintained by the adviser's main office) to verify that they are complete and that portfolio holdings are suitable and appropriate for the investment profile information in the client files. This review may be done additionally, concurrently, or separately from the client file review done at the adviser's main office;
- MIL and remote office personnel agree to in-office reviews, both announced and un-announced, on a periodic basis and no less often than annually that will be dictated by MIL's CCO and based on the remote office's activity level, business model, or other items. These reviews will be conducted by MIL's CCO or designee.

Political Contributions ("Pay to Play Rules")

Rule 206(4)-5 under the Advisers Act curtails (the "Pay to Play Rules") improper influence on government officials and entities when awarding contracts to a registered investment adviser to advise/manage public funds.

The Pay to Play Rules generally prohibit MIL, as an investment adviser, from providing advisory services for compensation to a government entity (including the investment by the government entity in any fund) for two years when MIL or certain supervised persons makes a contribution (as defined below) to certain state, local or federal government-elected officials or candidates where the office of such official or candidate is directly or indirectly responsible for or can influence (or has authority to appoint any person who is directly or indirectly responsible for or can influence) the hiring of MIL to manage the assets of the government entity. Government entities covered by the Pay to Play Rules include state, local or federal government pension plans, state university endowments and other state, local or federal government accounts.

The compensation prohibition would be triggered when a "contribution" to a government official or campaign is made by MIL or by certain supervised persons. Examples of "contributions" include, but may not be limited to: the donation of money (check, credit card or cash) for a political campaign or in-kind contributions such as the use of a personal residence or office location, staff or refreshments for a campaign event, payment to attend a political fund-raising event or anything else of value for the purpose of influencing an election.

In addition, MIL may be prohibited from receiving compensation from a government client for two years if either MIL or a supervised person engages in fundraising activities that include soliciting or coordinating ("bundling") political contributions or payments to a state or local political party where, or to an official or candidate of a government entity to which, MIL is providing or seeking to provide advisory services. Supervised persons should be sensitive that fundraising may occur at a formal event organized and classified as a fundraiser or on an unplanned basis in an informal setting.

Pre-Clearance Requirements and Procedures

MIL and its supervised persons are required to obtain written pre-clearance from the CCO prior to MIL or the supervised person, the supervised person's spouse, or any immediate family member:

- Making any political contribution to a candidate for state, local or federal office, or an official of any state, local or federal government entity or subdivision thereof, or to a political action committee ("PAC");
- Engaging in fundraising or volunteer activities related to any state, local, federal political or governmental activities, or on behalf of an official of any state, local, federal government entity or subdivision thereof;
- Making contributions to a political party or designated group to indirectly contribute to a government official or candidate otherwise prohibited by this policy; or

- Soliciting or coordinating ("bundling") from any person or PAC to make any contribution or payment (whether or not intended to influence an election or campaign) to a government official, candidate for government office, political party or PAC.

Each supervised person is required to pre-clear his or her (or spouse's or any immediate family member's) proposed political contributions described above, as well as fundraising, volunteering for, or otherwise engaging in any activity with respect to any of the above.

Prohibition on Indirect Contributions and Activities

Neither MIL nor any supervised person shall use any person or entity to circumvent or act as a "conduit" to make contributions, or coordinate any contributions, to an official or candidate. Supervised Persons may not be directly or indirectly reimbursed or otherwise compensated by MIL for any political contribution or activity prohibited by this policy and otherwise cannot do indirectly what they cannot do directly pursuant to this policy.

New Employees

New employees (and certain consultants deemed supervised persons by the CCO) will be required to complete a form to report political contributions made by them (and their spouses and immediate family members) over the previous two years. This information will be submitted to the CCO prior to hiring or engagement to ensure compliance with the Pay to Play Rule.

Third Party Solicitors

The federal Pay to Play Rule also prohibits MIL from providing or agreeing to provide, directly or indirectly, payment to any third party solicitor who, for a fee, solicits advisory business from any government client on behalf of MIL, unless the solicitor is a regulated person. A regulated person is a (i) registered broker-dealer, also subject to pay to play restrictions; (ii) registered investment adviser also subject to pay to play restrictions; or (iii) registered municipal adviser subject to the pay to play restrictions adopted by the Municipal Securities Rulemaking Board. The CCO should be consulted prior to engaging any solicitor to receive pre-clearance to engage such solicitor and to ensure that such solicitor meets the definition of a "Regulated Person" and has sufficient "pay to play" policies in effect. Each agreement with a solicitor prior to its execution must be reviewed and approved in writing by the CCO.

In certain limited circumstances, MIL may have a limited ability to cure the consequences of an inadvertent political contribution to an official for whom the supervised person making it is not entitled to vote, provided that the contributions, in the aggregate, do not exceed $350 to any one official, per election, if discovered within four months of the date of such contribution. Therefore, in order to catch any such inadvertent contribution, the CCO will require quarterly certification from supervised persons that political contributions and activities have been pre-approved and are recorded in compliance with the Pay to Play Policy.

Business Continuity Plan

Background

While it is recognized it is not possible to create a plan to handle every possible eventuality, it is the intent of MIL to set up a framework to be used in the most likely of scenarios. It is also the intent that this framework provide guidance as to how to respond should an unforeseen situation occur.

MIL believes that an adviser's fiduciary obligation to its clients includes the obligation to take steps to protect the clients' interests from being placed at risk as a result of MIL's inability to provide advisory services after, for example, a natural disaster or, in the case of some smaller firms, the death of the owner or key personnel. The clients of an adviser that is engaged in the active management of their assets would ordinarily be placed at risk if the adviser ceased operations.

Emergency Information

Firm Contact Persons

MIL's emergency contact persons are:

Contact Name	Phone	Email	Relationship
Cassandra Ottofaro	7728074628	cassie@motiv8advisors.com	Operations
Michael Terrio	772-807-4628	mike@motiv8advisors.com	Owner

Support Services

In the event of an emergency, the following is a list of support services and the methods by which they may be contacted:

Emergency Services (EMS): 772-288-5693

Fire Department: 772-288-5360

Police Department: 772-288-5300

Internet Service Provider: (800) 934-6489
Support@xfinity.com

Data Backup Provider: (561) 744-3282
rbosworth@2jdata.com

Service Provider	Company Name	Contact Name	Phone	Email
Accountant	Ellen Joseph CPA	Ellen Joseph	9542421200	contact@ellenjoseph.com
Computer technician	2JData	Ryan Bosworth	(561) 744-3282	rboswortth@2jdata.com

Alternative firm contact in case of death of Key Personnel	Cassandra Ottofaro

This information will be updated in the event of a material change, and MIL's CCO will review the plan on an annual basis.

Firm Policy

MIL's policy is to respond to a Significant Business Disruption (SBD) by safeguarding employees' lives and firm property, making a financial and operational assessment, quickly recovering and resuming operations, protecting the firm's books and records, and allowing its clients to transact business.

In the event that MIL determines it is unable to continue its business, it will assure clients prompt access to their funds and securities.

Significant Business Disruptions (SBDs)

MIL's plan anticipates two kinds of SBDs, internal and external. Internal SBDs affect only MIL's ability to communicate and do business, such as a fire in its building or the death of a key member of the firm. External SBDs prevent the operation of the securities markets or a number of firms, such as a terrorist attack, a city flood, or a wide-scale, regional disruption.

MIL's response to an external SBD relies more heavily on other organizations and systems, such as the brokerage firm(s) and Internet Service Providers it uses.

Pandemics, Epidemics, & Outbreaks

MIL recognizes that pandemics, epidemics, and other types of outbreaks constitute business disruptions of a special nature. These situations impact not only MIL as a company, but also its

personnel, clients, and vendors. Accordingly, MIL intends to implement the following procedures during such a situation.

General Business Operations

Promptly, and then intermittently thereafter, MIL will conduct a high-level assessment of the situation's impact on business and operations. Specifically, MIL will identify and address:

- any weaknesses or unforeseen issues
- any inability to conduct essential operations or operate essential systems
- any inability to monitor third party vendors

Information Security & Remote Operations

MIL will also alert personnel to the increase likelihood of phishing attempts and client impersonation schemes related to the situation. For example, bad actors may target individual staff members with requests for wire transfers posing as a client, emails related to state or federal work from home updates, changes to healthcare benefits, changes in information security policy related to working from home, software required to install on computers in order to work from home, the latest epidemic statistics, or even discounted offers on items in short supply. Accordingly, the firm will refer personnel to MIL's cybersecurity best practices and ensure that those practices are up to date.

If necessary, MIL will also conduct training for its personnel to address (i) potential information security issues commonly associated with remote work and (ii) the importance of protecting non-public client information at all times. In particular, advisory personnel are instructed to:

- access the internet only from secure WiFi connections or via a virtual private network ("VPN")
- avoid using public WiFi networks, which are vulnerable to exploitation
- store any sensitive, non-public information on non-company devices only after taking the proper security protections and obtaining authorization

If having personnel work remotely, then MIL will also:

- catalogue systems that cannot be accessed remotely, if any
- shut down non-essential hardware (e.g., computers)
- lock its physical storage (e.g., file cabinets) and all office access
- check in with building management, if applicable, to determine current security at the facility
- require that firm personnel continue following advertising guidelines for applicable communications
- ensure electronic cataloguing of communication is still taking place
- continue to document all interactions with clients, regardless of the medium of interaction
- update MIL's business continuity plan as needed

Third Party Vendors

If appropriate, MIL will endeavor to discuss with vendors the following:

- the vendor's business continuity efforts
- the vendor's disaster recovery plans
- the vendor's reliance on, and communications to date with, the vendor's vendors

Company Personnel

If appropriate, MIL will limit or altogether avoid in-person meeting with clients and advisory personnel and allow or require (as appropriate) personnel to work remotely. Any personnel that is limited in their ability to work remotely, will immediately inform their supervisor. Limitations include but are not limited to:

- Inadequate hardware, software, or other systems
- Need to perform caregiving services for children or other persons
- Physical incapacity

If essential personnel are limited in their ability to work remotely, then the firm will determine if alternate or temporary personnel are available to perform necessary functions. Additionally, MIL will conduct check-ins with advisory personnel no less than weekly regarding remote work conditions.

Approval and Execution Authority

The CCO is responsible for approving the plan and for conducting the required annual review. The CCO has the authority to execute this BCP.

Plan Location and Access

MIL maintains copies of its BCP and annual reviews, and all changes that have been made. A physical copy of the BCP is stored with the company's Written Policies and Procedures Manual, which is kept in the following location: Server and Safe. An electronic copy of this plan is stored: PDF on External Server/Sharepont.

Each employee is given a copy of the plan and notified of the location/file within MIL's electronic systems to which employees have access. Physical copies need to be returned upon termination of employment with the firm.

Custodian and Brokerage Firm Contacts

Charles Schwab & Co., Inc. Advisor Services
450 Newport Center Dr. Suite, #410
Newport Beach, CA 92660
(877) 687-4085

TD Ameritrade Institutional, a division of TD Ameritrade, Inc. Member FINRA/SIPC
200 S 108th Ave

Omaha, NE 68154-263
(800) 934-6124

Office Locations

MIL's primary office address and phone number are:

2104 Se Rays Way
Stuart, FL 34994
United States
772-807-4628

MIL's other addresses are:

5430 Three Points Blvd
#112
Mound, MN 55364
United States

3810 N Front St
Fayetteville, AR 72703
United States

4800 Mayfair Dr
Oklahoma City, OK 73112
United States

19478 Springfield Road
Groveland, IL 61535
United States

2535 Tech Drive, Ste 313a
Bettendorf, IA 52722
United States

200 Ne Missouri Rd. Ste 200
Lee's Summitt, MO 64086
United States

4021 Vernon Ave. S
St. Louis Park, MN 55416
United States

2715 Eugene Court
Fitchburg, WI 53711
United States

18411 Gray Stone Rd.
White Hall, MD 21161
United States

850 E. Franklin
Meridian, ID 83642
United States

MIL engages in client servicing, order taking and entry at these locations.

Alternative Physical Location(s) of Employees

In the event of an SBD that makes it impossible or impractical to use any or all of the company offices, MIL will move its staff from affected offices to the closest of its unaffected office locations. In the case of a power outage, MIL has a generator available to power its facilities. Delegated employees, along with a backup individual, are trained in the generator's use.

If MIL's other office locations are not available, it will move the firm operations to:

542 Nw University Blvd
Suite B102
Port St Lucie, FL 34986
United States
7728074628

An additional alternate location is:

650 Sw Bittern Street
Palm City, FL 34990
United States
3215740450

Clients' Access to Funds and Securities

MIL does not maintain physical custody of clients' funds or securities, which are maintained at its brokerage firm. In the event of an internal or external SBD, if telephone service and internet service are available, MIL's investment adviser representatives (IARs) will take customers' orders or instructions from its alternative locations, phone numbers, websites or alternative email addresses and contact its brokerage firm on their behalf. If internet access is available, MIL will post on its website and Facebook, Twitter, LinkedIn, Friendster and YouTube that clients may access their funds and securities by contacting it.

Data Back-Up and Recovery (Hard Copy and Electronic)

MIL maintains its primary hard copy books and records and its electronic records at its primary office.

The firm's CCO is responsible for the maintenance of these books and records. MIL maintains the following document types and forms that are not transmitted to its brokerage firm: Investment Policy Statements, Client Contracts and other related documents.

The firm backs up its electronic records daily by online digital backup and local digital backup and keeps a copy at Amazon Web Services and External Hard Drive Located at Port St Lucie Location.

In the event of an internal or external SBD that causes the loss of its paper records, MIL will physically recover them from its back-up site(s). If its primary site is inoperable, MIL will continue operations from its back-up site or an alternate location. For the loss of electronic records, it will either physically recover the storage media or electronically recover data from its back-up site(s). If its primary site is inoperable, MIL will continue operations from its back-up site or an alternate location. MIL obtains the Business Continuity Plans of its electronic storage partners for access to its records in case of a regional event.

Operational Assessments

Operational Risk

In the event of an SBD, MIL will immediately identify what means will permit it to communicate with its clients, employees, critical business constituents, and regulators. Although the effects of an SBD will determine the means of alternative communication, the communications options MIL will employ will include its website, telephone voice mail, secure email, etc. In addition, MIL will retrieve its key activity records as described in the section above, Data Back-Up and Recovery (Hard Copy and Electronic). Employees will establish contact with the firm's Emergency Contacts and communicate key firm directives as they apply to operating the business whether it be from a new location, each employee's residence or an alternative regional location with access to a different power grid from the principal office.

Mission Critical Systems

MIL's "mission critical systems" are those that ensure client communication, access to client accounts and trading systems. More specifically, these systems include the office computer systems.

MIL has primary responsibility for establishing and maintaining its business relationships with its clients. MIL's brokerage firms/custodians provide the execution, comparison, allocation, clearance and settlement of securities transactions as well as the maintenance of customer accounts, access to customer accounts, and the delivery of funds and securities.

MIL's brokerage firm/custodian contracts provide that the brokerage firms/custodians will maintain business continuity plans and the capacity to execute those plans.

MIL's brokerage firms/custodians represent that they back up MIL's records at remote sites. MIL's brokerage firms/custodians represent that they operate back-up operating facilities in geographically separate areas with the capabilities to conduct the same volume of business as their primary sites. They have also confirmed the effectiveness of their back-up arrangements to recover from a wide scale disruption by testing.

Recovery-time objectives provide concrete goals to plan for and test against. They are not, however, hard and fast deadlines that must be met in every emergency situation, and various external factors surrounding a disruption, such as time of day, scope of disruption, and status of critical infrastructure—particularly telecommunications—can affect actual recovery times. Recovery refers to the restoration of clearing and settlement activities after a wide-scale disruption; resumption refers to the capacity to accept and process new transactions and payments after a wide-scale disruption. The recovery times for custodians are expected to be consistent with the recovery time indicated in the specific custodian's business continuity plan or other relevant documentation. However, the firm will not typically have access to the custodian's business continuity plan and recovery times will of course differ depending on the specific system affected. Please see "Custodian and Brokerage Firm Contacts" above.

The Firm's Mission Critical Systems

Trading

MIL uses the electronic order entry system provided by its custodian or another third party to enter trading activity and transactions. If electronic means are not available, MIL may place orders by fax or telephone, in which case order tickets will still be maintained.

In the event of an internal SBD, MIL will enter and send records to its brokerage firm by the fastest alternative means available. In the event of an external SBD, MIL will maintain the order in electronic or paper format, and deliver the order to the brokerage firm by the fastest means available when it resumes operations. In addition, during an internal SBD, MIL may need to refer its clients to deal directly with its brokerage firm for order entry.

Client Account Information

MIL currently accesses client account information via its brokerage firm's website. In the event of an internal SBD, MIL would access client information via fax correspondence, alternate phone systems, etc. MIL may relocate to its alternative business location(s) if access to the brokerage firm website can be accomplished.

Alternate Communications with Clients, Employees, and Regulators

Clients

MIL now communicates with its clients using the telephone, email, its website, fax, U.S. mail, and in person visits at MIL's or at the other's location. In the event of an SBD, MIL will assess which means of communication are still available to it, and use the means closest in speed and form (written or oral) to the means that it has used in the past to communicate with the other party. For example, if MIL has communicated with a party by email but the Internet is unavailable, MIL will call the party on the telephone and follow up and where a record is needed with paper copy in the U.S. mail. In the event of an anticipated significant regional business disruption, MIL will communicate to its clients in advance how to establish contact with it and its personnel or brokerage and custodian prior to the disruptive event occurrence.

Employees

MIL now communicates with its employees using the telephone, email, and in person. In the event of an SBD, MIL will assess which means of communication are still available to it, and use the means closest in speed and form (written or oral) to the means that it has used in the past to communicate with the other party. In the event of key employees being unable to perform their job functions, immediately and for any time period afterwards, MIL will delegate, if possible, those key functions to other employees.

Regulators

MIL communicates with its regulators using the telephone, email, fax, U.S. mail, and in person. In the event of an SBD, MIL will assess which means of communication are still available to it, and use the means closest in speed and form (written or oral) to the means that it has used in the past to communicate with the other party.

Regulatory Reporting

MIL is subject to regulation by the Securities and Exchange Commission (SEC). MIL now files reports with its regulators using the IARD System. In the event of an SBD, MIL will check with the SEC to determine which means of filing are still available to it, and use the means closest in speed and form (written or oral) to its previous filing method. In the event that MIL cannot contact its regulators, it will continue to file required reports using the communication means available to it and forward those reports at the earliest opportunity.

Regulatory Contact:

Office of Compliance Inspections and Examinations
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549
(202) 551-6200

Investment Adviser Regulation Office, Division of Investment Management
U.S. Securities and Exchange Commission
100 F Street, N.E.

Washington, DC 20549
(202) 551-6999

Death of Key Personnel

The following personnel are identified as "Key Personnel" without which it would be difficult or impossible to continue operating the firm and/or properly service clients:

Michael Terrio	President

If some event made it impossible for any person listed above able to continue to service the firm, MIL would implement the following succession plan:

Current team members will notify all clients and proper regulation authorities. Team will then meet to discuss if the firm will continue operations, sell the practice, or dissolve the firm.

In case of death of any key personnel, the following will assume the responsibility to make contact with the clients of the firm in the most efficient manner possible and as soon as possible to allow clients to access their accounts. If a business succession plan is to be implemented, clients will be contacted to obtain consent prior to any assignment of their advisory management contracts with this firm to a successor firm.

Cassandra Ottofaro	Director of Operations

Updates and Annual Review

MIL will update this plan whenever it has a material change to its operations, structure, business or location or to those of its brokerage firm. In addition, MIL will review this BCP annually, to modify it for any changes in its operations, structure, business, or location or those of its brokerage firm.

Approval & Signature

Supervisor Approval

Approve the firm's Business Continuity Plan (BCP) program by signing below.

I have approved this Business Continuity Plan as reasonably designe d to enable MIL to meet its obligations to clients in the event of a Significant Business Disruption.

Signed:

Officer Name and Title:	
Supervisor Signature	Date

Code of Ethics Statement

Background

In accordance with SEC regulations, Motiv8 Investments LLC ("MIL") has adopted a code of ethics to:

- Set forth standards of conduct expected of all supervised persons (including compliance with federal securities laws);
- Safeguard material non-public information about client transactions; and
- Require "access persons" to report their personal securities transactions. In addition, the activities of an investment adviser and its personnel must comply with the broad antifraud provisions of Section 206 of the Advisers Act.

Introduction

As an investment advisory firm, MIL has an overarching fiduciary duty to its clients. They deserve its undivided loyalty and effort, and their interests come first. MIL has an obligation to uphold that fiduciary duty and see that its personnel do not take inappropriate advantage of their positions and the access to information that comes with their positions.

MIL holds its supervised persons accountable for adhering to and advocating the following general standards to the best of their knowledge and ability:

- Always place the interest of the clients first and never benefit at the expense of advisory clients;
- Always act in an honest and ethical manner, including in connection with the handling and avoidance of actual or potential conflicts of interest between personal and professional relationships;
- Always maintain the confidentiality of information concerning the identity of security holdings and financial circumstances of clients;
- Fully comply with applicable laws, rules and regulations of federal, state and local governments and other applicable regulatory agencies; and
- Proactively promote ethical and honest behavior with MIL including, without limitation, the prompt reporting of violations of, and being accountable for adherence to, this Code of Ethics.

Failure to comply with MIL's Code of Ethics may result in disciplinary action, up to and including termination of employment.

Definitions

"Access Person" includes any supervised person who has access to non-public information regarding any client's purchase or sale of securities, or non-public information regarding the

portfolio holdings of any client account or any fund the adviser or its control affiliates manage, or is involved in making securities recommendations to clients, or has access to such recommendations that are non-public. All of the firm's directors, officers, and partners are presumed to be access persons.

"Advisers Act" means Investment Advisers Act of 1940.

"Adviser" means MIL.

"Beneficial ownership" shall be interpreted in the same manner as it would be under Rule 16a-1(a)(2) under the Securities Exchange Act of 1934: a direct or indirect "pecuniary interest" that is held or shared by a person directly or indirectly in a security, through any contract, arrangement, understanding, relationship or otherwise, which offers the opportunity to directly or indirectly profit or share in any profit from a transaction. An access person is presumed to have beneficial ownership of any family member's account.

"CCO" means Chief Compliance Officer per rule 206(4)-7 of the Investment Advisers Act of 1940.

For the purposes of this Code of Ethics, a **"Conflict of Interest"** will be deemed to be present when an individual's private interest interferes in any way, or even appears to interfere, with the interests of the adviser as a whole.

"Initial Public Offering" means an offering of securities registered under the Securities Act of 1933, the issuer of which, immediately before the registration, was not subject to the reporting requirements of Section 13 or Section 15(d) of the Securities Exchange Act of 1934.

"Investment personnel" means any employee of the investment adviser or of any company in a control relationship to the investment adviser who, in connection with his or her regular functions or duties, makes or participates in making recommendations regarding the purchase or sale of securities for clients.

"Limited Offering" means an offering that is exempt from registration under the Securities Act of 1933 pursuant to Section 4(2) or Section 4(6) thereof or pursuant to Rule 504, Rule 505 or Rule 506 thereunder.

"Reportable Security" means any note, stock, treasury stock, security future, bond, debenture, evidence of indebtedness, certificate of interest or participation in any profit-sharing agreement, collateral-trust certificate, preorganization certificate or subscription, transferable share, investment contract, voting-trust certificate, certificate of deposit for a security, fractional undivided interest in oil, gas, or other mineral rights, any put, call, straddle, option, or privilege on any security (including a certificate of deposit) or on any group or index of securities (including any interest therein or based on the value thereof), or any put, call, straddle, option, or privilege entered into on a national securities exchange relating to foreign currency, or, in general, any interest or instrument commonly known as a "security", or any certificate of interest or participation in, temporary or interim certificate for, receipt for, guaranty of, or warrant or right to subscribe to or purchase any of the foregoing, except:

- Direct obligations of the Government of the United States;
- Bankers' acceptances, bank certificates of deposit, commercial paper and high quality short-term debt instruments, including repurchase agreements;
- Shares issued by money market funds;
- Shares issued by open-end funds other than reportable funds;
- Shares issued by unit investment trusts that are invested exclusively in one or more open-end funds, none of which are reportable funds.

"Supervised Persons" means directors, officers, and partners of the adviser (or other persons occupying a similar status or performing similar functions); employees of the adviser; and any other person who provides advice on behalf of the adviser and is subject to the adviser's supervision and control.

Compliance Procedures

Compliance with Laws and Regulations

Supervised persons of MIL must comply with applicable state and federal securities laws. Specifically, supervised persons are not permitted, in connection with the purchase or sale, directly or indirectly, of a security held or to be acquired by a client:

- To defraud such client in any manner;
- To mislead such client, including making any statement that omits material facts;
- To engage in any act, practice or course of conduct that operates or would operate as a fraud or deceit upon such client;
- To engage in any manipulative practice with respect to such client;
- To engage in any manipulative practice with respect to securities, including price manipulation.

Prohibited Purchases and Sales

Insider Trading

Illegal insider trading refers generally to buying or selling a security, in breach of a fiduciary duty or other relationship of trust and confidence, while in possession of material, non-public information about the security. The SEC defines information as material if "there is a substantial likelihood that a reasonable shareholder would consider it important in making an investment decision." Information is non-public if it has not been disseminated in a manner making it available to investors generally.

MIL strictly prohibits trading personally or on the behalf of others, directly or indirectly, based on the use of material, non-public or confidential information. MIL additionally prohibits the communicating of material non-public information to others in violation of the law. Employees who are aware of the misuse of material non-public information should report such to the CCO.

This policy applies to all of MIL's employees and associated persons without exception.

Please note that it is the SEC's position that the term "material non-public information" relates not only to issuers but also to the adviser's securities recommendations and client securities holdings and transactions.

Initial Public Offerings (IPOs)

No access person or other employee may acquire, directly or indirectly, *beneficial ownership* in any securities in an *Initial Public Offering* without first obtaining the prior approval of the CCO.

Limited or Private Offerings

No access person or other employee may acquire, directly or indirectly, beneficial ownership in any securities in a Limited or Private Offering without first obtaining the prior approval of the CCO. *Investment personnel* are required to disclose such investment to any client considering an investment in the issuer of such Limited or Private Offering.

Miscellaneous Restrictions

Blackout Periods

From time to time, representatives of MIL may buy or sell securities for themselves at or around the same time as clients. This may provide an opportunity for representatives of MIL to buy or sell securities before or after recommending securities to clients resulting in representatives profiting off the recommendations they provide to clients. Such transactions may create a conflict of interest. When similar securities are being bought or sold, MIL employees will either transact clients' transactions before their own or will transact alongside clients' transactions in block or bunch trades.

Margin Accounts

Investment personnel are prohibited from purchasing securities on margin, unless pre-cleared by the CCO.

Option Transactions

Investment personnel are prohibited from purchasing options, unless pre-cleared by the CCO.

Short Sales

Investment personnel are prohibited from selling any security short, in their own accounts, that is owned by any client of the firm, except for short sales "against the box", unless pre-cleared by the CCO.

Short-Term Trading

Securities held in client accounts may not be purchased and sold, or sold and repurchased, within 30 calendar days by investment personnel. The CCO may, for good cause shown, permit a short-term trade, but shall record the reasons and grant of permission with the records of the Code.

Prohibited Activities

Conflicts of Interest

MIL has an affirmative duty of care, loyalty, honesty, and good faith to act in the best interest of its clients. A conflict of interest may arise if a person's personal interest interferes, or appears to interfere, with the interests of MIL or its clients. A conflict of interest can arise whenever a person takes action or has an interest that makes it difficult for him or her to perform his or her duties and responsibilities for MIL honestly, objectively and effectively.

While it is impossible to describe all of the possible circumstances under which a conflict of interest may arise, listed below are situations that most likely could result in a conflict of interest and that are prohibited under this Code of Ethics:

- Access persons may not favor the interest of one client over another client (e.g., larger accounts over smaller accounts, accounts compensated by performance fees over accounts not so compensated, accounts in which employees have made material personal investments, accounts of close friends or relatives of supervised persons). This kind of favoritism would constitute a breach of fiduciary duty;
- Access persons are prohibited from using knowledge about pending or currently considered securities transactions for clients to profit personally, directly or indirectly, as a result of such transactions, including by purchasing or selling such securities.

Access persons are prohibited from recommending, implementing or considering any securities transaction for a client without having disclosed any material beneficial ownership, business or personal relationship, or other material interest in the issuer or its affiliates, to the CCO. If the CCO deems the disclosed interest to present a material conflict, the investment personnel may not participate in any decision-making process regarding the securities of that issuer.

Political and Charitable Contributions

Supervised persons that may make political contributions, in cash or services, must report each such contribution to the CCO who will compile and report thereon as required under relevant regulations. Supervised persons are prohibited from considering the adviser's current or anticipated business relationships as a factor in soliciting political or charitable donations.

Gifts and Entertainment

Supervised persons shall not accept inappropriate gifts, favors, entertainment, special accommodations, or other things of material value that could influence their decision-making or

make them feel beholden to a person or firm. Similarly, supervised persons shall not offer gifts, favors, entertainment or other things of value that could be viewed as overly generous or aimed at influencing decision-making or making a client feel beholden to the firm or the supervised person.

No supervised person may receive any gift, service, or other thing of more than de minimis value from any person or entity that does business with or on behalf of the adviser. No supervised person may give or offer any gift of more than de minimis value to existing clients, prospective clients, or any entity that does business with or on behalf of the adviser. The annual receipt of gifts from the same source valued at $100 or less shall be considered de minimis. Additionally, the receipt of an occasional dinner, a ticket to a sporting event or the theater, or comparable entertainment also shall be considered to be of de minimis value if the person or entity providing the entertainment is present.

All gifts, given and received, will be recorded in a log (see Sample 10).

No supervised person may give or accept cash gifts or cash equivalents to or from a client, prospective client, or any entity that does business with or on behalf of the adviser.

Bribes and kickbacks are criminal acts, strictly prohibited by law. Supervised persons must not offer, give, solicit or receive any form of bribe or kickback.

Service on Board of Directors

Supervised persons shall not serve on the board of directors of publicly traded companies absent prior authorization by the CCO. Any such approval may only be made if it is determined that such board service will be consistent with the interests of the clients and of MIL, and that such person serving as a director will be isolated from those making investment decisions with respect to such company by appropriate procedures. A director of a private company may be required to resign, either immediately or at the end of the current term, if the company goes public during his or her term as director.

Confidentiality

Supervised persons shall respect the confidentiality of information acquired in the course of their work and shall not disclose such information, except when they are authorized or legally obliged to disclose the information. They may not use confidential information acquired in the course of their work for their personal advantage. Supervised persons must keep information about clients (including former clients) in strict confidence, including the client's identity (unless the client consents), the client's financial circumstances, the client's security holdings, and advice furnished to the client by the firm.

Pre-Clearance

For any activity where it is indicated in the Code of Ethics that pre-clearance is required, the following procedure must be followed:

- Pre-clearance requests must be submitted by the requesting supervised person to the CCO in writing. The request must describe in detail what is being requested and any relevant information about the proposed activity;
- The CCO will respond in writing to the request as quickly as is practical, either giving an approval or declination of the request, or requesting additional information for clarification;
- Pre-clearance authorizations expire 48 hours after the approval, unless otherwise noted by the CCO on the written authorization response;
- Records of pre-clearance requests and responses will be maintained by the CCO for monitoring purposes and ensuring the Code of Ethics is followed.

Personal Securities Reporting and Monitoring

Holdings Reports

Every access person shall, no later than ten (10) days after the person becomes an access person and annually thereafter, file a holdings report containing the following information (see Sample 8):

- The title, exchange ticker symbol or CUSIP number (when available), type of security, number of shares and principal amount of each Reportable Security in which the access person has any direct or indirect beneficial ownership when the person becomes an access person;
- The name of any broker, dealer or bank with whom the access person maintains an account in which any securities are held for the direct or indirect benefit of the access person;
- The date that the report was submitted by the access person.

The information in the holdings report must be current as of a date no more than forty-five (45) days prior to the date the report was submitted.

Transaction Reports

Every access person shall, no later than 30 days after the end of calendar quarter, file transaction reports containing the following information (see Sample 9):

- For each transaction involving a Reportable Security in which the access person had, or as a result of the transaction acquired, any direct or indirect beneficial interest, the access person must provide the date of the transaction, the title, exchange ticker symbol or CUSIP number (when available), type of security, the interest rate and maturity date (if applicable), number of shares and principal amount of each involved in the transaction;
- The nature of the transaction (e.g., purchase, sale);
- The price of the security at which the transaction was effected;
- The name of any broker, dealer or bank with or through the transaction was effected;
- The date that the report was submitted by the access person.

Access persons may use duplicate brokerage confirmations and account statements in lieu of submitting quarterly transaction reports, provided that the required information is contained in those confirmations and statements.

Report Confidentiality

Holdings and transaction reports will be held strictly confidential, except to the extent necessary to implement and enforce the provisions of the code or to comply with requests for information from government agencies.

Exceptions to Reporting Requirements

Access persons do not need to submit:

- Any report with respect to securities held in accounts over which the access person had no direct or indirect influence or control;
- A transaction report with respect to transactions effected pursuant to an automatic investment plan;
- A transaction report if the report would duplicate information contained in broker trade confirmations or account statements that the firm holds in its records so long as it receives the confirmations or statements no later than 30 days after the end of the applicable calendar quarter.

Review of Personal Securities

MIL is required by the Advisers Act and applicable state law to review access persons' initial Holdings report and to do so annually thereafter. Transaction reports are reviewed at least quarterly. The CCO is responsible for reviewing these transactions and holdings reports. The CCO's personal securities transactions and reports shall be reviewed by designated firm personnel.

Access persons are subject to the reporting requirements detailed above for personal accounts and all accounts in which they have any beneficial ownership in any *reportable securities*. For clarification, these terms are defined in this Code.

Single Access Person Advisers

If at any time MIL only has one access person, the person will not be required to submit reports but will maintain records of all holdings and transactions. It is assumed that all trades by the sole access person are reviewed as the trades are entered.

Certification of Compliance

Initial Certification

The firm is required to provide supervised persons with a copy of this Code. Supervised persons are to certify in writing via an attestation statement (see Sample 1) that they have: (a) received a copy of this Code; (b) read and understand all provisions of this Code; and (c) agreed to comply with the terms of this Code.

Acknowledgement of Amendments

The firm must provide supervised persons with any amendments to this Code and supervised persons must submit a written acknowledgement that they have received, read, and understood the amendments to this Code.

Annual Certification

Supervised persons must annually certify via an attestation statement that they have read, understood, and complied with this Code of Ethics and that the supervised person has made the reports required by this code and has not engaged in any prohibited conduct.

The CCO shall maintain records of these certifications of compliance (see Sample 1).

Reporting Violations and Whistleblower Provisions

Supervised persons must report violations of the firm's Code of Ethics promptly to the CCO. If the CCO is involved in the violation or is unreachable, supervised persons may report directly to the CCO's supervisor or other firm principal. Reports of violations will be treated confidentially to the extent permitted by law and investigated promptly and appropriately. Persons may report violations of the Code of Ethics on an anonymous basis. Examples of violations that must be reported include (but are not limited to):

- Noncompliance with applicable laws, rules, and regulations;
- Fraud or illegal acts involving any aspect of the firm's business;
- Material misstatements in regulatory filings, internal books and records, clients records or reports;
- Activity that is harmful to clients, including fund shareholders;
- Deviations from required controls and procedures that safeguard clients and the firm; and
- Violations of the firm's Code of Ethics.

No retribution will be taken against a person for reporting, in good faith, a violation or suspected violation of this Code of Ethics.

Retaliation against an individual who reports a violation is prohibited and constitutes a further violation of the Code.

Compliance Officer Duties

Training and Education

CCO shall be responsible for training and educating supervised persons regarding this Code. Training will occur periodically as needed and supervised persons are required to attend any training sessions or read any applicable materials.

Recordkeeping

CCO shall ensure that MIL maintains the following records in a readily accessible place:

- A copy of each Code of Ethics that has been in effect at any time during the past five years;
- A record of any violation of the Code and any action taken as a result of such violation for five years from the end of the fiscal year in which the violation occurred;
- A record of written acknowledgements and/or attestation statements of receipt of the Code and amendments for each person who is currently, or within the past five years was, a supervised person. These records must be kept for five years after the individual ceases to be a supervised person of the firm;
- Holdings and transactions reports made pursuant to the code, including any brokerage confirmation and account statements made in lieu of these reports;
- A list of the names of persons who are currently, or within the past five years were, access and/or supervised persons;
- A record of any decision and supporting reasons for approving the acquisition of securities by access or supervised persons in initial public offerings and limited offerings for at least five years after the end of the fiscal year in which approval was granted;
- A record of any decisions that grant employees or access or supervised persons a waiver from or exception to the Code.

Annual Review

CCO shall review at least annually the adequacy of this Code of Ethics and the effectiveness of its implementation and make any changes needed.

Sanctions

Any violations discovered by or reported to the CCO shall be reviewed and investigated promptly, and reported through the CCO to the supervisor or other firm principal. Such report shall include the corrective action taken and any recommendation for disciplinary action deemed appropriate by the CCO. Such recommendation shall be based on, among other things, the severity of the infraction, whether it is a first or repeat offense, and whether it is part of a pattern of disregard for the letter and intent of this Code of Ethics. Upon recommendation of the CCO, the supervisor may impose such sanctions for violation of this Code of Ethics as it deems appropriate, including, but not limited to:

- Letter of censure;
- Suspension or termination of employment;

- Reversal of a securities trade at the violator's expense and risk, including disgorgement of any profit;
- In serious cases, referral to law enforcement or regulatory authorities.

Diminished Capacity & Elder Financial Abuse Policy

Diminished Capacity

Increased life spans bring an increased chance that clients may suffer from some sort of diminished capacity (an impaired mental state or condition). Diminished capacity may be the result of trauma, intoxication, disease/disorder (e.g., dementia, Alzheimer's disease, bipolar disorder), age-related memory changes, or other changes to the client. Signs of diminished capacity may include:

- Memory loss (is the client repeating orders or questions?)
- Disorientation (is the client confused about time, place or simple concepts?)
- Difficulty performing simple tasks
- Significantly poorer judgment than in the past
- Drastic mood swings
- Difficulty with abstract thinking

As clients reach a certain age, the effects of diminished capacity may begin to impact financial capacity. Financial capacity can be defined as the ability to independently manage one's financial affairs in a manner consistent with personal self-interest.

Elder Financial Abuse

Elder financial abuse spans a broad spectrum of conduct including but not limited to: forging signatures; getting an individual to sign over financial ownership of property; taking assets without consent; obtaining a power of attorney (POA) through deception, coercion, or undue influence; using property or possessions without permission; promising various care in exchange for money or property and not following through; perpetrating scams; or engaging in other deceptive acts. While MIL may not be aware of many of these situations at large, supervised persons may suspect such situations when the assets upon which the firm is advising become the targets of these acts. These situations often occur along with the onset of diminished capacity. Signs of elder financial abuse may include:

- Increased reluctance to discuss financial matters
- Drastic shifts in investment style
- Abrupt changes in wills, trusts, POAs, or beneficiaries
- Concern or confusion about missing funds
- Atypical or unexplained withdrawals, wire transfers or other changes in financial situation
- Appearance of insufficient care despite significant wealth

As a fiduciary to clients, MIL will research the options for reporting of these situations to the proper authorities. Most jurisdictions have the option of using a Department of Social Services (or other similar department) anonymous "tip line" to report possible elder financial abuse issues.

Firm Policy

MIL recognizes its responsibility to work with clients and any necessary family, friends, or medical personnel the client has named in order to move forward if the client's financial capacity has been compromised. In order to address these circumstances, MIL has adopted the following policies:

- MIL will ascertain whether clients have created a living will (durable power of attorney) directed at the client's financial interest in the event financial capacity becomes compromised.
- MIL will ask all clients to provide the name and contact information of at least one family member (ideally), trusted professional, or non-relative client "advocate" to contact in the event its suspect any irregular activities that may be related to diminished capacity or elder financial abuse (see Sample 11).
- MIL will request signed permission from client to discuss any suspicious activity in client's accounts with approved third party(ies) if diminished capacity or elder financial abuse is suspected.
- If a supervised person suspects a client may be suffering from diminished capacity or elder financial abuse, then the supervised person shall immediately inform the CCO or supervisor. MIL will document the interaction with the client that prompted the suspicion in the client's file or in a separate file that contains details of all reported suspicions of diminished capacity or elder financial abuse. Until the suspicion is resolved, supervised persons will not meet with the client alone and will continue to thoroughly document all client interactions.
- In the event the financial capacity of the client has deteriorated beyond the point of effective and ethical investment advice and a POA, guardian, or trustee has not been appointed, MIL will terminate the investment advisory relationship and report the circumstances to the designated family member, client advocate, or approved third party or, if none, to the appropriate authority in the applicable jurisdiction (e.g., adult protective services agency).

Staff Training

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

Privacy of Client Information

Information Collected and Shared

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

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

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

- With specific third parties as requested by the client (see Sample 11);
- For everyday business purposes – such as to process client transactions, maintain client account(s), respond to court orders and legal investigations, or report to credit bureaus;
- For marketing by MIL – to offer MIL's products and services to clients;
- For joint marketing with other financial companies;
- For affiliates' everyday business purposes – information about client transactions and experience; or
- For non-affiliates to market to clients (only where allowed).

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

Storing Client Information

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

In addition to MIL's listed access persons, any IT persons or other technical consultants employed at the firm may also have access to non-public client information at any time. An on-site or off-site server that stores client information, third-party software that generates statements or performance reports, or third-party client portals designed to store client files all hold the potential for a breach of non-public client information.

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

Identity Theft Red Flags

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

SAFEGUARDING IDENTIFYING INFORMATION

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

POTENTIAL CAUSES OF IDENTITY INFORMATION BREACHES

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

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

Staff Training

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

Client Records

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

MIL takes the privacy and confidentiality of all its clients and personnel very seriously. It will continue to make, and document, any changes needed to promote the security of client information. Additional safeguards are described in the Cybersecurity & Information Security Policy section of this manual.

Cyber Security & Information Security Policy

Non-Public Information (NPI)

In the course of conducting its investment advisory business, MIL has access to clients' personally identifiable financial information, which constitutes *non-public personal information* ("NPI"). NPI generally includes any:

- Information that a consumer provides in order to obtain a financial service or product from MIL;
- Information about a consumer resulting from transactions involving a financial service or product; or
- Information MIL otherwise may obtain about a consumer in connection with providing a financial service or product to that consumer.

This encompasses a broad range of data when it comes to MIL's clients, who are generally considered to be "consumers" under Regulation S-P. As a registered investment adviser, MIL is generally required to adopt written policies and procedures reasonably designed to protect the security and confidentiality of client information and records.

Safeguarding clients' confidential information is a primary focus of MIL's cybersecurity program. MIL appreciates that a cybersecurity data breach involving NPI can lead not only to regulatory issues, but also to loss of client trust and significant reputational damage to MIL.

National Institute of Technology (NIST) Framework

MIL has appointed Michael Terrio as the firm's Chief Information Security Officer ("CISO"). The CISO is responsible for managing MIL's information security program. To help establish and implement MIL's information security program, the CISO utilizes the National Institute of Technology ("NIST") cybersecurity framework. NIST is a government agency within the U.S. Department of Commerce that fosters cybersecurity research, education, and collaboration.

As such, MIL's information security policy is modeled on the **NIST cybersecurity framework** which includes five functions:

1. Identify
2. Protect
3. Detect
4. Respond
5. Recover

These five NIST functions serve as the primary pillars of the MIL information security program. These five functions also help MIL to address particular areas of current regulatory focus, which include:

- Governance and Risk Assessment
- Access Rights and Controls
- Data Loss Prevention
- Vendor Management
- Training
- Incident Response

MyRIACompliance Cybersecurity Platform

MIL utilizes the MyRIACompliance cybersecurity program to help implement and maintain its information security program. Cybersecurity awareness training, testing, and documentation for MIL staff is delivered via the MyRIACompliance platform.

Role of Each Staff Member

MIL recognizes that many investment adviser cybersecurity events resulting in the exposure of NPI begin with the inadvertent action of a staff member. While MIL has implemented an information security policy designed to protect against the exposure of sensitive client information, each staff member of MIL must take a proactive approach to helping MIL and the CISO implement the information security program.

To help educate and train each staff member, all MIL staff members will be required to do the following via the MyRIACompliance platform:

- Carefully review and attest to understanding this information security policy;
- Complete information security awareness training and testing; and
- Report any potential suspicious activity or conduct.

Any staff member who has discovered or experienced a *potential* cybersecurity incident should immediately inform MIL's CISO via MyRIACompliance in order to properly investigate the incident. MIL's personnel are the firm's first and best line of defense when it comes to cybersecurity.

IDENTIFY

The **identify** function helps MIL to identify relevant human, technology system, and third party vendor risks.

Inventory of Technology Infrastructure

On an annual basis, the CISO of MIL will utilize MyRIACompliance to make an inventory of the following:

- Physical devices and systems (computers, servers, etc.);

- Software platforms and applications (email applications, file management, etc.);
- Systems that house client data; and
- Third-party contractors that have access to these systems, platforms, etc.

MIL utilizes cloud-based technology systems, which it believes provide increased information security capabilities including:

- Ability to leverage the established infrastructure of trusted technology industry leaders; and
- Improved system alert capabilities, including better user activity logging and alerts related to unusual user activity.

MIL also recognizes that cloud-based technology creates a greater reliance on passwords and user login security. In particular, MIL understands that certain users with administrative access to the firm's cloud-based technology systems may pose even greater risk given their expanded access to sensitive client data. As such, MIL has designed and will continue to further develop information security policies with this increased risk as a focus.

Inventory of Staff Devices and System Access Levels

On an annual basis, the CISO of MIL will utilize MyRIACompliance to make an inventory of the following:

- Each staff member's physical devices (computers, mobile devices, etc.);
- Each staff member's access level to internal systems; and
- Each staff member's access level to third-party systems.

The CISO will regularly review the system access levels for personnel to ensure that each MIL staff member only has the necessary level of access to each system in order to perform that individual's job.

PROTECT

The **protect** function helps MIL create safeguards to help prevent, limit, or contain the impact of a cybersecurity incident or attack.

Security of Technology Infrastructure

MIL has implemented the following firm-wide information security polices to help prevent unauthorized access to sensitive client data:

- All computers used to access client data will have antivirus software installed. In addition, the antivirus software will have an active subscription and all updates will be scheduled to automatically install.
- All staff will utilize devices with up to date operating system software with all security patch and other software updates set to automatically install

- All staff workstations (e.g. desktop, laptop, mobile device) will be locked when the device is not in use
- All staff workstations (e.g. desktop, laptop, mobile device) will be shut down completely at the end of each workday
- All staff workstations (e.g. desktop, laptop, mobile device) will use proper data encryption when possible
- All staff mobile devices used to access work email and files will be password protected and will have the capability to be remotely wiped if lost or stolen
- All staff members are prohibited from accessing MIL systems from unsecured internet connections

All staff should immediately alert the CISO of any suspicious behavior or potential incidents.

User Access Rights and Controls

MIL has implemented the following firm-wide user access privilege polices to help prevent unauthorized access to sensitive client data:

- Staff members will only have access to systems deemed necessary by the CISO;
- Each new staff member's login credentials will be created by the CISO;
- Staff members, besides the CISO or other designated personnel, will not have administrative privileges on systems unless deemed necessary and approved by the CISO; and
- Upon a staff member's departure or termination, the CISO will immediately remove the former staff member's access to all firm systems.
- The CISO will use MyRIACompliance to keep a record of former staff members and the date that access to each firm system was terminated for such former staff member.

Staff members may request additional access to systems by contacting the CISO.

Prevention of Unauthorized Funds Transfers

MIL recognizes the risk of client impersonation attacks and the need to validate the identity of its clients before transmitting funds. For example, after gaining unauthorized access to a client's email or financial account, a bad actor may then target MIL by impersonating the client in order to access the client's funds. Client impersonation campaigns are particularly dangerous to MIL because, given their financial profile, clients of MIL may be more likely targets for bad actors.

MIL has implemented the following firm-wide security polices to help prevent unauthorized funds transfers:

- Wire requests should be reviewed for suspicious behavior (e.g. time of request, atypical amount of request, etc.); and
- Clients must confirm all third party wire requests verbally. Wire requests may not be authorized solely via email

MIL is particularly aware of the risk caused by fraudulent emails, purportedly from clients, seeking to direct transfers of customer funds or securities and will train staff members to properly identify such fraudulent emails.

User Login Security

MIL has implemented the following firm-wide user login security polices to help prevent unauthorized access to sensitive client data:

- All staff passwords are required to meet or exceed the following guidelines. Each password must:
  - Contain both upper and lower case letters
  - Contain at least one number
  - Contain at least one special character
  - Be at least 10 characters in length
  - Not contain personal information such as pet names, birthdates, or phone numbers
  - Not contain sequenced or repeated characters (e.g., 123456, abc123, etc.)
  - Not be similar to the username
- All staff are required to have unique passwords to access each technology system (e.g., desktop computer, CRM system, etc.)
- All staff are required to update passwords on a quarterly basis
- No passwords are allowed to be stored in writing on paper or on any system
- Staff members should not use the "remember password" feature of any application, including on web browsers
- Staff members should never share passwords with any other staff member or third party whether via email, phone, or text message
- When available, staff is required to utilize two-factor authentication

Password Management

MIL is aware of the risks and challenges in managing multiple, unique passwords to access technology systems. As such, MIL has implemented the following password manager tool to help safeguard and organize staff member login credentials: DUO, VPN. All staff members are required to:

- manage all user login credentials via the password manager
- utilize the password manager's two-factor authentication capabilities (as mentioned above)
- follow all user login security password policies as outlined above when establishing their "master password" for the password manager

Social Engineering Protection

Sophisticated bad actors looking to gain access to MIL's sensitive information may target particular staff members personally via a cyber attack method called social engineering. In such an attack, cyber criminals will research the individual staff member online, looking for publicly available information that may help them answer the staff member's personal security questions, decipher a username and password, or launch an email phishing attack specifically targeted at what they know about the individual.

As such, all staff members are instructed not to disclose personal information on social media websites. Such information includes but is not limited to:

- Birthdate
- Place of birth
- Place of wedding
- Name of high school
- Name of elementary school
- Best friend's name
- Name of favorite pet
- Name of favorite drink
- Name of favorite song
- Mother's maiden name
- Make and model of first car
- Favorite color
- Name of favorite teacher

In addition, staff member should be aware of these best practices:

- Do not make personal social media profiles accessible to the public
- Be cautious when accepting social media friend or connection requests
- Utilize less common online security questions
- Use different online security questions for different systems

Email Phishing

Email poses one of the greatest cybersecurity risks to MIL. Bad actors look to exploit this vulnerability using fake emails designed to look like legitimate correspondence or offers. Often, the "phishing" email directs MIL personnel to click on an attachment or link with the goal of either installing dangerous software (malware) on the individual's computer or stealing sensitive access information from the staff member, such as an email username or login credentials to one of MIL's software platforms.

MIL has implemented the following firm-wide email security polices to help prevent unauthorized access to sensitive client data:

- Staff should never open or download any email attachments from unknown senders;

- Staff should never open or download any email attachments from known senders that look suspicious or out of the ordinary;
- Staff should never directly click on or open any suspicious links sent in emails;
- Staff should not send sensitive client or NPI via unsecured email to clients;
- Staff should be acutely aware of how to identify attempted "phishing" emails seeking to obtain the staff member's user login credentials. Warning signs to look for include:
    - Bad spelling or poor grammar in the email subject or body text;
    - A company or website with which the staff member is not familiar;
    - The sender's email address does not match the display name;
    - The sender's email address is valid, but something looks suspicious;
    - An "urgent" or "action required" subject line; and
    - A suspicious sender email domain.

MIL understands the risks that email phishing poses to an investment adviser. A successful phishing attack is particularly dangerous for MIL because if hackers gain access to one of MIL's technology systems, they may also gain unauthorized access to sensitive, non-public client and company information. In addition, as discussed above, email phishing can lead to fraudulent wires or other unauthorized transfers of funds.

When a staff member receives a suspicious email, the CISO should be immediately alerted. The CISO will then determine next steps and communicate to other staff members if deemed appropriate.

Ransomware Attack Protection

In a ransomware attack, hackers look to access MIL data or even personal information, block access to that information, and hold the information "hostage" until a ransom is paid to unlock the data. Ransomware is a specific type of malware that, when installed on staff member's computer, encrypts the data on the computer or company network, preventing MIL from accessing the data without the requisite decryption key. Ransomware is often circulated via phishing emails and most commonly installed when an individual downloads a malicious file via an email attachment, email link, or web link.

As such, all MIL personnel should take the following precautions to help protect against a potential ransomware attack:

- Follow MIL's email use security and guidelines including:
    - Never open or download any email attachments from unknown senders
    - Never open or download any suspicious email attachments from known senders
    - Never directly click on or open any suspicious links sent in emails
- Never provide remote computer access to a third party unless the CISO approves the request

Safe Internet Browsing

MIL recognizes that with the prevalence of web-based applications and the need to consistently access the internet in personal and professional life, proper vigilance while browsing the

internet is essential. Malware, spyware, and other viruses can be unknowingly distributed to MIL staff members while browsing the internet if proper safeguards are not in place.

As such, all staff members should take the following steps:

- Only use a modern web browser, such as Google Chrome, Mozilla Firefox, or Microsoft Edge
- Disable the browser's autofill form completion feature
- Do not use the browser's "save password" feature
- Utilize the browser's pop-up window blocking feature
- Only browse on secure websites (look for *https://*)
- Be highly cautious before downloading files or applications online
- Keep all device operating system software updated
- Do not access file sharing websites unless authorized by CISO
- Do not use unsecured wireless internet connections

Clean Desk Policy

MIL recognizes that third parties, such as visitors or service providers, may have access to a staff member's office area during or after normal business hours.
As such, all MIL personnel should take the following steps throughout the day and before departing for the day to help secure their respective office areas:

- Securely store any physical client files
- Avoid the use of flash drives
- Shred sensitive client and firm documents when appropriate
- Promptly gather any documents that have been printed
- Never write down passwords
- Erase any white board or similar displays containing sensitive or confidential information

Preventing Unauthorized Office Access

MIL recognizes that sensitive client information may be accessible in the firm's office. Staff members should always exercise great caution before letting an unknown or unauthorized third party, such as unexpected vendor or former staff member, into the office.

In particular, staff should be mindful of "tailgating" - a classic type of physical security breach. In a tailgating incident, an individual is exploited when trying to extend a common courtesy by opening or holding the door for a visitor or uniformed vendor when entering the office. Unfortunately, this gesture can be exploited by potential bad actor attempting to gain unauthorized office access. As such, MIL staff should be cognizant of this possibility when entering and leaving the office.

Mobile Device Usage Guidelines

In order to help prevent unauthorized access to sensitive client and firm data, MIL permits the limited use of personal mobile devices only under the following firm-wide mobile device usage guidelines:

- Before utilizing a personal mobile device to access company systems, such as company email or CRM system, the device must be inspected and approved by the CISO to ensure proper security features are activated on the device.
- The mobile device's built-in password / passcode security feature must be activated at all times. If the staff member's mobile device does not offer a built-in password / passcode security feature, then the device is not permitted to be used to access company systems.
- Sensitive client or firm information should never be downloaded directly onto a personal mobile device, since that bypasses the additional password protection that cloud-based systems offer.
- If available, the mobile device's local or remote wipe security features(s) should be activated.
- In the event a mobile device used to access company systems is lost or stolen, the staff member should immediately alert the CISO.
- Before disposing of any mobile device used to access company systems, all data must be wiped from the mobile device.

Cybersecurity Travel Policy

MIL recognizes that staff members may need to travel as part of their job responsibilities, but that the risk of a cybersecurity incident is higher when traveling.

As such, all staff members should take the following steps before traveling:

- Any mobile device being used for travel to conduct MIL business should first be approved by the CISO
- Avoid bringing unnecessary mobile, tablet, or laptop devices
- Ensure the latest operating system updated and patches are installed on any mobile device that will be used
- Make sure all necessary file back-ups have been conducted

While traveling, staff member should take the following precautions:

- Make sure auto connectivity and Bluetooth features are disabled on all devices
- Do not use devices in a public manner that could expose sensitive information
- Never leave a device unattended in a public area
- Properly secure all devices before leaving a hotel room
- Avoid publicly accessible and shared computers
- Never connect to unsecured wireless networks
- Use a virtual private network (VPN) connection to access the internet before conducting business on behalf of MIL

Third Party Vendor Security and Diligence

MIL has implemented the following firm-wide third party vendor security and diligence polices and guidelines to help prevent unauthorized access to sensitive client data:

- All third party vendors that have physical access to the office and/or the firm's systems are required to enter into a non-disclosure agreement (NDA) before establishing a business relationship in order to protect sensitive client information; and
- Proper due diligence will be performed on all relevant technology vendors prior to establishing a business relationship and then again on at least an annual basis. This will include review of the vendor's:
    - information security policies;
    - disaster recovery policies; and
    - broader capabilities to ensure the vendor meets MIL's business and security needs.

All of this information will be stored and maintained in MIL's vendor diligence file.

Staff Training

All MIL personnel are required to complete mandatory cybersecurity awareness training and testing, delivered via the MyRIACompliance platform. Mandatory training topics include:

- Non-Public Information
- Preventing Identity Theft
- Email Phishing
- Social Engineering
- Ransomware Attacks
- Client Impersonation
- Safe Internet Browsing
- Password Best Practices
- Physical Security
- Cybersecurity while Traveling

The MyRIACompliance platform will provide training videos and quizzes that are required to be completed by all MIL staff.

New staff members will receive training, led by the CISO, within one (1) month of their initial hire date. The training conducted by the CISO will include the following topics:

- Review of the current Cybersecurity & Information Security Policy, including a note of any changes to the policy since the last training session;
- Review of any relevant information security incidents or suspicious activity;
- Review of how to identify potential "phishing" or fraudulent emails;
- Review of how to identify potential "ransomware" or similar attacks;
- Review of any relevant regulatory compliance issues; and
- Review of general information security best practices.

On an annual basis, MIL's CISO will conduct a firm-wide training session to ensure that all staff members are properly trained and equipped to implement the Cybersecurity & Information Security Policy.

DETECT

The detect function helps MIL to establish the framework to identify a potential cybersecurity vulnerability or event in a timely manner.

Testing

On a quarterly basis, MIL will test its current Cybersecurity & Information Security Policy and capabilities. The test conducted by the CISO will include the following activities:

- Ensure all staff members have proper system access privileges;
- Ensure all relevant software patches designed to address security vulnerabilities have been implemented on MIL's server; and
- Make a physical inspection of the office to ensure that all workstations have the proper security measures including:
    - Attempt to access a random sample of firm devices to ensure that proper passwords are in place to prevent access;
    - Observe staff members access systems to ensure that two-factor authentication has been activated;
    - Ensure staff members are not using the "remember password" feature of any application;
    - Ensure computers used to access client data have an antivirus software subscription; and
    - Ensure passwords are not visibly stored in writing on paper or on any system.
- *For its remote offices, the CISO will either perform directly or assign a delegate to perform the above-referenced physical inspection*.

Risk Assessment

On an annual basis, MIL will further test and evaluate its current Cybersecurity & Information Security Policy and capabilities. The test conducted by the CISO will include the following activities:

- Conduct a risk assessment to determine if any changes need to made to information security policies and procedures;
- Attempt to access users' accounts with the proper password to ensure that two-factor authentication prevents system access;
- Perform any relevant third party penetration tests or vulnerability scans and remediate any relevant discoveries; and

- Attempt to restore a sample of files and records from the systems documented in *MIL's Inventory of Technology Infrastructure* to ensure that the restoration process is sufficient and properly configured.

The results from the annual testing program and risk assessment will be documented and utilized as an opportunity to update the Cybersecurity & Information Security Policy.

Detection of Unauthorized Activity or Security Breaches

The CISO is responsible for monitoring on-site and cloud-based systems for suspicious activity and security breaches. Such activity may include:

- Logins to company systems after traditional business hours
- Logins to company systems from non-local regions (e.g., outside of the local region, outside the United States, etc.)
- Large transfers of files or data

When suspicious activity or a potential security breach is discovered, the CISO will restrict access to the systems, assess what information may have been accessed, and determine what actions need to be taken to remediate the event.

Regardless of the severity, the CISO will keep a log on MyRIACompliance of all incidents and note the action taken. This log will include the following information about each incident:

- Date and time of the incident
- How the incident was detected
- The nature and severity of the incident
- The response taken to address the incident
- Any changes made to the Cybersecurity & Information Security Policy as a result of the incident

All MIL staff are required to immediately alert the CISO of any suspicious behavior or other information security concerns.

RESPOND

The respond function helps MIL to establish the framework to respond to a potential cybersecurity incident once detected, and also how to mitigate the impact of such an incident.

Responding to Unauthorized Activity or Security Breaches

If a cybersecurity incident is deemed by the CISO to have led to unauthorized release or use of sensitive client information, then the CISO will take the following steps:

- Communicate the details of the event to the relevant principals of the firm
- Determine if any staff disciplinary action needs to be taken

- Determine if any third party vendors were involved in the incident
- Contact proper law enforcement and/or regulatory agencies as required by law (if necessary)
- Communicate the details of the event and steps being taken to rectify the incident to impacted clients of the firm (if necessary)
- Follow all relevant state data breach notification laws (if necessary)

Improvements to Cybersecurity Policies and Procedures

Following the proper mitigation and response to a cybersecurity incident, MIL's CISO will review the details of the incident to determine if any changes to be made to the Cybersecurity & Information Security Policy or other related procedures.

Any changes made to the Cybersecurity & Information Security Policy will be communicated to all MIL staff members and all staff members will be required to review and attest to the updated policy via the MyRIACompliance platform.

RECOVER

The recover function helps MIL to plan for and recover to normal operations in a timely manner in the event of a cybersecurity breach.

Significant Technology System Disruption Plan

In the event of a significant business disruption that results in a significant interruption in access to the firm's technology systems; MIL will implement its business continuity plan as detailed in its policies and procedures manual.

Client Information

In the event of the theft, loss, unauthorized release, or unauthorized use or of access of client information due to a technology system breach, the incident will be investigated and documented by the CISO and the CCO. If client information is involved, then MIL will follow its separate procedures concerning such exposure client information. The non-exhaustive list of possible follow-up actions includes notification of the parties involved, notification of appropriate regulatory officials if required, taking remedial actions to assist in the recovery of the stolen information, and possible sanctions of firm personnel if deemed necessary.

Data Back-Up Policies

MIL stores sensitive firm and client data on local and third party systems as documented in *MIL's Inventory of Technology Infrastructure*. This data is backed up in accordance with MIL's data back-up and recovery procedures.

Chief Compliance Officer Appointment

The person herein named "Chief Compliance Officer" is stated to be competent and knowledgeable regarding the Advisers Act or applicable state rule or regulation and is empowered with full responsibility and authority to develop and enforce appropriate policies and procedures for the firm. The compliance officer has a position of sufficient seniority and authority within the organization to compel others to adhere to the compliance policies and procedures.

Chief Compliance Officer	Date Responsibility Assumed	Annual Review Completed
Mike Terrio		

Samples

Sample 1 – Attestation Statement
Sample 2 – Terminated Advisory Account Record
Sample 3 – OBA Disclosure Template
Sample 4 – Email Review Checklist
Sample 5 – Email Review Activity Report
Sample 6 – Checks & Securities Receipt / Disbursement Record
Sample 7 – Trade Error Log
Sample 8 – Securities Holding Record
Sample 9 – Securities Transaction Record
Sample 10 – Gifts & Entertainment Log
Sample 11 – Authorization to Share Designated Information

Please note: The samples provided herein are not necessarily the form that records kept by MIL will take, as these records may be made and stored in a different manner, including via clod-based software. Additionally, any records containing non-public information (NPI), will be stored securely in accordance with the provisions in the Privacy Policy section of MIL's Code of Ethics.

Sample 1 - Attestation Statement

All Investment Adviser Representatives, access persons or supervised persons dealing with or having access to client files and other public or non-public information must initially upon hiring, and then annually, read, review, and acknowledge to abide by at a minimum the following firm items:

- Privacy Policy
- Code of Ethics
- Policies and Procedures Manual
- AML Red Flag Items

The firm's Chief Compliance Officer is responsible for documenting the completion of these tasks and therefore requires each of the firm's responsible parties and personnel to complete and sign the statement shown below.

ATTESTATION STATEMENT

By signing this document, I certify that I have read MIL's above listed documents and fully understand the legal, regulatory, policy, and other requirements outlined therein and agree to abide by the ethics, procedures, policies, agreements, and other stipulations contained therein.

Printed Name: _____ Signature: _____

Date: ____/____/_____

Sample 2 - Terminated Advisory Account Record

Date of Termination	Client Name	Reason for Termination	Type of Advisory Program Being Terminated

Sample 3 - Outside Business Activity Approval Form

In order to comply with MIL's policies and procedures, you are required to obtain prior written permission to have any outside employment or to receive any employment compensation other than through your affiliation with MIL.

1. Are you currently employed by or do you accept any compensation from, any business, organization, or entity not affiliated with MIL?

2. Do you serve as a director of any organization not affiliated with MIL?

For each "yes" answer above, complete the following: (Each question may have more than one "yes" answer)

Name of Company / Organization: _____

Your Title: _____ Start Date: _____

Description of your duties: _____

_____

_____

_____

Compensation (if any) to be received: _____

Amount of time per month that will be spent on activity: _____

APPROVED: _____ **DENIED:** _____ **(completed by supervisor or CCO)**

Submitted by: (signature) _____ (print) _____

Date: _____

Reviewed by: _____ Date: _____

Sample 4 - Email Review Checklist

Date: _____

Review Period: From: _____ To: _____ (Monthly, Quarterly, etc.)

- ❑ The CCO, or the CCO's designee, has reviewed electronic communications as determined adequate (keyword, random sample and/or key issue search).

- ❑ The review of emails was for content that may be deemed a violation of any compliance policies. Such content may include, for example, and is not limited to:

    1. Inappropriate marketing (e.g., use of unapproved marketing materials or performance figures);
    2. Indications of custody that raise issues regarding the actual possession of client funds and securities;
    3. Relationships with broker-dealers, service providers or clients indicating conflicts of interest not otherwise addressed by the firm's policies and procedures;
    4. Violations of the firm's Code of Ethics;
    5. Inappropriate gifts;
    6. Unreported client complaints; and
    7. Other issues deemed inappropriate.

- ❑ A summary report of the email review is attached as an exhibit to this email review checklist.

- ❑ Were any emails reviewed that revealed suspicious or inappropriate activity?

    - ❑ Yes
    - ❑ No

    If yes, attach a copy of such emails along with the Email Review Activity Report

CCO Signature _____ Date _____

Sample 5 - Email Review Activity Report

Email From: _____ Email To: _____

Email Subject: _____ Email Date: _____

- ❑ Describe the suspicious or inappropriate activity:

- ❑ Does this employee have previous email activity reports?
  - ❑ Yes
  - ❑ No
- ❑ Describe the previous sanctions imposed upon the employee:
  - ❑ Warning
  - ❑ Reprimand to Employee File
  - ❑ Compensation Reduction
  - ❑ Suspension
  - ❑ Termination
  - ❑ Other? _____
- ❑ Describe the new sanctions imposed upon the employee:
  - ❑ Warning
  - ❑ Reprimand to Employee File
  - ❑ Compensation Reduction
  - ❑ Suspension
  - ❑ Termination
  - ❑ Other? _____

CCO Signature _____ Date _____

Sample 6 - Checks and Securities Receipt/Disbursement Record

Date Received	Name of Client	Check #/Cert. #	Check Amt./# of Shares	Date Sent	Sent To	Method of Sending Doc

Sample 7 – Trade Error Log

Date of Error	Name of Client	Accounts Affected	Date Error Discovered	Date of Error Log Entry	Effect (Gain vs. Loss)	Amount

Description of Error: *(describe and document, including attachments as needed, the nature of the error, the cause of the error, and the including internal/external parties involved)*

_____

_____

_____

Corrective Actions: *(describe actions taken to resolve this specific error)*

_____

_____

Preventative Actions: *(describe actions taken, if any, to guard against similar trade errors in the future)*

_____

_____

Sample 8 - Securities Holding Record

In order to comply with MIL's record keeping and Code of Ethics requirements, you are required to provide a list of all securities in which you have any direct or indirect influence or control (e.g., joint or custodian ownership, securities owned by your spouse, etc.).

Excluded from the reporting requirements are:

- Transactions in which Access Persons have no direct or indirect influence or control or beneficial ownership. Beneficial ownership includes securities owned by the Access Person's immediate family members sharing the Access Person's household.
- Transactions in direct obligations of the US (e.g., T-Bills, etc.), Bank CDs, commercial paper, high quality short-term debt (including repos).
- Transactions in shares of open-end investment companies. Transactions in shares of open-end mutual funds may be relieved from this record keeping requirement (unless MIL or a control affiliate acts as the investment adviser to or principal underwriter of the fund).

Access Person's Name: _____

Date: _____

Name of the Security	# of Shares/ Amount	Broker/Dealer, Bank, or Custodian

Date Report Received: _____

Date Report Reviewed: _____

Reviewed by: _____

Sample 9 - Securities Transaction Record

In order to comply with MIL's record keeping and Code of Ethics requirements, you are required to provide a list of all security transactions in which you have any direct or indirect influence or control (e.g., joint or custodian ownership, securities owned by your spouse, etc.).

Excluded from the reporting requirements are:

- Transactions in which Access Persons have no direct or indirect influence or control or beneficial ownership. Beneficial ownership includes securities owned by the Access Person's immediate family members sharing the Access Person's household.
- Transactions in direct obligations of the US (e.g., T-Bills, etc.), Bank CDs, commercial paper, high quality short-term debt (including repos).
- Transactions in shares of open-end investment companies. Transactions in shares of open-end mutual funds may be relieved from this record keeping requirement (unless MIL or a control affiliate acts as the investment adviser to or principal underwriter of the fund).

Transaction reports are not required if the reports would duplicate information contained in broker trade confirmations or account statements that MIL holds in its records so long as confirmations or statements are received no later than 30-days after the end of the applicable calendar quarter.

Access Person's Name: _____
Date: _____

Name of the Security	# of Shares/ Amount	Date of Transaction	Transaction Price	Transaction Type (buy, sell)	B/D or Bank Transaction Executed

Date Report Received: _____
Date Report Reviewed: _____
Reviewed by: _____

Sample 10 - Gifts & Entertainment Log

Date	Client / Prospect Name	Client ID	Amount	Description / Details	CCO Review (Initial)

Sample 11 - Authorization to Share Designated Information

Client Name(s): _____
Client Account Number(s): _____

The above shown client(s) authorize MIL to share designated information concerning the above shown account(s) with the party(ies) listed below. This shared information may include but not be limited to the following information:

(initial next to each applicable item to allow sharing)

1) _____Registration of Account(s), Type of Account(s), and Ownership Information
2) _____Custodian for Account(s) (or other information about where account assets are held)
3) _____Holdings and Asset Allocations for Account(s)
4) _____Suitability Information (Income, Net Worth, etc.)
5) _____Investment Strategies For Account(s)
6) _____Other: _____

Below is the name and contact information of the parties to which MIL is authorized to release the information indicated above:

_____
_____
_____
_____

_____ _____
Client Signature / Date Client Signature / Date

Sample 12 - Written Acknowledgement of Fiduciary Status

Written Acknowledgement of Fiduciary Status

When we provide investment advice to you regarding your retirement plan account or individual retirement account, we are fiduciaries within the meaning of Title I of the Employee Retirement Income Security Act and/or the Internal Revenue Code, as applicable, which are laws governing retirement accounts. The way we make money creates some conflicts with your interests, so we operate under a special rule that requires us to act in your best interest and not put our interest ahead of yours. Under this special rule's provisions, we must:

- Meet a professional standard of care when making investment recommendations (give prudent advice);
- Never put our financial interests ahead of yours when making recommendations (give loyal advice);
- Avoid misleading statements about conflicts of interest, fees, and investments;
- Follow policies and procedures designed to ensure that we give advice that is in your best interest;
- Charge no more than is reasonable for our services; and
- Give you basic information about conflicts of interest.