Compliance Policies And Procedures Manual

As Required by the Investment Advisers Act of 1940

Adasina Social Capital

548 Market Street, Suite 60335,

San Francisco, California 94104

(415)986-5500 phone | (415)986-5502 fax

info@adasina.com

Adoption of Compliance Policies and Procedures Manual

Adasina Social Capital, Inc., doing business as Adasina ("Adasina" also sometimes "Advisor" or the "Firm"), is required by law and regulation to implement a compliance program that includes the designation of a Chief Compliance Officer ("CCO") and the adoption of written policies and procedures. The Firm has designated Maya Philipson, Principal and Chief Operating Officer, as the Firm's Chief Compliance Officer. Ms. Philipson has proposed, and upon the Principals' review and concurrence, the Firm adopts the following Compliance Policies and Procedures Manual to guide the Firm's regulatory compliance effort. The adoption of the updated Compliance Policies and Procedures Manual is effective commencing January 1, 2024.

Table of Contents

1.0 Overview of Compliance Program

Adasina is committed to the highest legal and ethical standards in the investment management industry. It is the responsibility of every member, officer and employee (sometimes collectively "Access Persons") of the Firm to fulfill this commitment to ethical conduct and comply with applicable laws and regulations.

PURPOSE OF COMPLIANCE POLICIES AND PROCEDURES MANUAL

Adasina is registered as an investment advisor with the U. S. Securities and Exchange Commission (the "SEC") under the Investment Advisers Act of 1940, as amended (the "Act"). The Act and SEC rules impose requirements on the Firm to adopt ethics policies and procedures and to establish, maintain and enforce operational and compliance policies.. In addition, the SEC requires registered investment advisors to adopt written compliance procedures, review the adequacy of those procedures annually and designate a chief compliance officer to review and implement those procedures. This Compliance Policies and Procedures Manual ("Manual") has been adopted by the Firm to comply with the Act and other applicable laws.

The Manual does not attempt to describe every requirement relating to its activities, but instead establishes general policies and procedures that apply to the Firm. All Firm personnel have a fiduciary duty to the Firm's clients to maintain high ethical standards and to comply with all applicable federal and state securities laws.

This Manual is the property of the Firm and its contents are proprietary. Employees are not permitted to reproduce or distribute this Manual, in whole or in part, without the authorization of the CCO.

INVESTMENT ADVISOR REGISTRATION

Adasina is an investment advisor with assets under management in excess of $100 million and is registered with the SEC under the Act and the rules and regulations promulgated thereunder. The Firm's SEC registration number is: 801-113385. The Firm's IARD/CRD registration number is: 151411.

FIRM OVERVIEW

Adasina provides investment management and other financial consulting services to funds for which it serves as Sub-Adviser, and its clients, which include high net worth individuals, trusts and charitable organizations. Investment management services include, among other services:

- Education regarding investment instruments and strategies,
- Investment strategy creation,
- Selection of sub-advisors,
- Determination of appropriate asset allocation, and
- Ongoing account management

Adasina supervises, directs and/or recommends investments in accordance with the investment objectives, guidelines and restrictions set by the client . The Firm offers its investment supervisory services to clients on primarily a discretionary basis. This means that the Firm is generally granted broad investment discretion over client assets including the authority to select the investments to be made, the quantity of securities to be bought and sold and the executing broker-dealer to be used in effecting securities transactions all without prior client authorization. This discretion may be limited by client investment guidelines and any investment restrictions established by the client.

Although our primary client relationships entail discretionary management, clients may designate certain assets or portions of their portfolios for non-discretionary management. For these assets, clients receive investment recommendations and the client elects whether or not to implement the recommended transaction. Often assets designated for non-discretionary management are privately held, illiquid or held for the benefit of designated beneficiaries.

The Firm does not act as the physical custodian for any client accounts or assets. Rather, the client appoints a third-party custodian to take possession of the assets of the account, to settle transactions for the account, and to accept instructions from Adasina regarding transactions in the account. The client is responsible for the acts of the custodian and all direct expenses of the account, such as custodial fees, brokerage expenses etc. Generally, brokerage transactions are directed to the custodian of the client's account to avoid "trade away" fees. Although the Firm does not maintain physical custody of client investment accounts, it is deemed to have custody of client assets on the basis of the Firm's authority to: 1. direct client-approved transfers of assets between a client's own accounts and if authorized, to client-designated third-party accounts; and 2. to receive payment of its management fees directly from a client's account.

In addition to investment management services, Adasina provides financial consulting services on either an hourly fee or fixed fee basis. Financial consulting services may include a financial review and analysis of some or all of the following areas:

- Cash flow and debt analysis;
- Net worth calculation and review;
- Risk assessment and insurance review;
- Equity compensation analysis and advice;
- Retirement, estate, real estate, and college planning; and
- Capital needs analysis (goal funding)

Unless provided in connection with the investment management services described above, clients engaging Adasina to provide financial consulting services will generally be required to enter into a separate written hourly or fixed fee agreement with Adasina setting forth the terms and conditions of the planning engagement and describing the scope of the services to be provided. Financial consulting clients are not required to be investment management clients of the Firm.

DESIGNATION OF CHIEF COMPLIANCE OFFICER

The Firm has designated Maya Philipson, Co-Founder and Chief Operations Officer to serve as the Firm's Chief Compliance Officer and has vested complete authority in her to develop appropriate compliance policies and procedures, to enforce those policies and procedures. The Chief Compliance Officer may designate one or more qualified persons to perform any portion of her responsibilities under this Manual. Other employees with responsibilities under this Manual also may delegate to appropriate persons subject to their supervision.

The Chief Compliance Officer may make exceptions, on a case-by-case basis, to any of the provisions of this Manual upon a determination of the facts and circumstances involved. Approvals of such exceptions are documented.

Any review that is required to be completed under this Manual is completed by the Chief Compliance Officer or her designee. The documentation of each review includes the date of the review.

Each employee is subject to the policies and procedures contained in this Manual. Employees should contact the Chief Compliance Officer if they have any questions about any compliance-related matters.

The Chief Compliance Officer will review this Manual at least annually and, in light of legal and business developments, changes in Firm operations and the staff's experience in implementing the Manual, propose changes to the Manual as deemed appropriate.

LEGAL AND REGULATORY OVERVIEW

Investment advisers are subject to complex rules and regulations promulgated under the federal and state securities laws, including but not limited to various provisions of the Securities Act of 1933, the Securities and Exchange Act of 1934, the Investment Advisers Act of 1940, the Employee Retirement Income Security Act ("ERISA"), the U.S. Patriot Act and the corporate securities laws of various states, including the State of California that are applicable to investment advisors.

The Firm is subject to examination by the SEC staff. If an employee receives any contact or inquiries from regulators, they immediately must refer them to the Chief Compliance Officer.

All Firm personnel must remain alert to any potential conflicts of interest, by virtue of their outside activities, personal trading, affiliated relationships or otherwise. All such potential conflicts must be assessed in terms of their potential risks to clients/investors and must be fully disclosed to senior management and the Chief Compliance Officer.

THE FIDUCIARY STANDARD

As an investment advisor, the Firm and its staff are subject to principles of fiduciary duty, which are enforceable under both federal and state law. These principles dictate that the Firm conduct its business in a manner that places the interests of its clients ahead of those of the Firm and to identify any and all potential conflicts of interest to clients that may impair its ability to do so. The obligations of an investment advisor as a fiduciary include, but are not limited to:

- A duty to act in the best interests of each client;
- A duty to place the interests of clients ahead of the interests of the Firm and its personnel;
- A duty to provide advice that is not tainted by false or misleading statements about investments, firm compensation, fees and costs of securities or conflicts of interest;
- A duty to disclose all material facts about the Firm and the advisory services it provides;
- A duty to disclose all conflicts of interest;
- A duty to mitigate to the fullest extent possible all conflicts of interest that cannot be eliminated;
- A duty to charge reasonable fees;
- A duty to disclose all forms of client and third-party compensation received by the Firm and its personnel and affiliates, if any;
- A duty not to trade on the basis of material non-public ("inside") information; and
- A duty to allocate investment opportunities fairly amongst clients and not favor accounts that may benefit the Firm financially, such as proprietary accounts, the Firm's largest client accounts or accounts paying performance fees.

CONFLICTS OF INTEREST

Adasina is accountable to its clients as a fiduciary and, consequently, must exercise good faith and integrity in conducting its investment management services. Nevertheless, in the conduct of its advisory business, conflicts may arise between the interests of Adasina or its staff and those of its clients. It is Firm policy for the Chief Compliance Officer to routinely review Firm practices to identify all potential conflicts of interest and to ensure that all identified potential conflicts are disclosed in the Firm's Form ADV Part 2 and either eliminated or mitigated to the greatest extent possible.

ACCESS PERSON RESPONSIBILITIES

All Firm principals and Access Persons are required at all times to comply with applicable state and federal securities laws and regulations and with the provisions of the Firm's compliance policies and procedures and

code of ethics. Any Access Person with knowledge of or suspicion of any facts evidencing a violation of state or federal securities laws or of the Firm's policies and procedures or code of ethics is required immediately to report such knowledge or suspicion to the Chief Compliance Officer, or as appropriate to another member of the Firm's senior management team. Neither the Firm nor any member of senior management may retaliate against any reporting Access Person for compliance with this provision.

As a matter of Firm policy, compliance with this Manual is a condition of continued employment and Access Persons must report any violation of this Manual promptly to the Chief Compliance Officer. The Chief Compliance Officer will investigate any reported or suspected violation of the provisions of this Manual and will document the factual findings and recommend sanctions, where appropriate. Access persons are required to cooperate in any such investigation.

Each Access Person is required to acknowledge having reviewed the provisions of the Manual. At least once a year, the Firm's principals and Access Persons are required to certify on an Initial and Quarterly Access Person Certification Form that each has read and understood this Manual, has complied with its requirements, and has disclosed or reported all personal securities transactions required to be disclosed or reported.

PROHIBITED PRACTICES
The anti-fraud provisions of the securities laws prohibit Firm principals and Access Persons from engaging in the following business practices:

- Employing any device, scheme, or artifice to defraud any client, the firm, the market or otherwise;
- Making any untrue statement of a material fact;
- Omitting to state a material fact necessary in order to make a statement, in light of the circumstances under which it is made, not misleading;
- Engaging in any fraudulent or deceitful act, practice or course of business; or,
- Engaging in any manipulative practices.

2.0 Advertising And Marketing

2.1 BACKGROUND
Advisor advertising and marketing is highly regulated, requiring that any advertising and marketing materials be truthful and accurate, consistent with applicable rules, and reviewed and approved by the Compliance Department. All Advertising materials are considered External Collateral and are therefore subject to the policies and procedures as specified in the ASC External Collateral Policy.

CHIEF COMPLIANCE OFFICER STAFF TRAINING AND REVIEW OF MARKETING MATERIALS
The Chief Compliance Officer is responsible for training all marketing staff and third-party marketing and public relations personnel regarding the Firm's advertising and marketing policies and procedures, as part of the Annual Firm-Wide Compliance Training. The Chief Compliance Officer works with staff to avoid any use of overstated results, hyperbole, unverifiable representations, omissions of facts and other misrepresentations of the Firm's services or performance record by any staff member responsible for creating marketing content.

Advertising materials may include, but are not limited to:

- Emails
- Tweets
- Instant messaging
- Form ADV
- Other brochures
- Newsletters

- Website
- Article reprints
- Press related marketing materials
- Responses to Request for Proposals
- Quarterly and annual data provided to consultants
- Consultant questionnaires
- Presentations developed for seminars for client meetings
- Transcripts of newspaper interviews
- Transcripts or tapes of television appearance

2.2 GENERAL PROHIBITIONS

Firm policy prohibits any advertising or marketing materials that may be misleading, fraudulent, deceptive and/or manipulative. All client and prospective client communications must be presented fairly, in a balanced manner and not otherwise be misleading. In addition, the Firm must disclose all material facts necessary to evaluate the Firm's marketing materials and solicitations to all current and prospective clients. Staff are specifically precluded from:

- Making an untrue statement of a material fact, or omitting a material fact necessary to make the statement made, in light of the circumstances under which it was made, not misleading;
- Making 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;
- Including 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 adviser;
- Discussing any potential benefits without providing fair and balanced treatment of any associated material risks or limitations;
- Referencing specific investment advice provided by the adviser that is not presented in a fair and balanced manner;
- Including or excluding performance results, or presenting performance time periods, in a manner that is not fair and balanced; and
- Including information that is otherwise materially misleading.

2.3 PERFORMANCE ADVERTISING

The following limitations are not intended to be all-inclusive or to provide a safe harbor for performance advertising. It is the Firm's responsibility when using any kind of performance results to ensure that the advertising is not false or misleading. The Firm must disclose all factors and limitations of its performance data that would materially affect the fair and accurate comprehension of the data by the intended recipient(s) of the presentation.

All required disclosures must be made on each page of the performance presentation that contains information requiring the disclosure or, if terminating disclosures are used at the end of the presentation, a reference to the disclosures page must be included on each page containing information that requires a disclosure.

2.3.1 GENERAL PROHIBITIONS FOR ADVERTISEMENTS THAT CONTAIN PERFORMANCE DATA

The Firm is prohibited from and may not include in any advertisement:

- Gross performance, unless the advertisement also presents net performance;
- Any performance results, unless they are provided for standardized time periods of one, five, and ten years; additional time periods may be included.

- Any statement that the SEC has approved or reviewed any calculation or presentation of performance results;
- 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;
- 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;
- Hypothetical performance (which does not include performance generated by interactive analysis tools), unless the adviser 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 the adviser provides certain information underlying the hypothetical performance; and
- Predecessor performance unless there is appropriate similarity with regard to the personnel and accounts at the predecessor adviser and the personnel and accounts at the advertising adviser. In addition, the advertising adviser must include all relevant disclosures clearly and prominently in the advertisement.

2.3.2 NET AND GROSS OF FEES.

- The Firm may not include a presentation of gross performance unless it also presents net performance in equal prominence to, and calculated over the same time, as the gross performance.[1]
- It cannot use model fees to make its performance look better than it would have if actual fees had been deducted.
- The Firm may use a model fee equal to the highest fee that would be charged to the intended audience of the performance presentation.

2.3.3 REQUIRED TIME PERIODS.

- All performance data used must be presented using standardized time periods of one, five, and ten years.
- Portfolios managed for shorter time periods should include performance information for the life of the portfolio.
- The Firm may include performance from other time periods if it includes the required periods as well.
- The time periods required must be shown with "equal prominence" to any other period used and not highlighted or in any way given prominence to higher performance periods.

2.3.4 RELATED PERFORMANCE.
If the Firm uses "related performance" it must include the performance of all portfolios with substantially similar investment objectives, subject to the following:

- Portfolios managed in the same investment style can be excluded if the results are not materially higher than they would have been if the portfolios were included.

[1] The Rule defines "net performance" as the performance results of a portfolio after the deduction of all fees and expenses that a client or investor has paid or would have paid in connection with the investment advisor's investment advisory services to the relevant portfolio. The Rule states that net performance includes asset-based advisory fees, performance-based fees, and carried interest and excludes items such as capital gains taxes or costs the advisor agrees to bear. Custodial fees paid to a third party are not required to be included in the calculation of net performance.

- Portfolios can be excluded if doing so would not affect the prescribed time periods for the performance returns.

2.3.5 FAIR AND ACCURATE REPRESENTATION AND DISCLOSURE CONSIDERATIONS
The following factors should be considered for all performance presentations and, where applicable, relevant disclosures should be included:

- The effect of material market or economic conditions on the results portrayed;
- Are any comparisons of model or actual performance results made with market or index results for comparable time periods;
- Does the use of "back-tested" model results require specific disclosures regarding any historical changes in the investment strategy during the time period;
- Comparisons of model or actual results to an index must be to a closely comparable index and must disclose all material facts relevant to the comparison (such as differences in volatility and diversification); and
- Material conditions, objectives or investment strategies used to obtain the performance advertised must be disclosed.
- Is each source of market or analytical data used in the performance presentation identified;
- Do the results portrayed include the reinvestment of dividends and other earnings and is this disclosed;
- Any performance advertisement that suggests or makes claims about the potential for profit must also disclose the possibility for loss.

2.3.6 HYPOTHETICAL PERFORMANCE.
The use of performance results that were not actually achieved by the Firm is significantly scrutinized under applicable regulation. Hypothetical Performance advertising includes model, back-tested and "targeted" or "projected returns. The SEC strongly emphasizes that advisors should have a compelling argument for using any kind of hypothetical performance and that hypothetical performance should only be presented to sophisticated and institutional investors rather than less experienced retail investors.

The Firm is prohibited from using hypothetical performance unless:

- The hypothetical performance is relevant to the likely financial situation and investment objectives of the performance data's intended audience.
- All disclosures are made that are necessary to the intended audience's understanding of the criteria used, assumptions made and limitations affecting the calculation of the hypothetical performance; and
- The performance presentation is sufficient to allow the intended audience to understand the risks and limitations of using such hypothetical performance in making investment decisions.

2.3.6.1 LIMITATION ON DISTRIBUTION OF HYPOTHETICAL OR MODEL PERFORMANCE RESULTS

The Firm provides Hypothetical Performance results only to the following types of clients/prospective clients:

- Institutional Clients
- Retail Clients or Prospective Retail Clients meeting or exceeding the criteria of High-Net-Worth ("HNW") Clients or Qualified Clients ($1,000,000 under management with the Firm; reasonably believed to have a net worth of at least $2,000,000, exclusive of any primary residence; or has a total of least $5,000,000 of investments.)
- Retail Clients or Prospective Retail Clients that do not qualify as HNW clients or qualified clients but whom the Chief Compliance Officer determines have a level of relevant education in or prior investment experience with the financial markets and have obtained a relevant level of sophistication in matters relating to the financial markets and investing.

NOTE: Hypothetical performance can be given to current or prospective clients when provided in response to an unsolicited request in a one-on-one communication. These communications are not considered advertising.

2.3.6.2 DISCLOSURES REQUIRED FOR HYPOTHETICAL OR MODEL PERFORMANCE

All disclosures required for a fair and accurate understanding of the hypothetical or model performance results by the intended recipient of the data must be provided. The following disclosures for hypothetical or model performance presentations should be considered and included as applicable (the following list is not exclusive):

- A description that the hypothetical performance results do not represent actual trading using client assets, but were achieved using a back-testing methodology and with the benefit of hindsight;
- The methodology used to create the model;
- A description on each page in which the performance results are compared to those of a market index all material facts relevant to the comparison (why the index is relevant, what limitations are present in the data of the compared index, etc.);
- Material changes in the conditions, objectives or investment strategies of the model portfolio during the period portrayed and the effect thereof;
- A description of how the investing methodology reflected in the back-testing was developed and whether it or the underlying has been modified;
- The limitations inherent in model results, particularly that such results may not reflect the effect of material economic and market factors on the advisor's decision-making if the Firm were actually managing clients' assets in the strategy during the time periods presented;
- An indication of the time periods that the firm was not yet managing money or not managing money according to the investment strategy modeled;
- Whether the strategies reflected in the model portfolio either do not relate, or relate only partially, to the services currently offered by the Firm.

2.4 TESTIMONIALS AND ENDORSEMENTS

The Firm will not include testimonials and endorsements in an advertisement, unless the following disclosure, oversight, and disqualification requirements are met:

- Disclosure. Advertisements must clearly and prominently disclose whether the person giving the testimonial or endorsement (the "promoter") is a client and whether the promoter is compensated. Additional disclosures are required regarding compensation and conflicts of interest. There are exceptions from the disclosure requirements for SEC-registered broker-dealers

under certain circumstances. The rule will eliminate the current rule's requirement that the adviser obtain from each investor acknowledgements of receipt of the disclosures.

- Oversight and Written Agreement. If the Firm uses testimonials or endorsements in an advertisement it must oversee compliance with the marketing rule. The Firm must enter into a written agreement with any third-party promoters, except where the promoter is an affiliate of the adviser or the promoter receives de minimis compensation (i.e., $1,000 or less, or the equivalent value in non-cash compensation, during the preceding twelve months).
- Disqualification. The Firm is prohibited from appointing certain "bad actors" to act as promoters, subject to exceptions where other disqualification provisions apply.

2.5 THIRD-PARTY RATINGS

The Firm will not include Third-Party Ratings in an advertisement, unless:

- The firm has a reasonable basis for believing 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; and
- The advertisement clearly and prominently discloses, or the firm reasonably believes that the third-party rating clearly and prominently discloses:
    - The date on which the rating was given and 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, that compensation has been provided directly or indirectly by the firm in connection with obtaining or using the third-party rating.

2.6 FORM ADV PART 2

The Form ADV Part 2 must be given to all new clients at the time they enter into an investment advisory agreement with the Firm. In addition, the Firm is required, at least annually, to make an offer to all existing clients to provide a current Form ADV Part 2 on request. The Part 2 is considered the Firm's "brochure" and must contain all required disclosures to clients.

The Form ADV Part 2 must be amended whenever any of the following occurs:

- A material conflict of interest is identified
- The Firm takes on the custody of assets
- Change in custodian relationships
- Change of firm address and/or phone number;
- Change of investment strategy;
- Change of investment advisory personnel;
- Change of trade allocation policy;
- Change of best execution policy;
- Change of fee schedule or fee arrangements;
- Change of proxy voting policy;
- Change in affiliates and/or
- Additions of other information deemed important to the Firm.

2.7 SOCIAL MEDIA

2.7.1 PRINCIPAL AND EMPLOYEE PERSONAL SOCIAL MEDIA SITES

Any reference to the Firm, its services, its principals, its clients, its investment strategy or investment recommendations, or any other aspect of its business on any employee website or social media site may constitute investment advisor advertising. In order to avoid the inadvertent violation of applicable regulatory restrictions on marketing and advertising, principals and employees may only reference their employment with the Firm and their job title on any personal social media account. No principal or employee personal social media account may be used to communicate any reference to the Firm's services, its principals, its clients, its investment strategy or investment recommendations, its performance or any other aspect of its business.

No principal or employee may conduct Firm or client correspondence or business over any personal social media account.

Employees that maintain personal social media content on LinkedIn (or an equivalent professional networking site) may reference only their educational history, the name of the Firm, their dates of employment and job title and prior professional experience. They may reference their professional skills and work experience but may not use the site to solicit new clients or otherwise discuss their personal or Firm financial consulting and/or investment management services. They may not post investment-related analysis or securities recommendations that have not been pre-approved by the Chief Compliance Officer.

These restrictions do not limit an employee's right to make social or political commentary on their personal social media account related to the financial services industry that does not rise to the level of investment analysis or recommendations for securities transactions.

2.7.2 NOTIFICATION OF PERSONAL SOCIAL MEDIA USE

Any authorized employee that seeks to maintain or create a social media account, blog or website upon which the employee intends to post content that references the Firm or its business practices, or that references the employee's skills, professional training, or professional activities in any way, must request approval from the Chief Compliance Officer, prior to posting such content on the site. New employees with pre-existing sites must notify the Chief Compliance Officer of the site via an Initial Access Person Certification prior to posting content that references the Firm or its business practices.

Each authorized employee who maintains or contributes to an approved social media account is required to:

- Attend an annual social media training session conducted by the Chief Compliance Officer as part of the Annual Firm-Wide Compliance Training.
- Notify the Chief Compliance Officer in writing of each existing and any new social media accounts or blogs the authorized employee has or intends to create and maintain.
- Provide the Chief Compliance Officer with the name of the account for integration with the Firm's electronic communications archival system.
- Via the Quarterly Access Person Certification, sign an attestation that all social media accounts or blogs he/she has contributed Firm- or professionally-related content to during the prior year have been previously reported to the Chief Compliance Officer and if one or more are no longer in use, a statement to that effect.

2.7.3 AUTHORIZED FIRM SOCIAL MEDIA ACCOUNTS

Subject to these policies and procedures and Chief Compliance Officer authorization, monitoring and supervision, the Firm may permit certain authorized employees to create, maintain and publish to Adasina's corporate social media accounts. The content posted on these accounts is subject to approval and monitoring by the Chief Compliance Officer, per Adasina's External Collateral Policy.

Any and all content posted on Adasina's corporate social media accounts is and will remain the copyrighted, proprietary and intellectual property of the Firm and not of the employee that creates or authors the content. All Firm social media accounts must be accessible to the Chief Compliance Officer and are subject to the Firm's archiving and recordkeeping procedures.

2.7.4 ARCHIVING OF FIRM SOCIAL MEDIA CONTENT

To meet its regulatory obligations, Adasina requires each authorized Firm-related or professionally related social media account to be incorporated into the Firm's email and electronic communications archival system so that all communications sent and received over the site are archived by the Firm. All such social media communications are subject to regulatory review by the Chief Compliance Officer, senior management, outside legal counsel and federal and State of California examiners, as applicable.

2.7.5 RESTRICTIONS ON AND REQUIREMENTS OF FIRM SOCIAL MEDIA CONTENT

Any and all content posted by an authorized employee on any of the Firm's professional website, blog, or social media site must adhere to the following specific restrictions and requirements. Authorized employees posting on the Firm's social media are:

- Subject to the policies and procedures set forth in Adasina's External Collateral Policy.
- Required to use appropriate disclosures as to the Firm's and/or authorized employee's business affiliations, relevant conflicts of interest and to correctly attribute ownership/authorship of any content, comments, statements or quotes to their originator.
- Prohibited from making any reference to past specific successful recommendations of securities, unless approved by the Chief Compliance Officer who will require the authorized employee to provide a separate detailed list of all past recommendations good or bad over at least the past year, with the name of the security, the date recommended, and the price at which it was recommended. Any such post requires a disclosure that past performance is not an indication of future performance with the materials. The authorized employee must disclose all material facts relating to any recommendation.
- Prohibited from making any post that contains an untrue statement of material fact or otherwise is false or misleading.
- Prohibited from posting or linking to any content that violates applicable federal and/or state rules and regulations, industry and professional group guidelines and these policies and procedures set forth in the Firm's compliance Manual.
- Prohibited from accepting third-party endorsements, testimonials and/or recommendations of the employee's background or skills or the Firm's successes from clients, family, friends, other professionals or site users.
- Prohibited from using Facebook Chat or any similar instant messaging or chat service on LinkedIn and Twitter for any business-related communication that is not being archived by the Firm.
- Prohibited from re-posting/re-tweeting fraudulent, misleading, inaccurate or unreliable third-party content. The re-posting/re-tweeting of third-party content must include all original disclosures, disclaimers and explanations of the content provided in the original third-party content. If in doubt, the Chief Compliance Officer should be consulted to make the determination as to the Firm's risk of inadvertently adopting content that is inaccurate or misleading.

- Prohibited from posting or linking to comments or content that is harassing, defamatory or indecent or misrepresents the stated policies, practices, successes or investment strategies of the Firm.

- Required to be honest and consistent with prior professional comments the authorized employee has provided to clients while providing investment advisory services or in presentations previously made on behalf of the firm.

- Prohibited from making comments that are in retaliation to negative posts or comments received on the site. If warranted, the Chief Compliance Officer will address any issues that directly relate to negative client content identified in such posts.

- Prohibited from writing and posting any favorable comment regarding the Firm on a third-party social media site or blog.

- Required to protect the financial and personal privacy of all Firm clients by prohibiting the use of a client's name address, identification information, financial, account holdings or any other information specific to a customer on the authorized employee's social media site.

- Prohibited from providing legal or tax opinions or making specific investment recommendations on any social media site.

- Prohibited from making any negative references about the Firm or any Firm employee on any social media site, or from making any misrepresentation as to the authorized employee's title, responsibilities or position with the Firm.

- Prohibited from posting content that resorts to the use of hyperbole, superlatives, exaggeration or that projects specific investment returns (or a range of returns).

- Required to consider the likely audience of any social media post and refrain from relying upon industry jargon or overly technical and confusing content if less sophisticated readers would otherwise misunderstand such content.

- Prohibited from disclosing any material non-public information.

- Prohibited from disclosing any Firm proprietary information, intellectual property or trade secrets.

2.8 THE PRESS AND PUBLIC STATEMENTS

All firm-level responses to the press and other public statements are considered External Collateral under Adasina's External Collateral Policy, and are therefore subject to the review and pre-approval requirements set forth therein.

2.9 COMMUNICATIONS WITH CLIENTS AND PROSPECTIVE CLIENTS

- Only certain authorized employees of the Firm including senior management, employees registered via a Form U-4 or those that have passed the Series 65 exam, CFP certification exam, CFA certification exam (or other professional designation approved by the Chief Compliance Officer) are permitted to communicate directly with the Firm's clients and prospective clients.
- All electronic communications with the Firm's clients and prospective clients are required to be maintained in the Firm's books and records. All communications via email, smartphone or other personal, handheld electronic communication device must be archived by the Firm's electronic communication archiving system.

2.10 WEBSITE MAINTENANCE

- All content on any of the Firm's corporate websites is subject to the policies and procedures specified in Adasina's External Collateral Policy.

- The following additional requirements apply to the Firm's website content:
    - The Firm's client privacy statement should be posted on the website;
    - Appropriate disclosures/disclaimers must be clearly visible and accurate; and
    - Links to third-party sites must be pre-approved by the Chief Compliance Officer.

2.11 COMMUNICATIONS WITH THE MEDIA
Personnel should exercise caution in speaking with the press. The following guidelines should be followed in connection with interviews and discussions with the media as well as external speeches and group presentations.

2.11.1 IN GENERAL

- All materials, excluding only oral statements, submitted to an external party or used for an external presentation are subject to the pre-approval requirements set forth in Adasina's External Collateral Policy.
- Staff should not identify or discuss specific private client accounts.
- Staff should not discuss specific client account performance and should use caution when discussing sample account performance. Any performance information provided must be accompanied by required disclosures identified elsewhere in this Manual.
- Staff should not discuss illiquid securities the Firm holds within clients' accounts.
- Staff should not guarantee or predict a specific level of investment performance.
- Staff should not discuss firm confidential information, including legal or regulatory issues.
- Staff should not discuss competitors of The Firm.

2.12 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer is responsible for the Firm's compliance with applicable marketing and advertising recordkeeping requirements. Records may be kept electronically in a non-rewritable format. The following records are kept by the Firm for at least 5 years from the end of the year in which they were last used:

CURRENT AND SUPERSEDED COPIES OF THE FIRM'S MARKETING AND ADVERTISING MATERIALS

- Copies of each advertisement or piece of marketing material issued by the Firm;
- Copies of each email or other electronic communication that contains marketing or advertising material;
- Superseded versions of the Firm's website;
- Archives of Firm social media content; and
- All worksheets and account statements necessary to substantiate and demonstrate the accuracy of every performance statement disseminated.
- All accounts, books, internal working papers, and any other records or documents that are necessary to form the basis for any or all securities recommendations.

3.0 Anti-money Laundering

3.1 POLICIES

It is the policy of the Firm not to provide services to persons or entities that have connections to organized crime, violent crime, drug trafficking, arms trafficking, foreign official corruption or terrorism. The Firm will not accept any client that carries a risk of involvement with any of the above activities. Further, the Firm prohibits the use of any of its facilities (including its offices, computer systems or assets) by its members, officers, employees or affiliated persons for any illicit or illegal activities. Any Firm employee who detects any suspicious activity is required to immediately report such activity to the Chief Compliance Officer without discussing it or the report of it with the client or other implicated person involved.

In an effort to avoid AML and sanctions concerns, the Firm will only consider relationships with client entities owned by or for the principal benefit of a foreign official with explicit and written approval by the CCO. In any instance where the AML/Chief Compliance Officer suspects an account (or transaction) has connections to foreign official corruption, she immediately will notify the Firm's senior management.

3.2 PROCEDURES

Because the Firm does not custody client assets, all Firm clients are required to establish custodial accounts with an independent broker-dealer. Broker-dealers are required to adopt extensive anti-money laundering policies and procedures. As a part of their anti-money laundering programs, broker-dealers must verify the identity of each customer of the brokerage firm, determine whether each customer has been identified by the U. S. Department of Treasury (or other government entity) to be involved in terrorism, drug trafficking or organized crime and to monitor customer accounts for suspicious activity. Adasina generally relies on the AML review procedures of our clients' custodians and brokers to verify our clients identities.

3.2.1 CUSTODIAN REQUESTED EFFORT TO VERIFY CLIENT IDENTITY

Although most custodians undertake client identity verification as a part of their new customer procedures, to the extent a new client's identity cannot be verified by their custodian, or their custodian identifies an AML violation or risk associated with such client, Adasina will not agree to provide services to such client. At the custodians request, to support the identity verification process, the Chief Compliance Officer may request supplemental documentation from new, existing, and prospective clients, including, but not limited to copies of tax returns, employment representations and verifications, credit reports, non-resident alien client profile forms, banking verifications, audited financial statements, or any other relevant documentation.

3.2.2 SAR — SUSPICIOUS ACTIVITY REPORTING

The Chief Compliance Officer will file a suspicious activity report (FinCen Form 101: SAR-SF) under the following circumstances:

- If the Firm in connection with its advisory services, identifies any activity on the part of a Firm client with persons or entities that appear on any government list of restricted persons, and upon further investigation into the matter, it is determined that suspicious activity may have occurred.
- If the Firm detects or reasonably suspects a criminal violation or attempted violation by one of the Firm's clients, officers or employees or any other suspect using the Firm's services or facilities, including any incidence of cyber-security breaches.
- The Firm detects or suspects that its computer systems have been accessed by persons or entities to remove, steal, procure or otherwise affect the Firm's client or own accounts or other critical information or to damage or disable the Firm's computer systems and databases.

Suspicious activity report forms and instructions for filing are available on the FinCen website: https://www.fincen.gov/resources/filing-information. All forms filed with FinCen must be filed electronically through the BSA E-Filing system available at http://bsaefiling.fincen.treas.gov/main.html. SARs must be filed within 30 days of the detection of the suspicious activity. Records of reports filed must be kept for a minimum of five years.

The Firm maintains a file of each suspicious activity report for five years from the date the report is filed. No such reports have been filed as of December 31, 2023.

3.2.3 MONITORING FOR SUSPICIOUS ACTIVITIES

Employees are required to report to the Chief Compliance Officer any instances of suspicious activity that may indicate money-laundering is occurring in client accounts. These types of activities include:

- A client who exhibits unusual concern for secrecy, particularly with respect to his/her identity, type of business, assets or dealings with firms, or the client provides non-verifiable references or is reluctant or refuses to provide financial information or information concerning financial relationships and business activities.
- A client who has difficulty describing the nature of his/her business or lacks general knowledge of his/her industry.
- A client who exhibits unusual concern regarding the Firm's compliance with government reporting requirements, does not reveal or provides unusual or suspect identification or information to the Firm.
- A client who instructs the Firm to engage in transactions that lack business sense or are contrary to the client's stated business or objectives.
- A client who has a questionable background or is subject to news reports indicating possible criminal activity.
- A client who exhibits a lack of concern regarding investment risks, portfolio performance, advisory fees, commissions or other transaction costs.
- A client who is more interested in writing checks and utilizing a debit card than investing.
- A client who appears to be acting as an agent for another entity, but is reluctant or refuses to disclose any information about that entity.
- A client who has a pattern of unusual withdrawals, contrary to his or her stated investment objectives.
- A client who asks for multiple accounts managed under a single name or multiple names, or requests frequent transfers between his or her accounts or outside bank and other brokerage accounts, including foreign transfers.
- A client who requests that transactions be processed without normal documentation.
- A client that is from, or has accounts in, a country identified as a haven for money laundering.
- A client or a person publicly associated with a client that has a questionable background including prior criminal convictions.

3.2.4 CTR — CURRENCY TRANSACTION REPORTING

It is unlikely that the Firm will be called upon to report client currency transactions under applicable currency transaction reporting regulations. The Firm custodies no client assets and accepts no client funds or securities. Nevertheless, if a currency transaction of $10,000 or more (deposit, withdrawal, exchange of currency or other payment or transfer through the Firm), is mistakenly accepted, the Chief Compliance Officer must immediately be notified and will return the currency to its source. If warranted, the Chief Compliance Officer may determine to file a Currency Transaction Report (U. S. Dept. of Treasury Form 5789). Records of reports filed must be kept for a minimum of five years.

Currency Transaction report forms and instructions for filing are available on the FinCen website: https://www.fincen.gov/resources/filing-information. All forms filed with FinCen must be filed electronically

through the BSA E-Filing system available at http://bsaefiling.fincen.treas.gov/main.html. CTRs must be filed within 15 days of the transaction.

3.2.5 CMIR — CURRENCY OR MONETARY INSTRUMENT TRANSPORT REPORTING
The Firm prohibits the receipt of currency. Nonetheless, if an employee discovers that currency of $10,000 or more has been received from a source outside the U.S., the Chief Compliance Officer must be notified immediately and will file a CMIR with the Commissioner of Customs as required.

Currency or monetary instrument transport report forms and instructions for filing are available on the FinCen website: https://www.fincen.gov/resources/filing-information. All forms filed with FinCen must be filed through the BSA E-Filing system available at http://bsaefiling.fincen.treas.gov/main.html. Reports filed must be kept for five years.

3.2.6 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer supervises the Firm's compliance with applicable AML recordkeeping requirements. Records may be kept electronically in a non-rewritable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- Any suspicious activity reports, currency transaction reports or currency and monetary instrument transport report filed by the Firm.
- Documentation of annual anti-money laundering training for staff and affiliated persons, as required.

4.0 Best Execution

4.1 BACKGROUND
Federal law requires the Firm to seek "Best Execution" for client transactions. Best Execution is defined as combining a reasonable commission rate in relation to the quality of the execution and value of the brokerage services provided by the executing broker.

Adasina executes individually managed client account securities trades through the custodial broker holding the client's account in order to avoid "trade away" fees that would be imposed if executed at another executing broker. However, where a particular security is not available through the client's custodian, or where better execution is available through an alternative broker-dealer, the Firm may direct a client trade to a non-custodial broker-dealer for execution and incur a trade away fee for the client. In practice, the Firm's portfolio managers are rarely, if ever, called upon to evaluate and compare the services and execution quality of competing broker-dealers in connection with a trade.

4.2 POLICIES

4.2.1 BROKER-DEALER RECOMMENDATION AND SELECTION
It is Firm policy that portfolio managers evaluate the following performance factors before recommending broker-dealers to clients for custodian services and selecting brokers for trade execution services:

- The execution capabilities of the broker(s);
- Custodial services of the broker(s) to Firm clients;
- The confidentiality provided by the broker(s);
- Availability of technological aids to process trade data;
- Opportunity for price improvement on trades;
- The promptness of execution of securities transactions;

- Competent block trading coverage ability, if necessary;
- Capital strength and financial stability;
- Reliable and accurate communications and settlement capabilities;
- Administrative ability;
- Commissions/trading costs;
- Knowledge of other buyers and sellers;
- The broker's ability and willingness to position portions of orders;
- Research provided (and other soft dollar considerations);
- Breadth of services provided to clients;
- Availability of information regarding the most favorable market for executing trades;
- Conflicts of interest with the broker or that may result from trading activity; and
- The broker's general reputation.

4.2.2 CHANGE IN RECOMMENDED BROKER-DEALER RELATIONSHIPS

In deciding whether to select a new broker or brokers, or change a brokerage relationship, the Firm must consider the estimated cost in terms of time and administration to the Firm and its clients in making a change. This effort would include having all affected clients sign new brokerage and/or custodial agreements, the time taken away from portfolio management, and the operational duties to effect such a large change. As a result, the decision to establish a new brokerage relationship would require a finding by the Firm that substantial cost and/or service savings or benefits would accrue to the Firm and/or its clients that would justify the time and administrative effort to move affected client accounts.

4.2.3 CONFLICTS OF INTEREST

When selecting an executing broker-dealer to execute client trades, portfolio managers must remain sensitive to the following potential conflicts of interest and, where necessary, address such conflicts by disclosure, client consent, or other appropriate action:

- Broker-dealer provides access to Initial Public Offerings (IPOs);
- Broker-dealer makes client referrals to the Firm; and
- Broker-dealer provides soft dollar research or brokerage services to the Firm.

4.3 PROCEDURES

4.3.1 ANNUAL BEST EXECUTION REVIEW OF EXECUTING BROKER-DEALERS

At least annually, the Firm's Chief Compliance Officer, with input from the Firm's portfolio managers, evaluates all broker-dealers that are recommended by the Firm and through which any trade executions have been entered during the year. The evaluation should compare the custodial and execution services between available broker-dealers and whether the broker-dealers currently recommended by the Firm meet the Firm's best execution standards.

The Chief Compliance Officer evaluates the performance of the Firm's approved broker-dealers with other available broker-dealers that offer the same class of services. The Chief Compliance Officer conducts

sufficient due diligence regarding the services available, quality of services, pricing and other factors of other broker-dealers in the industry offering custodial and execution services. A comparison of broker-dealer institutional services should be made.

Documentation of such due diligence and relevant findings are included in the annual best execution review. The annual review is documented using the accompanying Annual Best Execution Evaluation Checklist.

4.3.2 ONGOING EVALUATION OF EXISTING BROKER-DEALER RELATIONSHIPS
If an existing broker-dealer receives a poor evaluation during the Chief Compliance Officer's annual review, the Firm will discontinue its recommendation of that broker. In addition, a broker-dealer relationship will be terminated if it comes to the attention of the Chief Compliance Officer that the broker is:

- Suffering business continuation difficulties that have been publicly reported upon that in the opinion of the Chief Compliance Officer impacts its ability to perform; or
- A party to litigation or the subject of government investigation that, in the opinion of the Chief Compliance Officer, impacts its ability to perform.

4.3.3 TRADE-AWAY TRANSACTIONS- EVALUATING EXECUTING BROKERS
If a client's custodial broker-dealer is not able to execute a contemplated transaction or to execute the transaction in a manner that is in the best interests of the client, the portfolio manager may select an alternative broker-dealer for execution after consideration of the following factors:

- The type of security;
- Commission and pricing;
- If an OTC trade, when the executing broker is acting as agent or principal;
- Whether it is a new issue;
- The size of the contemplated trade;
- The security's liquidity and availability;
- Whether the broker-dealer is an underwriter of the security or follows the security;
- The then prevailing market conditions for the security and the market as a whole;
- The other costs associated with executing the trade (such as transaction fees and settlement fees); and
- The communication skills of the broker-dealer representative assigned to the firm.

4.3.4 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer supervises the Firm's compliance with applicable best execution recordkeeping requirements. Records may be kept electronically in a non-rewriteable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- Annual Best Execution Evaluation of Broker Dealers
- Broker-Dealer Schedules of Commissions and Other Fees

5.0 Client Portfolios And Valuation Procedures

5.1 POLICIES

5.1.1 CLIENT PORTFOLIOS
It is Adasina's policy to manage its client account portfolios in a manner that is consistent with its investment strategy, client investment guideline, client investment restrictions, client risk tolerance, and the Firm's Form

ADV disclosures and regulatory requirements. The Firm's portfolio managers routinely review client account transactions to prevent and identify any material deviations from the these criteria. Reviews include:

- Semi-annual review of portfolio holdings; and
- Annual review of client investment guidelines with each client, or more frequently as appropriate

All Firm clients are requested to inform the Firm of material changes to their financial circumstances and any desired modifications to their investment guidelines and risk tolerance. If the client indicates a change in his or her financial condition, risk tolerance, investment goals or investment guidelines, the portfolio manager documents the change in the client's account file or otherwise.

5.1.2 INVESTMENT MANAGEMENT FEE AGREEMENTS

Investment management services are provided pursuant to a written investment management agreement between the Firm and the client. The Firm's current fees for its investment management services must be reflected in the investment management agreement and the Firm's Form ADV Part 2. Deviations from the standard fee schedule may be approved on a case-by-case basis by senior management and reflected in the individual client's investment management agreement.

5.1.3 FINANCIAL CONSULTING SERVICES

Adasina provides project–specific financial consulting services to its clients. Financial consulting clients receive services pursuant to a separate written hourly or fixed fee agreement. The Firm's current standard fees for hourly and fixed fee services are reflected in the Firm's Form ADV Part 2. Deviations from the standard fee schedule may be approved on a case-by-case basis and only by senior management.

5.1.4 ELECTRONIC COMMUNICATIONS WITH CLIENTS AND PROSPECTIVE CLIENTS

All Firm business communications are required to be maintained in the Firm's books and records. All written electronic communications via email, smartphone or other personal, handheld electronic communication device and social media must be archived by the Firm's electronic communication archiving system. Business communications over social media sites are not permitted.

5.1.5 ELECTRONIC DELIVERY OF CLIENT ACCOUNT DOCUMENTS

To satisfy regulatory requirements regarding electronic delivery of client communications and documents, the Firm:

- Obtains and documents client authorization to receive electronic communications (i.e., custodian statements, Firm account reports, Form ADV updates) from the Firm in lieu of hard copy correspondence. Such authorization may be obtained either by provision in the client's investment management or hourly agreement, by a written communication from the client or by the client's authorization in the client's custodial agreement; and
- Encrypts all electronic communications and attachments that contain private client financial and identification data or provides access to such documents through a secure online portal.

5.1.6 SECURITIES CLASS ACTIONS

Personnel are precluded by law from giving legal advice to clients. It is Firm policy that staff may not make any recommendations to clients as to whether to participate or not in any legal action. The Firm restricts its client support regarding class action lawsuits to assisting clients with the verification of securities holdings, acquisition and disposition dates and cost to allow them to participate in the settlements of such actions.

Any client requesting assistance with the decision to join a securities class action must be informed of the Firm's policy against providing legal advice and the limited extent to which staff is allowed to provide assistance. For clients who wish to participate in a class action and require investment data, the Firm will authorize staff to assist in providing trade and cost basis information. Firm personnel should advise clients that require additional assistance with the process to seek qualified legal counsel.

5.2 PROCEDURES

5.2.1 BEST INTEREST OF THE CLIENT AND INVESTMENT STANDARDS

As a fiduciary, the Firm must make investment decisions that are in the best interests of the client. Toward this end, all client investment decisions must be guided by the portfolio manager(s)' understanding of which securities investments are "suitable" for the client's age, financial condition and other factors.[2]

5.2.1.1 INVESTMENT STANDARDS

Portfolio managers must maintain a reasonable basis to believe that any client securities transaction or investment strategy selected is suitable for the client. This reasonable belief must be based on the information obtained through the Firm's new client documentation process which creates a client-specific investment profile based upon the client's:

- Age;
- Employment status;
- Sources of income;
- Liquid net worth;
- Tax status, such as marginal tax rate;
- Investment objectives ;
    - generating income
    - preserving wealth
    - market speculation
- Risk tolerance, (a client's willingness to risk losing some or all of the original investment in exchange for greater potential returns);
- Liquidity needs;
- Investment time horizon to achieve a particular financial goal;
- Investment experience; and
- Other investments.

This information is reviewed on an annual basis and updated as required by changes in client employment, financial conditions, financial needs and proximity to retirement.

5.2.2 INVESTMENT DISCRETION

Clients must appoint Adasina as their investment advisor and grant full trading and investment authority over their assets at the time they establish their investment accounts. Subject to the Firm's investment strategy, the relevant investment management agreement, and the client's investment objectives, our portfolio managers are given full discretion to determine:

- Types of investments;
- Which securities to buy;

[2] While "best interest" is the fiduciary standard, "suitability" is the framework for the analysis.

- Which securities to sell;
- The timing of any buys or sells;
- The amount of securities to buy or sell; and
- The broker-dealer to be used in the transaction

This discretion may be limited by client investment guidelines and by any investment restrictions set by the client.

5.2.3 CLIENT INVESTMENT RESTRICTIONS
The Firm keeps track of individual client investment restrictions in the client's account records or otherwise. The portfolio managers are responsible for updating the records as necessary if there are changes to existing restrictions.

5.2.4 CLIENT ACCOUNT REVIEWS
The portfolio managers review client accounts not less than semi-annually. Additionally, client accounts are reviewed in response to changes in the financial markets, changes in the Firm's investment decisions and/or changes in individual client investment guidelines or financial circumstances. The portfolio managers monitor that client portfolios are invested and managed in a manner that is consistent with client objectives and stated investment guidelines.

5.2.4.1 ANNUAL CLIENT CONFERENCES - RULE 3A-4 OF THE INVESTMENT COMPANY ACT

The Firm complies with Rule 3a-4 to ensure that its management of multiple client accounts is not deemed as the management of an "inadvertent investment company." To satisfy the requirements of Rule 3a-4, the Firm takes the following actions:

- Each client's account is managed on the basis of the client's individual financial situation and investment objectives and in accordance with any restrictions imposed by the client.
- At least annually, the Firm contacts its clients to update, as necessary, the client's profile regarding financial condition, investment objectives, liquidity requirements..
- Documents each annual contact.
- The employees responsible for managing each client account are knowledgeable about the client account and reasonably available to each client for consultation.
- Each client has a custodial arrangement that provides the client the right to:
    - withdraw securities or cash;
    - vote securities or delegate the authority to vote securities to another person (including the Firm);
    - be provided timely written confirmation of each securities transaction and all other documents required by law to be provided to securities holders; and
    - proceed directly as a security holder against the issuer of any security in a client account and not be obligated to join with any other client account as a condition precedent to initiating such proceeding.
    - At least quarterly, each client receives directly from their custodian a statement listing all transactions made in a client account, all contributions and withdrawals, all fees and expenses charged to a client's account and the value of the client's account at the beginning and the end of the period.

5.2.5.1 VALUATION OF CLIENT ASSETS UNDER MANAGEMENT

The Firm provides on-demand (via an electronic portal) client account reports that reflect portfolio holdings, asset allocations and portfolio performance as of the last business day. Client portfolios are valued according to the value of the assets held which is determined as follows.

Valuations of liquid securities are provided to the Firm by third-party custodians (e.g., Schwab, or the custodian where client assets are held) that use industry leading pricing services, such as Thompson Reuters, Interactive Data, Standard and Poor's, or Bloomberg for valuation data. The Firm may utilize a 3rd party portfolio management service for valuation support.

To the extent non-liquid investments such as limited partnerships, limited liability companies or non-traded real estate investment trusts (REITs) are held in client accounts, they are valued at asset values reported by the relevant investment issuer or sponsor. If a sponsor does not report a current price, (which typically occurs during the initial investment stages of capital investment) then the units or shares are carried at the amount of the original investment.

5.2.5.2 DISREGARD OF MARKET QUOTATION - FAIR VALUE PRICING FACTORS TO BE CONSIDERED

In the rare instance that the custodian is unable to obtain a price, or where the portfolio managers believe the custodian is not pricing a security fairly, or trading has been halted, the Firm will attempt to determine a fair value for that security. When determining a fair value for a security, the Firm attempts to obtain a quote from at least three independent pricing sources. Based upon these, the Firm determines a reasonable fair value.

Under certain circumstances, the Firm may determine that the market quotation price for a security should be disregarded because it is unreliable or otherwise not "readily available." This might occur in light of a market halt in the trading of a particular security or a disruption of the market in general by a "significant event" (natural disaster, terrorist event, power outage, civil unrest). Similarly, news reports or corporate announcements released after the close of the market or on a market holiday may significantly undermine the reliability of the most current market quotation. If the Firm determines that the market quotation does not fairly represent market value, it may value such securities as it reasonably determines in consideration of established fair value pricing factors including, but not limited to:

- The type of security;
- The financial statements of the issuer of the security;
- The cost of the security at purchase;
- The size of the position held in the security;
- Special reports relating to the security issued by industry analysts;
- Information as to any transactions or offers with respect to the security;
- Fundamental analytical data relating to the investment;
- Nature and duration of restrictions on the transferability of the security;
- An evaluation of the relevant market forces in which the security is bought and sold;

- The impact of intervening “significant events” on the individual security or its market sector; and
- Any other factor deemed appropriate by the investment managers.

Upon request, any client may obtain a description of the fair value pricing factors considered.

5.2.5.3 ADVISORY FEE ASSESSMENTS

5.2.5.3.1 FEE CALCULATIONS

Investment management fees are calculated in accordance with the fee provisions of each client’s investment management agreement and assessed against the securities valuations provided by the custodian of the portfolio assets.

5.2.5.3.2 ALTERNATIVE AND/OR ILLIQUID INVESTMENTS

The Firm’s investment strategy does not rely on alternative investments, illiquid investments, or other hard-to-value securities. In the event a client’s portfolio holds a legacy position in such an asset, and the asset value is zero (via the Custodian valuation process) it will not be assessed a management fee.

5.2.5.3.3 DESIGNATED ACCOUNTS FOR FEE DEDUCTIONS

Clients with multiple investment accounts may elect to have fees owed by the collective portfolio to be paid from one or more designated accounts within the portfolio. Equally, extended family members who are clients of the Firm may elect to have all fees owing from each family member aggregated and deducted from one or more designated accounts owned by one or more of them.

5.2.5.3.4 FEE REIMBURSEMENTS AND FEE OFFSETS

In the event a client becomes entitled to a fee reimbursement (at termination of the client relationship) or a fee offset (reimbursement for a trade error), the Chief Compliance Officer will review the client’s fee calculation prior to deduction from the client’s account.

5.2.5.4 INVESTMENT MANAGEMENT FEE – PAYMENT FROM CLIENT ACCOUNT

In most cases, the Firm’s clients authorize their individual custodians to deduct the Firm’s management fees directly from the client’s account. The Firm should verify that this client authorization is in writing on the custodial agreement between the client and the custodian and should maintain a copy of the authorization/agreement in the Firm’s client file. It is a best practice for the Firm to send an itemized fee statement to the client, showing the fee calculation, at the time payment is requested from the custodian by the Firm. Payment of the fee is reflected on the client’s monthly custodial statement. The Firm’s fee statement must include a disclaimer to clients. The fee payment also is reflected on the custodian’s statement to the client.

5.2.5.5 ANNUAL FORENSIC TESTING OF MANAGEMENT FEES

At least annually, in order to avoid overcharging client fees, the Chief Compliance Officer conducts a forensic test of fees charged to a statistically relevant (15 – 20%) sampling of client accounts to verify that

the fees charged clients correspond to the client's individual investment management agreement and are calculated accurately. The results of this test are documented either as a part of the Chief Compliance Officer's annual compliance program review or separately in a stand-alone report.

5.2.6 CLIENT COMPLAINTS
Any staff member that receives a complaint, whether oral or written, from any client must promptly bring such complaint to the attention of the Chief Compliance Officer. Employees are prohibited from attempting to respond to or resolve any complaint unilaterally.

The Chief Compliance Officer will review the client complaint and bring it to the attention of the appropriate members of the Firm's senior management and officers who will investigate the circumstances surrounding the complaint and determine the appropriate response. The Chief Compliance Officer or other member of senior management may consult with outside legal counsel to determine whether regulatory reporting is required.

The Chief Compliance Officer maintains records of all inquiries and complaints and accompanying responses.

5.2.7 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer is responsible for maintenance of the Firm's client account records. Records may be kept electronically in a non-rewritable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- List of terminated accounts.
- Documentation of management fee forensic testing, either as a part of the Chief Compliance Officer's annual compliance program review or in a separate report.
- Client securities class action participation documentation, if any.
- Client complaint file.

6.0 Code Of Ethics

6.1 DESIGNATION OF ACCESS PERSONS
All owners, officers, all portfolio managers, all trade personnel, all research personnel, all client services personnel, and generally all employees of the Firm are considered Access Persons of the Firm subject to these policies and procedures. Persons conducting business for another entity on the premises, that have access to the Firm's client files or trading records, are also considered Access Persons of the Firm.

6.2 ETHICAL AND REPORTING OBLIGATIONS OF FIRM ACCESS PERSONS
All Access Persons are required at all times to comply with applicable state and federal securities laws and regulations and with the provisions of the Firm's written supervisory policies and procedures and code of ethics. Any employee with knowledge of or suspicion of any facts evidencing a violation of state or federal securities laws or of the Firm's policies and procedures or Code of Ethics is required immediately to report such knowledge or suspicion to the Chief Compliance Officer, or as appropriate to another member of the Firm's senior management.

6.3 ACCESS PERSON TRADING
Access persons are subject to personal investment account trade reporting designed to ensure that no Firm client is disadvantaged in any respect by the personal investment transactions of an Access Person or his or her household member. Firm policy requires prior Chief Compliance Officer approval of all non-exempt personal trades, the Firm's receipt of account statements for all personal investment accounts and specifically prohibits trading on the basis of inside information and trading ahead of client orders (front running).

6.4 ACCESS PERSONS AND INSIDER TRADING

It is Firm policy that no staff member may engage in insider trading, *i.e.* trade, either personally or on behalf of his or her Household Members or other third-party, on the basis of material non-public information. No staff member may communicate material non-public information to others. This policy applies to every principal and staff person, and extends to activities both within and outside of their duties at the Firm.

In making its investment decisions, Adasina compiles research and investment analyses and relies on information received from outside research sources and from securities issuers.

Information that staff should consider to be material and non-public includes, among other things, information about changes in dividend policies, earnings estimates, changes in previously released earnings estimates, manufacturing problems, executive turnover, significant merger or acquisition proposals, major litigation, liquidity problems, significant new products, services or contracts, or the cancellation of significant orders, products, services or contracts. Until made public, employees are precluded from trading on such information either for their personal accounts or on behalf of client accounts. Any determination of the material and/or non-public nature of a given piece of information is to be made by the Chief Compliance Officer at her sole discretion.

All information relating to the Firm's activities, including investment analyses, investment recommendations, and proposed and actual trades for the Firm or its clients, is proprietary to the Firm and must be kept confidential except to the extent disclosure of the information is necessary to accomplish the business of the Firm and only to the extent that disclosure does not violate applicable law. Where such information is material, it should be considered non-public and employees are precluded from trading on the information or communicating it to others without the approval of the Chief Compliance Officer.

6.4.1 POTENTIAL SOURCES OF INSIDE INFORMATION:

The following are potential sources of information that the portfolio managers, trade staff and the Chief Compliance Officer monitor:

- Principals, employees, or their family and friends, that hold senior management positions with or sit on the board of directors or advisory board of a public company or a company intending to go public;
- Clients, or their family and friends, that hold senior management positions with or sit on the board of directors or advisory board of a public company or a company intending to go public; and
- Other financial industry professionals that are friends/relatives of Firm personnel or clients.

6.4.2 RESTRICTED ACCESS TO MATERIAL NON-PUBLIC INFORMATION

The Chief Compliance Officer will employ additional procedures while the Firm is in possession of material non-public information, including, but not limited to:

- Procedures for handling documents containing material non-public information, including prohibitions on removing them from the office, limiting copying and distribution within the office, keeping them off desktops and conference tables when not in use, shredding them on disposal, and other measures to protect sensitive documents from accidentally being read by anyone without a lawful need to know the information;
- Restrictions on physical access to areas of the Firm where material non-public information may be discussed or stored, including locking file cabinets and doors and a system of visitor passes or other restrictions for non-employees on the premises;
- Computer access security measures, such as passwords on files or limited access to terminals through which material non-public information can be obtained; and/or

- Trading restrictions, including temporary Firm-wide moratoria on trading in the securities to which the material non-public information relates or management review of all employee trades in certain securities.

6.4.3 NO TRADING ON INSIDER INFORMATION
No trade may be executed if there is a possibility that the basis for the trade involves inside information. If staff believes that material and non-public information is in play or has questions as to whether the information is material and non-public, the trade must be reviewed and approved by the Chief Compliance Officer prior to execution. Staff should:

- Report the desired trade immediately to the Chief Compliance Officer;
- Not purchase or sell the securities until authorized by the Chief Compliance Officer; and
- *Not* communicate, other than to the Chief Compliance Officer, the potential inside information either to persons inside or outside the Firm.

The Chief Compliance Officer makes the determination as to whether the trade is permissible and will inform the employee whether and when the trade may be executed.

6.4.4 RESPONSE TO POTENTIAL INSIDE INFORMATION
If any Adasina staff member believes that he or she may have come into possession of material non-public information, or believes the Firm's activities may have accessed or generated material non-public information, the following steps should be taken:

- Stop all trading in securities of the company that are the subject of the material non-public information, including trading on behalf of the Firm and its clients, and trading in the Access Person's personal accounts. In addition, there should be no trades in securities of the company in question in the accounts of the staff member's acquaintances or Household Members after the information is identified;
- Stop recommending any transaction in any of the securities of the company in question to anyone, including clients of the Firm, other employees of the Firm and the employee's own associates, friends or relatives. This prohibition includes making any comment about the company that could in any way be interpreted as a recommendation;
- Do not discuss the material non-public information with anyone except as required by these policies and procedures and especially avoid referring to the information in hallways, elevators, stairways, restaurants, taxis or any other place where the conversation may be overheard;
- Immediately inform the Chief Compliance Officer of all details of the situation, so that appropriate security procedures can be implemented Firm-wide; and
- Direct all requests for information of third parties to the Chief Compliance Officer, who may contact the Firm's legal counsel before determining how to proceed.

6.5 ACCESS PERSON TRADES REQUIRING PRE-APPROVAL
Access personnel and their Household Members must obtain approval from the Chief Compliance Officer for all personal securities transactions that are not otherwise exempted or prohibited. The Chief Compliance Officer's personal trades are approved by a designee of the Chief Compliance Officer. Prior trade approval is documented on an *Access Person Request for Trade Approval* and/or the Firm's trade blotter if executed through the Firm.

Access person trade approvals, once granted, are valid for 72 hours from the time of approval and expire if the trade is not executed in that time allotment. The following transactions require prior approval:

- INITIAL PUBLIC OFFERINGS AND LIMITED (UNREGISTERED) OFFERINGS. No Access Persons may purchase any security in an initial public offering, unregistered limited offering or any "hot issue" in a follow-on offering without written approval of the Chief Compliance Officer.

- SHORT-TERM TRADING. The Firm believes that personal short-term trading may increase the risk of problems arising under these policies and procedures. While the Firm leaves the extent of trading to an individual's judgment, as is consistent with his or her objectives and past trading practices, short-term trading practices must be approved by the Chief Compliance Officer and will be periodically reviewed.

- PRIVATE PLACEMENTS. A Notice Of Participation In Private Securities Transaction And Request For Approval must be submitted to and approved by the Chief Compliance Officer prior to acquiring any securities in a private placement.

- TRADING IN JSTC. JSTC is treated as a restricted security and requires written approval for purchases exceeding the de minimis threshold of 1000 shares.

If during any two consecutive calendar quarters, an employee's aggregate purchase or sale transactions exceed a cumulative amount of 5,000 shares, any subsequent transaction in JSTC during that period will no longer be regarded as a de minimis transaction and requires written approval from the Chief Compliance Officer prior to executing such a transaction.

6.6 SECURITIES EXEMPTED FROM REPORTING AND TRADE PRE-APPROVAL REQUIREMENTS

- 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[3]); and

- Shares issued by unit investment trusts that are invested exclusively in one or more open-end funds, (none of which are reportable funds managed by the Firm); or

- Purchases or sales for which the Chief Compliance Officer determines in her sole discretion that the potential for harm to clients is remote because the transactions would be very unlikely to affect market price or liquidity, or because they are not related economically to the securities to be purchased, sold or held by clients, and because they do not involve material non-public information

6.7 INVESTMENT ACCOUNTS EXEMPTED FROM REPORTING AND TRADE PRE-APPROVAL REQUIREMENTS

- Securities held in accounts over which the Access Person or household member has no trading discretion or indirect influence or control (including "blind trusts")

- Purchases or sales pursuant to an automatic investment plan;

- Acquisitions of securities through stock dividends, dividend reinvestments, splits, reverse splits, mergers, consolidations, spin-offs, and other corporate reorganizations or distributions generally applicable to all holders of the same class of securities.

6.8 UNLESS EXEMPTED, NO UNREPORTED TRADING ACCOUNTS OR TRANSACTIONS

[3] A "reportable fund" would be a fund for which the Firm served as the investment adviser or any fund whose investment adviser is an affiliate of the Firm.

Access persons and their Household Members are required to identify to the Firm all investment accounts in which the Access Person has any beneficial ownership interest and all securities transactions therein. Except as provided herein, there are no exceptions to this requirement and any violation of this policy will establish grounds for discipline or termination.

6.9 ACCESS PERSON CERTIFICATIONS

Within 10 (ten) days of hire and within 15 (fifteen) days of each quarter-end thereafter, every Access Person must execute an Access Person Certification form that Identifies all personal investment accounts and certifies that they have read and agree to abide by the Firm's Access Person trading policies and procedures and the Firm's Code of Ethics.

6.9.1 INITIAL REPORTING OF SECURITIES HOLDINGS

New staff members that are designated as Access Persons are required to identify all personal securities holdings and accounts via an Initial Access Person Certification within 10 days of hire and the information provided must be current as of 45 days of hire. New personnel must also provide to the Chief Compliance Officer copies of a current statement for each of their individual investment accounts that include the following information:

- The name of any broker, dealer or bank with which the access person maintains an account in which any securities are held for the access person's direct or indirect benefit
- The title and type of security, and as applicable the exchange ticker symbol or CUSIP number
- The number of shares, and
- The principal amount of each reportable security in which the access person has any direct or indirect beneficial ownership.

To the extent an employee owns securities that are not reflected on a custodian/brokerage statement, the employee must indicate this on their Initial Access Person Certification, and provide the Chief Compliance Officer with any documentation deemed necessary to report such holdings.

6.9.2 QUARTERLY TRANSACTIONS REPORTING

Within fifteen (15) days of each quarter's end, Access Personnel are required to report to the Chief Compliance Officer all personal securities holdings and transactions via a *Quarterly Access Person Certification and supporting custodian/brokerage statements for each relevant investment account for each month of the relevant quarter.* This policy covers accounts held in the name of another person or entity, but over which the Access Person has discretionary authority.

For each transaction, the custodian/brokerage statements must include:

- Title and amount of the security traded;
- As applicable, the exchange ticker symbol or CUSIP number, interest rate and maturity date, number of shares, and principal amount of each reportable security involved
- Date of the transaction;
- Nature of the transaction (purchase or sale);
- Price at which the trade was effected; and
- Name of the broker-dealer or bank that executed the transaction.

For each holding, the custodian/brokerage statements must include:

- The name of any broker, dealer or bank with which the access person maintains an account in which any securities are held for the access person's direct or indirect benefit
- The title and type of security, and as applicable the exchange ticker symbol or CUSIP number
- The number of shares, and
- The principal amount of each reportable security in which the access person has any direct or indirect beneficial ownership.

To the extent an employee owns securities that are not reflected on a custodian/brokerage statement, the employee must indicate this on their Quarterly Access Person Certification, and provide the Chief Compliance Officer with any documentation deemed necessary to report such holdings.

Charles Schwab & Co., Inc. ("Charles Schwab") serves as the primary custodian for the Firm's managed accounts. To the extent an Access Person maintains a brokerage account with Charles Schwab under the Firm's management, such Access Person is not required to provide monthly brokerage statements to fulfill their quarterly transaction reporting requirements. The firm will rely on reports and statements obtained directly from Charles Schwab for such accounts. For the avoidance of doubt, Access Persons who maintain custodian/brokerage accounts with firms other than Charles Schwab or with Charles Schwab, but which are not managed by Adasina, must submit monthly statements from their custodian/broker on a quarterly basis as required by this section of the Manual.

6.9.3 REVIEW OF ACCESS PERSON TRADING

The Chief Compliance Officer monitors all Access Persons' personal securities transactions to safeguard against ethical violations (such as violations of Firm policies and procedures, conflicts of interest and insider trading) by reviewing Access Persons' brokerage account statements. A designee of the Chief Compliance Officer reviews the brokerage account statements of the Chief Compliance Officer and their Household Members, if applicable. At least quarterly, the Chief Compliance Officer will verify each Access Person's compliance with the Firms trading restrictions, pre-trade approval requirements, aggregation and timing requirements and Code of Ethics by reviewing all employee and household member brokerage statements and comparing them to:

- Requests for trade approvals submitted by the employee; and
- Relevant Personal Trading Blackout Periods.

6.10 RESTRICTED SECURITIES AND "BLACKOUT PERIODS"

6.10.1 Blackout Periods

The Firm's Access Persons and persons associated with them, including Household Members, should not benefit from any price movement that may be caused by client transactions or the Firm's recommendations regarding such securities, nor should any client transaction suffer any price movement that results from any Firm or staff transactions. The Firm will use reasonable diligence to determine whether the executed transactions of its personnel through their personal investment accounts and/or accounts over which the staff member has discretionary authority, will adversely affect the interests of the Firm or its clients.

In order to avoid an event in which a Client and an Adasina Access Person trade in the same security on the same day, Adasina's Access Persons and their Household Members are restricted entirely from trading in their personal accounts during the Blackout Periods designated by the Compliance Team at the start of each calendar each year. If an Access Person or their Household Member wishes to trade any security during the Firm's Blackout Periods, pre-approval for the trade is required.

6.11 VIOLATIONS OF FIRM ACCESS PERSON TRADING POLICIES AND PROCEDURES

Sanctions will be imposed for failure to follow these policies and procedures, including but not limited to:

- Canceling of the offending trade(s);
- Disgorgement when an employee inadvertently receives an execution which is better than that of a client;
- Disgorgement is required when an employee trade constitutes a violation of the Firm's Code of Ethics.
- Termination of employment;
- Reporting the failure to regulatory authorities.
- In addition, the Firm may impose any other appropriate or required penalties.

6.12 OUTSIDE BUSINESS ACTIVITIES
The Firm's Access Persons are required to avoid any outside activities, interests or relationships that either directly or indirectly conflict with or create the appearance of the existence of a conflict of interest with their ability to act in the best interests of the Firm and its clients. If a conflict of interest or the appearance of a conflict arises between the interests of the Firm or its clients and the interest of the staff member, the interests of the Firm and its clients will prevail. The determination as to the existence or appearance of a conflict is made by the Chief Compliance Officer at her sole discretion.

It is Firm policy that no staff member may accept employment or compensation from any other person as a result of any business activity, other than a passive investment, outside the scope of his or her relationship to the Firm, unless he or she has provided prompt written notice to the Firm and received authorization from the Chief Compliance Officer. Exempted from this requirement are private securities transactions for which the Access Person has provided written notice to the Firm, received authorization for and complied with all conditions set, if any.

The following are prohibited without the prior written consent of the Chief Compliance Officer:

- Rebating, either directly or indirectly, to any person or entity any part of the compensation received from the Firm as a staff member;
- Accepting, either directly or indirectly, from any person or entity, other than the Firm, compensation of any nature as a bonus, commission, fee gratuity or other consideration in connection with any transaction on behalf of the Firm or a client account;
- Beneficially owning any security or having, either directly or indirectly, any financial interest in any other organization engaged in any securities, financial or related business, except for beneficial ownership of not more that 4.9% of the outstanding securities of any business that is publicly owned; and
- Executing transactions in securities for which any employee (or household member) sits on the board of directors or any other committee of a publicly traded company.
- No employee or their Household Members may serve as a director of any publicly- or privately-held company without prior approval by the Chief Compliance Officer

6.12.1 OUTSIDE BUSINESS ACTIVITIES MUST BE REPORTED BY EACH EMPLOYEE
on a Notice of Outside Business Activity and Request for Approval Form prior to engaging in such activity. Outside business activities which must be reviewed and approved in advance include:

- Employment or contract services that are compensated by any other person or entity;
- Participation in any other business including part-time, evening or weekend service;
- Serving as an officer, director, partner, etc. in any for-profit entity;

- Ownership of any non-publicly traded company; or
- Paid public speaking or writing activities.

6.13 CONFLICTS OF INTEREST

6.13.1 ANNUAL REVIEW OF CONFLICTS OF INTEREST

The Firm and its Access Persons are fiduciaries to Firm clients. At least annually, as a part of the senior management risk assessment effort, the Firm's principals review the Firm's business practices to identify potential conflicts of interests between the interests of the Firm and the interests of its individual clients. All identified potential conflicts of interest are evaluated and to the greatest reasonable extent, eliminated or minimized. For unavoidable conflicts of interests, the Chief Compliance Officer will review the Firm's investment advisory agreement, Form ADV Part 2, the Firm's website and other marketing materials to ensure that all appropriate disclosures are made to clients and potential clients.

6.13.2 GENERAL EXAMPLES OF AREAS WHERE CONFLICTS COULD ARISE

- Custody Arrangements
- Outside Business Activities
- Political Contributions
- Side by Side Agreements
- Trading
- Referral/Solicitation Arrangements
- Access Person Trading
- Compensation Arrangements
- Charging Performance Fees
- Soft Dollar Arrangements
- Revenue Sharing Arrangements
- Cross Trading
- Proprietary Product

6.13.3 RESOLUTION OF CONFLICTS THAT ARISE

If a conflict or the appearance of a conflict, between the interests of the Firm or its clients and the interest of staff arises, the staff member must immediately notify the Chief Compliance Officer who will take the matter under consideration, conduct any necessary investigation into the conflict or potential conflict and make a determination of what steps are to be taken. The interests of the Firm and its clients will prevail over the interests of the employee. The determination of all conflicts of interest is made by the Firm in its sole discretion. The Chief Compliance Officer will maintain records of all conflicts and potential conflicts identified, including the ultimate resolution of the conflict and the basis therefore.

6.14 STAFF COMMUNICATIONS

All staff communications with clients and third parties are subject to review by the Chief Compliance Officer and subject to applicable recordkeeping requirements. The Firm is obligated to maintain records of its communications to its clients, including, but not limited to investment advice and recommendations, records reflecting the receipt, disbursement or delivery of client securities or assets, and records documenting the execution of any trade. The Firm retains all communications related to clients and all trading activity.

6.14.1 REVIEW OF EMPLOYEE COMMUNICATIONS

All written correspondence related to the Firm's business, and in particular client correspondence is subject to review by the Chief Compliance Officer. The Firm is required to maintain records of all staff correspondence relating to clients, client accounts, client account transactions and proprietary account transactions. In addition, the Firm is required to monitor employee trading activities and compliance with the Firm's conflict of interest and insider trading policies and procedures. Consequently, it is Firm policy to archive and randomly review all employee communications, including email and other forms of electronic communication for compliance purposes. Such review, if any, may look for:

- Undisclosed client complaints
- Insider trading or selective disclosure
- Distribution of marketing materials not conforming to the Advisers Act, the rules promulgated thereunder, or applicable no-action letters (e.g., Clover Capital)
- Promissory claims or guarantee performance language
- Suspicious emails from clients who may have had their email account hacked
- Undisclosed matters requiring disclosure on an advisor's U4
- Breaches of non-public personal information or failure to follow privacy policies
- Failure to place the client's best interests first or other fiduciary failings
- Conflicts of interest
- Evidence of money laundering

Unless the Firm has subscribed to an instant messaging archiving service, staff are not permitted to communicate with clients or other third parties via instant messaging or other personal electronic messaging devices regarding any Firm business. All smart phones and other personal electronic messaging devices must be synchronized with the Firm's email server to enable the retention of client and Firm correspondence. Staff is further admonished that they may not communicate with Firm clients regarding any Firm business via any personal, non-Firm email or instant messaging account.

The Firm has adopted an email archiving system for all email. Email is subject to review and storage by the Chief Compliance Officer regardless of its nature as personal or work related. Staff is advised that they should have no expectation of privacy regarding personal communications that are sent or received via their Firm email account.

6.15 PROSPECTIVE EMPLOYEE DUE DILIGENCE

The Chief Compliance Officer is responsible for reviewing the qualifications of all prospective professional-level staff members. A determination is made as to whether the applicant is, or has ever been subject to statutory disqualification under state or federal securities laws. In making the determinations to hire, she may rely on the information provided to the Firm by the applicant. If she determines that such information is inadequate, the Chief Compliance Officer will make an independent investigation of the applicant. Such investigation may include a background check by a consumer reporting agency, an online examination of the character, business reputation, qualifications and experience of the applicant, and a verification of all information submitted for the

registration of such person. Investigation into whether the applicant is, or has ever been subject to statutory disqualification from employment in the industry is conducted.

6.15.1 REVIEW OF PRIOR INDUSTRY REGISTRATION FILINGS
If the prospective employee was previously a registered representative of a broker-dealer or a registered investment advisor representative, a pre-hire review of the applicant's Forms U-4 /U-5 is conducted. Copies of candidate's Forms U-4/U-5 are requested by the Chief Compliance Officer along with obtaining a written authorization from the candidate for the Firm to review these records.

6.15.2 DUE DILIGENCE INVESTIGATION OF PRIOR EMPLOYMENT
It is the policy of the Firm to contact each applicant's employers (if possible and practical) for the prior two positions of employment. In the event complaints, investigations or actions were brought, the applicant may be given an opportunity to explain the reasons for and outcome of any such complaints, investigations and/or regulatory actions.

6.15.3 REGULATORY INVESTIGATION, DISCIPLINARY ENFORCEMENT, LITIGATION
Any staff member that becomes the subject of a regulatory investigation, disciplinary enforcement action or litigation, or is served with a subpoena, or becomes subject to any judgment, order or arrest, or is contacted by any regulatory authority must immediately inform the Chief Compliance Officer of such.

6.16 CONFIDENTIALITY OF CLIENT AND PROPRIETARY INFORMATION
Any information regarding advice that the Firm furnishes to client accounts, the identity of securities and other investments owned or being considered for purchase by or for any client account, all methods and strategies that the Firm currently uses or develops in the future to decide how or when to purchase and sell securities and other investments, and other proprietary data or information about the Firm or its clients is strictly confidential and a trade secret and may not be revealed to third parties, except as required for Firm business, or as approved by the Chief Compliance Officer.

Employees also may not disclose the identity, affairs or investments, or other client information, of any current, potential or former client to anyone outside of the Firm, except as authorized by the client or required in servicing the client (such as disclosure to a brokerage firm at which client account assets are held) or for the business of the Firm (such as disclosure to the Firm's auditors and lawyers or as required by law).

All information described above is the property of the Firm. Disclosing any such information to any third-party, without the permission of the Chief Compliance Officer, will subject the employee to discipline or sanctions by the Firm at the Firm's sole discretion, including fines, dismissal, suspension without pay, loss of employment compensation, loss of severance benefits, if any, demotion or other sanctions. This confidentiality obligation continues even after the termination of employment, and such information is considered trade secrets and may not be used by the employee after termination of employment.

6.16.1 MAINTAINING CONFIDENTIALITY OF PRIVATE AND PROPRIETARY INFORMATION
To protect the confidentiality of the Firm's confidential and proprietary information and the confidentiality of clients' and potential clients' records, staff should take the following additional security precautions:

- Documents containing confidential information may not be taken from the Firm's offices, downloaded to an external drive, or emailed or otherwise shared externally for non-business purposes without the prior consent of the Chief Compliance Officer, and any copies removed from the Firm's offices or computers must be promptly returned or permanently and securely deleted. Photocopies of confidential information may only be made as required, and all copies and originals of such documents must be disposed of in a way that keeps the information confidential. Electronic records containing confidential information must be stored, accessed and used exclusively within the Firm's electronic storage. Employees are not permitted to download such records to any local drive or storage device, including any device provided by the Firm to the employee.

- Physical access to any non-electronic confidential information must be limited by either locking or monitoring access to the offices and storage areas where such information is located.

- Visitors to the Firm's office shall be monitored and/or accompanied by a staff member.

At times, the Firm may enter into one or more agreements with third parties, pursuant to which the Firm may provide access to confidential information to those third parties. If this occurs, the Firm will protect the privacy of confidential information and include in such agreements provisions protecting confidential information to the extent required by law.

6.17 ENTERTAINMENT, GIFTS AND POLITICAL CONTRIBUTIONS

The giving or receiving of gifts or other items of value to or from persons doing business or seeking to do business with the Firm could be considered as a form of bribery, raise conflicts of interest or otherwise call into question the independence of the Firm's judgment as a fiduciary to its clients. Accordingly, it is the policy of the Firm to permit such conduct only in accordance with the limitations stated herein. ALL GIFTS AND ENTERTAINMENT WITH A VALUE IN EXCESS OF $100 MUST BE REPORTED TO THE CHIEF COMPLIANCE OFFICER. Limited exceptions to these policies may be made with the written approval of the Chief Compliance Officer.

The Firm's policies on gifts and entertainment are derived from industry practices. If there is any question about the appropriateness of any particular gift, employees should consult the Chief Compliance Officer. Under no circumstances may a gift to the Firm or any employee be received as any form of compensation for services provided by the Firm or employee. The Chief Compliance Officer reviews all reports or other documentation regarding employee expense reimbursement to monitor compliance with this policy, and maintains an Entertainment and Gift Log for each year.

Accepting Gifts. On occasion, because of an employee's position with the Firm, the employee may be offered, or may receive, gifts or other forms of non-cash compensation from clients, brokers, vendors, or other persons not affiliated with the Firm. Under no circumstances may a gift to the Firm or any employee be received as any form of compensation for services provided by the Firm or employee. Extraordinary or extravagant gifts are not permissible and must be declined or returned, absent approval by the Chief Compliance Officer. Single or multiple gifts (including logoed promotional items with more than a nominal value) whose reasonable aggregate value is no more than $350 annually from a single giver may be accepted. Gifts of logoed promotional items with a nominal value (*e.g.*, pens, mugs, tote bags etc.) may be accepted.

Accepting Meals and Entertainment. Employees may accept customary business lunches, dinners, or entertainment at which both the employee and the giver are present (*e.g.*, sporting or cultural events). Extraordinary or extravagant entertainment events are not permissible and must be declined. All such meals and entertainment must be pre-approved by and/or reported to the Chief Compliance Officer.

Accepting Payments for Tuition or Fees to Conferences or Other Industry Events. *[NOTE: No tuition or expenses for conferences or industry events should be accepted if to do so would violate the Firm's soft dollar policies by falling outside the soft dollar "safe harbor".]* Employees may accept payments for tuition and expenses to conferences and other industry events as long as they are paid for by the sponsor of the event, they are held in an appropriate location, participation is not conditioned on meeting sales targets or other incentives and payments do not include expenses related to the employee's spouse or other guests. All such payments for tuition for conferences and meetings must be pre-approved by and reported to the Chief Compliance Officer, or in the case of the Chief Compliance Officer's participation, by another member of the Firm's senior management.

Giving Gifts to Industry Professionals and Vendors. Gifts to any broker-dealer, other industry professional, vendor or other person may not be used to correct a trade error or to offset any amount otherwise due to the recipient. Employees may not give any gift(s) with an aggregate value in excess of $350 per year to any person associated with a securities or financial organization, including exchanges, broker-dealers or other investment management firms, or to members of the news media.

Giving Gifts to Clients and Prospective Clients. Gifts to a client may not be used to rebate or refund fees, compensate a trade error or offset any amount due to the client. Employees may not give clients any gift(s) with an aggregate value in excess of $350 per year. Employees may not give prospective clients gift(s) with an aggregate value in excess of $100 per year.

Providing Entertainment. Employees may provide reasonable (neither extraordinary nor extravagant) entertainment to clients or prospective clients provided that both the employee and the recipient are present and there is a business purpose for the entertainment.

Solicitation of Gifts. All solicitation of entertainment, gifts or gratuities from any client, broker-dealer, vendor or other person is unprofessional and is strictly prohibited.

Client Complaints. Individual employees may not make payments to or waive fees from clients to resolve a complaint. All such matters must be handled by the Chief Compliance Officer.

ERISA Considerations. The acceptance of any form of compensation (not limited to gifts, entertainment, soft dollar research or brokerage services, conference tuition, charitable contributions) may rise to the level of "third-party compensation" under the ERISA fiduciary rule. All such forms of compensation must be reported to and approved by the Chief Compliance Officer. Further, ERISA prohibits the acceptance of fees, kickbacks, gifts, loans, money, and anything of value that are given with the intent of influencing decision-making with respect to any employee benefit plan. The acceptance or offering of gifts, entertainment or other items may be viewed as influencing decision-making and therefore unlawful under ERISA. In addition, many public employee benefit plans are subject to similar restrictions. Employees should never offer gifts, entertainment or other favors for the purpose of influencing ERISA client or prospective client decision-making. Similarly, employees should not accept gifts, entertainment or other favors offered by others who wish to do business with the Firm or its ERISA clients.

Political Contributions (No "Pay to Play"). Portfolio managers entities (e.g., for government sponsored pension plans) by making political contributions to public officials of such public entities have compromised their fiduciary duty. Therefore, the Firm and its employees are prohibited from directly or through a third-party making political contributions (whether in the U.S. or to non-U.S. officials), in excess of $350 to any public official *affiliated with a current or potential public entity client of the Firm* for which the employee is eligible to vote and/or in excess of $150 if for a public official for which the employee is not eligible to vote. Political contributions include payments to political action committees, political parties, inauguration/transition committees and to foundations or other charitable organizations associated with the public official.

All political contributions made by any Firm employee, regardless of amount or jurisdiction of the recipient, must be submitted to and approved by the CCO prior to making the contribution. Employees must use the Political Contribution Pre-Approval Form for such requests. The Chief Compliance Officer shall review all reports of political contributions upon receipt to determine potential conflicts of interest and compliance with this Manual. Political contributions made by the Chief Compliance Officer are reviewed by her designee.

6.18 WHISTLEBLOWER PROCEDURES ANTI-RETALIATION

Adasina will not retaliate or in any other way discriminate against any employee (whistleblower) that, whether at the initiative of the employee or in the ordinary course of the duties of the employee, has reported to or otherwise provided information to any governmental inquiry or judicial proceeding regarding any violation of state, federal or international law or objected to, or refused to participate in, any task that the employee reasonably believes to be in violation of any state, federal or international law or the Firm's fiduciary duties to its clients.

6.18.1 REPORTING PROCEDURE

The Firm has an open-door policy and encourages Access Persons to share their questions, concerns, suggestions or complaints with the Chief Compliance Officer. If a staff person is not comfortable reporting to the Chief Compliance Officer or the matter relates to the Chief Compliance Officer, the Access Person may report the matter to a member of senior management. If the Access Person is not satisfied with the Chief

Compliance Officer's or senior management's response, the Access Person is encouraged to speak with the with the Firm's outside corporate counsel, Wendy Phillippay of Best Practices Consulting Group, 19201 Sonoma Highway, No. 162

Sonoma, CA 95476, PHONE 707-939-3531, EMAIL bestpracticesgroup@hotmail.com, who has the authority to investigate all reported complaints of potential violations of federal or state law or the Firm's fiduciary duty to its clients.

6.18.2 CONFIDENTIALITY
Violations or suspected violations may be submitted on a confidential basis by the whistleblower. Reports of violations or suspected violations will be kept confidential to the extent possible, consistent with the need to conduct an adequate investigation.

6.18.3 HANDLING OF REPORTED VIOLATIONS
The Firm's Chief Compliance Officer or outside counsel will notify the person who submitted a complaint and acknowledge receipt of the reported violation or suspected violation. All reports will be promptly investigated and appropriate corrective action will be taken if warranted by the investigation.

6.18.4 ACTING IN GOOD FAITH
A whistleblower complaint concerning a violation or potential violation of applicable securities laws or Firm fiduciary responsibilities must be made in good faith and the person reporting the violation/possible violation should have reasonable grounds for believing the information disclosed indicates a violation and is true. Allegations that prove not to be substantiated, are without basis for a reasonable belief of a violation or which prove to have been made maliciously or knowingly to be false may be viewed as a disciplinary matter resulting in sanctions or termination.

6.19 SANCTIONS FOR VIOLATION OF FIRM POLICIES AND PROCEDURES
Any persons who violate any of the Firm's employee personal trading, insider trading, conflicts of interest or other Code of Ethics policy or procedures are disciplined by the Firm and subject to any of the following sanctions, among others not listed:

- Cancellation of trades
- Disgorgement of profits
- Orders to sell positions, even at a loss
- Fines
- Termination of employment
- Reporting to regulatory authorities to the extent required by law

7.0 Compliance Program Maintenance And Examinations

7.1 RISK ASSESSMENT
As a function of the Firm's fiduciary duty to its clients, Senior Management periodically evaluates the associated risks and associated internal control systems related to the Firm's business and operations. Risk monitoring is intended to identify the factors affecting the risk and return of clients' investments and the risk to the Firm itself of its business activities.

7.1.1 ANNUAL SENIOR MANAGEMENT RISK ASSESSMENT
At least annually, senior management along with the Chief Compliance Officer conduct a risk assessment of the Firm's business and operational practices taking into consideration any risks or potential risk that may have resulted in connection with:

- Changes in officers or officer job responsibilities;
- Changes in the Firm's investment strategy;
- The introduction of a proprietary investment vehicle;
- The hiring of new employees;
- Changes in Firm marketing and advertising practices;
- Changes in third-party service providers;
- Upgrades to Firm technology hardware or new software or service providers; and/or
- Current cybersecurity threats.

An *Annual Senior Management Risk Assessment Checklist* is included in this Manual..

7.1.2 ANNUAL COMPLIANCE PROGRAM REVIEW
The Chief Compliance Officer is responsible for conducting an annual review of the Firm's compliance program. The annual review should document:

- A detailed assessment of the Firm's compliance with its internal operational and compliance policies and procedures during the preceding year;
- A survey of new or amended SEC regulations; and
- A review of existing policies and procedures to identify new or modified procedures recommended for adoption and inclusion in the Manual.

An *Annual Compliance Program Review Checklist* is included in this Manual..

7.1.3 INTERIM COMPLIANCE REVIEWS
As necessary, the Chief Compliance Officer conducts periodic interim inspections of the various Firm functions addressed in these policies and procedures to verify compliance. She maintains a log of Compliance Reviews noting each such review. Any findings of non-compliance are immediately addressed.

7.2 SEC BOOKS AND RECORDS REQUIREMENTS
All required documentation may be kept in hard copy or electronic format for a period of no less than 5 years. Documents must be maintained in a format that may be immediately produced or reproduced upon request from a regulator. If documents are stored electronically, the following requirements must be met under SEC Rule 204(g) which permits micrographic and electronic storage of records provided:

- Records are arranged and indexed in a way that permits easy location, access, and retrieval of any particular record;
- Records are provided promptly upon request by the SEC or any other regulator;
- Records are legible, true, and complete in the medium and format in which it is stored;
- A legible, true, and complete printout of the record can be provided;

- There is proper means to access, view, and print the records; and
- Records are separately stored, for the time required for preservation of the original record, a duplicate copy of the record on any medium allowed by this section.
- Procedures must ensure the maintenance and preservation of the records, so as to reasonably safeguard them from loss, alteration, or destruction;
- Access to the records is limited to properly authorized personnel and the SEC (including its examiners and other representatives); and
- Reasonable steps have been taken to ensure that any reproduction of a non-electronic original record onto any electronic storage media is complete, true, and legible when retrieved from the electronic storage device.

7.3 REGULATORY EXAMINATIONS
All federally registered investment advisory firms are subject to regulation and periodic examination by the SEC. All regulatory contacts with the SEC must be referred to the Chief Compliance Officer. All regulatory actions initiated or examinations scheduled by the SEC are coordinated by the Chief Compliance Officer. The Chief Compliance Officer is responsible for coordinating the Firm's response to correspondence with relevant regulators and overseeing the implementation of all required operational and compliance procedural changes.

8.0 Custody Of Client Assets

8.1 NO CUSTODY OF CLIENT ASSETS
The Firm does not maintain physical custody of client funds or securities. All clients are required to establish custodial accounts with a broker dealer, bank or other qualified custodian.

8.2 "DEEMED" CUSTODY DUE TO DIRECT FEE WITHDRAWAL
In most cases, the Firm is authorized to instruct the client's custodian to withdraw and transfer the Firm's investment management fees directly from the client's custodied investment account. Consequently, the Firm is deemed to have limited custody of client assets under applicable rules. The fact that its custody is "limited" allows the Firm to avoid having to state on its Form ADV Part 1 that it has custody of client assets. More importantly, this limited custody exempts the Firm from the requirement that it retain the services of an independent public auditor to conduct an annual surprise examination of the client assets it manages.

8.3 TESTING OF MANAGEMENT FEES TO PRESERVE THE FIRM'S LIMITED CUSTODY STATUS
Any over assessment of client management fees may result in the determination that the Firm has custody of client assets equal to the amount of the overcharges.

8.4 CUSTODY CONFERRED BY CERTAIN CLIENT STANDING LETTERS OF AUTHORIZATION
A client standing letter of authorization ("SLOA") or other client directive that authorizes the Firm to make a transfer of assets from the client's investment account to a third-party account or to a like-titled client account held at a different custodian will not confer "custody" to the Firm if, and only if it specifies the exact timing and amount of the transfer and identifies the recipient's name and address or the recipient account number - including the ABA routing number(s) and name of the receiving custodian.

The Firm is deemed to have custody of client account assets – and is required to answer "yes" to the custody questions on ADV Part 1A, Item 9 if any Firm client issues an SLOA to their custodian that does not specify both the exact amount and exact timing of the authorized transfer but nevertheless authorizes the Firm to make money transfers to third parties or other client accounts held away from the custodian. If the following conditions are met by the Firm, the client and the custodian, with respect to each SLOA established the Firm will NOT be required to have the client's investment account(s) subjected to an annual surprise examination by a qualified, independent accountant/auditor:

- The client provides an instruction to the qualified custodian, in writing, that includes the client's signature, the third-party's name, and either the third-party's address or the third-party's account number (including the ABA routing number(s) or name(s) of the receiving custodian) at a custodian to which the transfer should be directed.

- The client authorizes the investment adviser, 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.

- NOTE: The Firm is allowed to determine the exact timing and amount of the transfer as long as all other conditions are met.

- The client's qualified custodian performs appropriate verification of the instruction, such as a signature review or other method to verify the client's authorization and provides a transfer of funds notice to the client promptly after each transfer.

- The client has the ability to terminate or change the instruction to the qualified custodian.

- The investment adviser has no authority or ability to designate or change the identity of the third-party, the address, or any other information about the third-party contained in the client's instruction.

- The investment advisor maintains records showing that the third-party is not a related party of the investment adviser or located at the same address as the investment advisor (an acknowledgement by the client via email or otherwise, or a note to the file detailing that the third-party is not affiliated with or related to the Firm or an employee and is not located at the same address as the Firm or any employee.)

- The client's qualified custodian sends the client, in writing, an initial notice confirming the instruction and an annual notice reconfirming the instruction.

8.5 OTHER PRACTICES THAT WOULD CONFER CUSTODY OF ASSETS ON THE FIRM

The following practices would confer custody of client assets with the Firm and such custody would require an annual surprise examination by an outside, qualified auditor. Therefore, no employee, officer, principal or the Firm itself may engage in the following practices without prior written approval of the Chief Compliance Officer:

- Manage client assets that are not held at a qualified custodian that sends client account statements directly to the client at least quarterly;

- Act as the general partner, managing member or principal of any client partnership, company or other entity that is not annually audited according to Generally Accepted Accounting Principles (GAAP) standards by an auditor that is registered with and examined by the Public Company Accounting Oversight Board (PCAOB) or whose offering memoranda or subscription agreements do not require such audits;

- Have signatory power over any client's or client entity's financial accounts without Firm approval;

- Have the power to effect any transfer of funds from a client's account to any third-party or non-Schwab/Folio outside account even if "like titled" and owned by the client without a written authorization required by the custodian of the account signed by the client specifying the payment details;

- Hold any client's securities or funds in his, her or its name at any financial institution;

- Physically possess or hold cash or securities of any client, including subscription agreements to private investments if they constitute the only indicia of ownership;

- Have an unlimited general power of attorney over a client's account;
- Hold client assets through any Firm affiliate;
- Hold status as a “related entity” to a qualified custodian that is not operationally independent of the Firm.
- Receive the proceeds from the sale of client securities or interest or dividend payments made on a client's securities or checks payable to the Firm except if intended by the client as payment for advisory fees and documented in writing;
- Act as a trustee, executor or guardian for any advisory client trust, estate or guardianship, unless the trustee or executor relationship is based upon a pre-existing family or personal relationship with the decedent, grantor or guardian (and not a result of the staff member’s employment with this or a prior firm); or
- Act as a client’s independent representative for purposes of receiving brokerage account statements, bank statements or other statements from qualified custodians.

8.6 ANNUAL SURPRISE EXAMINATION REQUIREMENT FOR ASSETS UNDER CUSTODY
If the Firm has custody of client assets by virtue of acting as a trustee of a client trust, by accepting a general power of attorney, by acting as the general partner or managing member of a client fund or by having the authority to transfer funds out of a client account without meeting the above criteria (see Section 2.0), it is required to retain the services of a qualifying independent certified public accountant (both registered with and supervised by the Public Company Accounting Oversight Board (“PCAOB”) to annually conduct either a full audit of the assets or a surprise examination of the assets under custody. At such time as the Firm acquires such custody, if ever, additional procedures meeting the surprise exam requirement will be adopted.

8.7 INADVERTENT RECEIPT OF CLIENT ASSETS
No Firm personnel may accept cash, checks, money orders, stock certificates or any other assets from a client. The Firm’s receipt of a client’s third-party check made payable to a custodian does not confer “custody” of client assets, but the check must be forwarded to the custodian as soon as possible and in no case greater than three business days from receipt.

As a courtesy to clients, and only where the Firm has determined that no alternative method of payment (direct deposit of payments to client accounts) is available, the Firm may accept payments on behalf of clients from (independent third-party) taxing authorities, class action administrators and private investment administrators as long as

- The payment and the client are promptly identified;
- The nature of the payment, its receipt by the Firm and its ultimate disposition are promptly documented in the Firm’s records;
- The payment is either forwarded to the client or deposited into the client’s qualified custodial account promptly but in no event in more than three business days after the Firm’s receipt;
- If not forwarded to the client or deposited in the custodial account, the payment is returned to the originating authority or administrator, but in no event in more than three business days after receipt.

In the event other (those not described above) client assets are inadvertently received by the Firm, the Chief Compliance Officer must be informed immediately and the following steps taken on the same or next business day, but not later than the third business day from receipt, and documented:

- Determine from whom the assets were received, whether client or client relative or representative, custodian or issuer.

- Telephone the sender of the assets and inform them that the Firm cannot accept the assets and make arrangements to return them.
- If the sender requires assistance in obtaining an address for the proper recipient (either the client or the client's custodian), provide current address information.
- Return the assets to the sender by one of the following methods.
    - Messenger (obtain delivery confirmation)
    - Overnight Delivery (obtain delivery confirmation)
    - First class mail.
- DO NOT UNDERTAKE TO FORWARD THE ASSETS TO THE PROPER RECIPIENT. THEY MUST BE RETURNED TO THE SENDER.

Pending return of the assets, they should be secured in a locked (fire safe) place within the Firm.

9.0 Electronic And Technology Systems and Cybersecurity Planning

9.1 FIRM ELECTRONIC AND TECHNOLOGY SYSTEMS
The Firm's electronic facilities and technology systems are the property of the Firm and are to be used for legitimate business purposes only. Staff members are provided with access to these systems to assist them in the performance of their jobs. All staff members have a responsibility to use the Firm's resources in a professional, lawful and ethical manner. Abuse of the Firm systems may result in disciplinary action, including possible termination, and civil and/or criminal liability.

As appropriate, limited personal use of the Firm's technology systems is permitted if such use does not:

- Interfere with the Firm's business or with any staff member's ability to perform their job responsibilities or;
- Violate any other Firm policies, provisions, guidelines or standards.

All laptops and computers provided by the firm are equipped with anti-virus software designed to protect the local device. The firm uses Gmail for emailing services, which contains built-in software that scans and filters email containing viruses, spam and other questionable content and may alert the Firm's system administrators to unauthorized activity and penetration of the Firm's security systems. [Note that some types of encrypted email cannot be scanned for viruses and staff members should always remain alert to the sender and stated purpose of incoming email.]

Staff members are advised not to install onto computers, laptops, tablets or smartphones any software, files or programs (including, but not limited to, any instant messaging program) purchased by the employee or downloaded or obtained from external sources without prior approval by the Firm.

Staff members must not use Firm computers or other electronic equipment and/or communications systems or internet access to send, receive, download, upload, access or review any unsecured and/or unsolicited material that may contain worms, viruses, Trojan horses or other computer programming routines or engines that are Intended to damage, detrimentally interfere with, surreptitiously intercept or expropriate any system, data or information.

The Firm does not guarantee the privacy of the electronic communications of its staff members, consultants, independent contractors, or 3rd party providers, using Firm electronic and technology systems. In order to promote and improve quality control, client relations, prevention of system misuse, investigation of misconduct,

compliance with legal requirements applicable to the Firm and compliance with legal and regulatory requirements, the Firm supervises and may monitor any communications that occur via Firm electronic and technology communication systems. Use of the Firm's communication facilities and electronic systems constitutes an acknowledgment by each staff member or affiliated person of the Firm's supervision and monitoring activities.

Documents and communications created on, downloaded to, received through or transmitted over Firm electronic and communication systems remain in the Firm's archived records, are subject to regulatory review and are reviewed by the Firm in connection with troubleshooting hardware and software problems, preventing system misuse, investigating misconduct and potential violations of applicable laws and regulations, assuring compliance with software distribution-policies, and assuring compliance with other legal requirements applicable to the Firm.

The Firm reserves the right to review, read, access or otherwise monitor all electronic documents and messages that are created on, received through, downloaded to, stored or processed on the Firm's computers or via other electronic equipment and communications systems, including any that may not directly relate to the Firm's business. Additionally, the Firm has the right to identify and block user access or e-mail containing material which is inappropriate in the workplace in accordance with the guidelines set out in this policy.

Staff members may not illegally use or copy illegal material, licensed material and material protected under copyright law or make that material available to others for copying. Staff members are responsible for complying with copyright law and licenses that may apply to software, files, graphics, documents, messages and other material you wish to use, download or copy. No software purchased by the Firm may be copied or reproduced for personal or business use. Staff members may not use the communications equipment, including, but not limited to, Firm telephones, facsimiles, computers (including smart phones, iPads, tablets, etc.), voice mail, e-mail system and Internet access to knowingly send, receive, download, upload, access or review any material that infringes on the intellectual property, privacy or publicity rights of others.

Staff members may not use Firm electronic facilities to knowingly send, receive, download, upload, access or review any material that constitutes a chain letter or pyramid scheme.

Staff members may not use Firm electronic facilities to knowingly send, receive, download, upload, access or review any material that is obscene, defamatory, racially, sexually or religiously discriminatory, threatening, harassing, abusive, sexually explicit, hateful or intended to annoy, harass or intimidate anyone, anywhere at any time.

E-mail has the same permanent and legal status as written hardcopy documents, and may be subject to disclosure obligations in exactly the same way. The professional standards that apply to hard copy correspondence must be observed for e-mail. Email to outside organizations may have the same power to create a binding contract as other hardcopy documents.

Unless explicitly authorized to do so, staff members are prohibited from sending, transmitting, or otherwise distributing confidential information belonging to the Firm. Unauthorized dissemination of such material may result in severe disciplinary action, including dismissal, as well as civil penalties and possibly criminal penalties.

9.2 POLICIES
The following general policies should guide employee use of Firm electronic systems:

It is Firm policy to take all reasonable steps to:

- Identify all current cybersecurity risks that threaten the security of Firm and Firm client data and assets;
- Identify all reasonable avenues for eliminating or mitigating all such risks;

- Routinely test the Firm's electronic hardware and software to determine the effectiveness of its cybersecurity mitigation measures; and
- Conduct periodic cybersecurity training for Firm employees and affiliated persons.

USE OF FIRM NETWORKS

- Use good judgment: Employees are responsible for exercising good judgment with respect to the accessing of and use of Firm electronic systems and networks.
- Software downloads: Avoid unnecessary downloads or install any unauthorized software on Firm computers while exercising caution.
- User-level network security: We consider what files each person needs access to perform their work, as well as who should have administration rights.
- Remote access: Employees who can access the Firm's network remotely are limited to a "need to access" requirement. By accessing the Firm network from non-Firm-owned electronic devices, employees agree to manage the security of their remote workspace with the same degree of care as one does their office workspace.
- Antivirus and Malware Protection: Security software is included on Firm-owned computers and laptops. Security software (Sophos, McAfee, Norton, others) for employee-owned electronics used to access the Firm network is mandatory.

EMAIL

- Transmission of Private Client Data: At any time that you are transmitting private client data to a client or third-party, the file must be encrypted or password-protected.
- File attachments: Exercise care with file attachments, especially if from unknown senders – use common sense and exercise caution.

WEBSITES & APPLICATIONS

- Passwords: Storing or saving passwords on third-party websites is prohibited. "Strong Password" policies must be adhered to.
- User-level security: Access to administered website resources (e.g. custodians, performance reporting, and rebalancing) is generally defined by and limited to functional role; this also helps maintain span of control and reduces risk of fraud.
- Multi-factor authentication: Enable multi-factor authentication on company-related websites and applications if possible. This is sometimes inconvenient, but we have weighed the risk of inconvenience against the risk of a security incident, and its clear information security is the higher priority. Be sure to manage the security of your multi-factor authentication tokens and report any loss of malfunction to the CCO and Systems Manager.

WORKING REMOTELY

- All access to each remote device used which was provided by the Firm (phone, tablet, laptop) requires a secure password.
- Laptops and computers that are provided to employees by the firm are pre-programmed to time-out after 30 minutes of inactivity. Employees are required to maintain this setting on devices provided by the firm.

- Each device provided by the firm limits the number of password “tries” before the device automatically prevents access.

- No software programs or applications that are intended to connect the device to the Firm’s database or to any cloud data storage should be set up without dual factor authentication – access to Firm data must require the entry of a program - or app-specific secure password each time the device is used to logon to the software program or app. It is recommended that such a program or app password should be different than that used to access the device.

- No firm data may be stored locally on any laptop, tablet, smartphone or hard drive, without approval from the Chief Compliance Officer. Remote access via laptop, smart phone and tablet to the Firm’s databases is facilitated for authorized personnel, thus storage on any device unnecessarily exposes the data to hacking.

- With remote access to the Firm’s network and data storage facilitated for authorized personnel, there should be no need to transfer and transport data via an external drive. Downloading any Firm data or files to an external drive is strictly prohibited for all Firm employees, with the sole exception of data or files downloaded to a local drive on a device provided by the Firm.

- The loss of any electronic device containing client data must be reported to the Chief Compliance Officer and IT Department immediately.

9.3 APPOINTMENT OF CYBERSECURITY COMPLIANCE TEAM
Firm senior management has appointed Maya Philipson, Chief Compliance Officer as the head of the Cybersecurity Compliance Team.

9.4 IDENTIFICATION OF CYBERSECURITY RISKS
The Firm relies upon an in-house computer network that connects to the internet, through which it accesses custodian-provided or subscription services for investment research, market monitoring, securities trading, portfolio tracking, trade reconciliation, portfolio reporting and account invoicing, recordkeeping of client files, database management, amongst a variety of other services. Security risks are present at each intersection of the Firm’s activities and the computer resources it relies upon. All Firm employees must remain alert to the following types of security risks, amongst others:

- Malware (viruses, worms, etc.) installed on the Firm’s computer network via insecure internet connections, software integrations, and through email attachments;

- Denial of service attacks limiting access to the Firm’s website or client portal;

- Subscriptions to online trading, portfolio management, data storage, client portal, proxy voting, class action settlement or other industry service platforms that are not in themselves secure;

- Software or hardware malfunctions that prohibit access to the Firm’s network or utilization of the firm’s firewall;

- Breach of the Firm’s network by an unauthorized user;

- Compromise of a client’s or a third-party consultant or vendor’s computer which is then used to remotely access the Firm network or client information;

- Receipt by the Firm of fraudulent client emails seeking to authorize wire transfers of client funds; and/or

- Employee misconduct that uses client data to misappropriate client assets or that damages or destroys the Firm’s reputation, network, or data.

In the event of any of the above security failures, staff should immediately inform the Cybersecurity Compliance Team who will determine whether private client data or client assets have been affected and whether the Firm

must notify: the affected client(s), law enforcement, FinCEN - Financial Crimes Enforcement Network (file a suspicious activity report) and/or the Firm's primary regulator.

9.5 OUTSIDE INFORMATION TECHNOLOGY CONSULTANT
The Firm retains the services of an outside IT consultant to ensure that all electronic data processing and storage is conducted over secure in-house networks and secure internet systems. In conjunction with the IT consultant, the Firm creates and periodically reviews the following as a part of its CyberSecurity Plan:

- The IT consultant prepares and ships devices according to our specifications. They factory restore and store old devices and manage the firm's computer inventory.
- An inventory of primary physical electronic devices and software systems used by the Firm and its employees;
- A map of network resources, connections, and data flows, including the identification of where any client data is stored, and a record of updates thereto; and
- The capability to create an audit log of all remote connections to the Firm's network, software applications, or data storage sites from external sources.

The Compliance Team works with the IT consultant to:

- Identify all pre-existing and new cyber security risks facing the business community in general and the securities industry in particular and conduct a risk assessment on the Firm's network, email, client portal, software subscriptions and data storage security in light thereof;
- Establish and monitor policies to control the access to private client data by Firm employees, outside consultants, vendors and online subscription providers of client services platforms;
- Test the login capabilities and practices of the Firm's network and systems to assess their adequacy, appropriate retention of credentials and security; and
- Assist the Cybersecurity Compliance Team in reviewing available cyber security insurance policies and determining which, if any are available to and suitable for the Firm and its business, including any policy currently covering the Firm's operations.

The Cybersecurity Compliance Team works with the IT consultant to provide information and system testing documentation related to Firm's information technology cyber security efforts, and as necessary assists the Firm in describing and explaining such efforts, to all regulatory examiners.

9.6 CYBERSECURITY TRAINING
At least annually, the Cybersecurity Compliance Team conducts periodic cybersecurity training of all staff and affiliated persons.

10.0 Business Continuity And Disaster Recovery

- **EMERGENCY CALL-IN NUMBER** - via Ruby Reception service **(415-986-5500)**
- **EMERGENCY CONTACT PERSONS**
- Rachel Robasciotti: rachel@adasina.com
- Maya Philipson: maya@adasina.com

10.1 POLICIES
It is Firm policy to respond to a significant business disruption by safeguarding employees, minimize risk to facilities, ensure that client assets are protected, and to resume the business of the Firm. In the event that we determine we are unable to continue our business, we will assure Clients prompt access to their accounts. It is

Firm policy to maintain a current Business Continuity and Disaster Recovery Plan at all times and to ensure that Firm employees are trained to respond to any disaster in accordance with adopted procedures.

The Firm maintains copies of its Business Continuity and Disaster Recovery plan (BCP) and annually reviews and updates it. An electronic copy of our plan is located on cloud-based data storage. A hard copy of these policies and procedures is distributed to the Cybersecurity Compliance Team, our IT consultant, and/or their designee and is kept in an offsite location so that it will be accessible in the event of a disaster or other emergency.

DISASTER RECOVERY COORDINATION
All disaster recovery coordination will be conducted by the Chief Compliance Officer, or in her absence, by the Firm principals.

SIGNIFICANT BUSINESS DISRUPTIONS
Significant business disruptions can be either internal or external and vary in their scope, such as only the Firm, a single building housing the Firm, the business district where the Firm is located, the city where we are located, or the whole region. Within each of these areas, the severity of the disruption can also vary from minimal to severe. In a disruption to only the Firm or a building housing the Firm, we will transfer our operations to local sites as and when needed. In a disruption affecting our business district, city, or region, we will transfer our operations to sites outside of the affected area.

We will also consider susceptibility to evolving risks and disruptions that may result from an infectious pandemic and prepare accordingly. In either situation, we plan to continue in business, and notify clients via our email or website www.adasina.com . We maintain an emergency number for the Firm that clients can use to contact us. If the significant business disruption is so severe that it prevents us from remaining in business, we will assure our clients receive prompt access to their funds and securities through our custodial firm(s).

In the event of departure of key personnel, fraudulent acts, or technology failure the Chief Compliance Officer, will confer with principals and most senior staff to determine a course of action, disclose to clients, and report to law enforcement and regulatory agencies as and when necessary.

FINANCIAL AND OPERATIONAL RISK
In the event of a significant business disruption, we will determine the value and liquidity of our investments and other assets to evaluate our ability to continue to fund our operations and remain in capital compliance. We will contact our custodial firms, banks and creditors to apprise them of our financial status. If we determine that we may be unable to meet our obligations to those third parties or otherwise continue to fund our operations, we will request additional financing from our bank or other credit sources to fulfill our obligations. If we cannot remedy a capital deficiency, we will file appropriate notices with our regulators and immediately take appropriate steps pursuant to Securities Exchange Act Rule 15c3-1.

10.2 PROCEDURES
These procedures are reasonably designed to address operational and other risks related to a significant business disruption caused by a natural disaster, an act of terrorism, a cyber-attack or another catastrophic event.

10.2.1 BUSINESS CONTINUITY PLAN AND FIRM DOCUMENTS
Our business continuity plan addresses all essential business systems; financial and operational assessments; data backup and recovery; alternative communications with clients, employees, and regulators; alternate physical location of employees; major supplier, contractor, banking and third-party impacts; regulatory reporting; and assuring our clients prompt access to their accounts if we are unable to continue our business.

The Chief Compliance Officer maintains the Firm's primary and essential business documents, including bank accounts, financial statements, licenses, registrations and other corporate documentation. Certain backup copies of these documents are maintained by the Chief Compliance Officer, or their designee, on cloud-based data storage or offsite.

10.2.2 COMMUNICATIONS

10.2.2.1 GENERALLY

In the event of a significant business disruption, we will promptly identify what methods will permit us to communicate with our customers, employees, critical business constituents, critical banks, critical counter-parties and regulators. Although the nature of the event will determine the methods of alternative communication options we employ, they will include our website, telephone voice mail, email, etc. We will provide timely communications that report progress, recovery efforts, resumption of business activities, during and after an event, which may include posting updates to websites or portals to facilitate accessibility and broad dissemination of information.

Our website: *www.adasina.com*
Telephone voice mail (answering service): 415- 986-5500
Fax: 415- 986-5502
mail: info@adasina.com

10.2.2.2 COMMUNICATION WITH EMPLOYEES

In the event of a disaster, all employees are required to call or text the Chief Compliance Officer, or their designee, within one day of a disaster. In the event a staff member does not text or call within one day of a disaster, the Chief Compliance Officer, or their designee, will use the Staff Emergency Contact Form to contact the employee and/or the employee's designated emergency contact. The Emergency Contact Form includes all staff home and cell numbers, email and physical addresses. We will assess which means of communication are still available to us.

The Chief Compliance Officer will coordinate communications with staff regarding the condition of the offices, safety needs of employees, commencement of operations at designated alternate locations and staff assignments.

10.2.2.3 COMMUNICATION WITH EMERGENCY RESPONSE VENDORS

The Chief Compliance Officer or their designees will contact all necessary emergency response teams, which may include emergency medical, police, fire, PG&E, Water Department, telephone service provider, insurance provider(s) and the like.

10.2.2.4 COMMUNICATION WITH VENDORS

The Chief Compliance Officer or their designees maintains a list of contact information for all major businesses with which we have an ongoing commercial relationship in support of our operating activities, such as vendors providing us critical services, and determine the extent to which we can continue our business relationship with them in light of the internal or external significant business disruption. We will quickly establish alternative arrangements if a business constituent can no longer provide the needed goods or services when we need them because of disruption to them or the Firm. The Chief Compliance Officer will contact vendors as required.

10.2.2.5 COMMUNICATION WITH CUSTODIANS

The Chief Compliance Officer or their designees maintain a list of contact information for all client custodians. As soon as staff safety is secured and the office premises have been stabilized, or alternate locations are established, the Chief Compliance Officer or their designees, will contact each custodian and apprise it of the Firm's emergency contact information.

10.2.2.6 COMMUNICATION WITH CLIENTS

Prompt client communications are vital to reassuring clients of the safety of their assets and of the ongoing viability of the firm. Once safety issues are stabilized and the office premises are secured or disaster recovery sites are established, the Principals and all other staff will contact clients, apprise them of

the disaster recovery effort and provide them with alternate contact information. Client contact will be via telephone, email, fax or mail as required by the circumstances.

10.2.2.7 COMMUNICATION WITH REGULATORS

The Chief Compliance Officer is responsible for all communications with regulatory authorities, including announcements and filing of reports. The Firm is subject to regulation by the U.S. Securities & Exchange Commission. We will communicate with them and other state and local regulatory agencies to file required reports using telephone, email, fax, U.S. mail, and online websites, or by whichever means of communication are still available to us.

10.3 RELOCATION OF OPERATIONS

10.3.1 DISASTER RECOVERY SITES

In the event of a significant business disruption, we may move our staff from the affected office to the disaster recovery site(s) listed below as appropriate:

- Philipson/Robasciotti Residence
- Former Chief Compliance Officers Residence
- Liljestrand Residence

10.3.2 TEMPORARY OFFICE

To the extent possible, all Firm operations may be relocated to the disaster recovery site(s) until temporary operations are established, if necessary. To the extent possible, the answering message or service on the office number will be revised as necessary to handle incoming calls once temporary operations have been established, the Chief Compliance Officer or their designees will be responsible for the following:

- Contact custodians for access to client account records
- Notify all clients and custodians of contact information and timeline to recovery
- New telephone service and internet access (if necessary)
- New computer system and installation (if necessary)
- Updated voicemail message
- Notifying all vendors of contact information and timeline to recovery
- Notifying attorney, accountant and compliance consultant
- Resuming daily operational functions (bookkeeping, invoicing, bank account reviews, accounts payable, payroll, compliance reporting, tax and regulatory reporting)
- Notifying all essential third-party service providers of contact information and timeline to recovery

10.4 PANDEMICS

10.4.1 OFFICE INFECTION CONTROL PRACTICES

The Firm's office infection control practices will include:

- Adoption of flexible worksites (e.g., telecommuting) and flexible work hours (e.g., staggered shifts), to increase the physical distance among employees and between employees and others.

10.4.2 STAFF OBLIGATIONS
During a pandemic or severe infectious disease outbreak, staff are:

- Encouraged to self-monitor for signs and symptoms of infectious disease if they suspect possible exposure.
- Directed to work from home or take sick days if there is any risk of their being sick.

10.5 ACCESS TO FUNDS AND SECURITIES OVER CUSTODIAN PLATFORMS
The Firm does not maintain custody of its clients' funds or securities, which are maintained at our custodial firms, such as Schwab. In the event of an internal or external significant business disruption, the Firm will post on our website or via email the manner in which Clients may access their funds and securities.

Charles Schwab:
Website: www.schwabinstitutional.com
and https://client.schwab.com/Login/SignOn/CustomerCenterLogin.aspx?sim=y
Telephone: 877-702-4466 or 1-800-515-2157
Fax: 877-283-2709
Email: service@schwab.com

We have primary responsibility for establishing and maintaining our business relationships with our Clients. Our custodial firm(s) provides, through contract, the execution, comparison, allocation, clearance and settlement of securities transactions, maintenance of client accounts, access to client accounts and the delivery of funds and securities.

All custodians are required to maintain business continuity plans and annually verify their capacity to execute those plans. Each custodian is obligated to notify the Firm of any material changes to its plan that might affect Adasina's ability to provide its services. In the event any custodian initiates its disaster recovery plan, it must notify us immediately and provide us equal access to its services as its other customers. If we reasonably determine that a custodian has not or cannot meet our needs, or is otherwise unable to provide access to services, each custodian represents that it will assist us in seeking services from an alternative source. Our Chief Compliance Officer will periodically review our custodial firm(s)'s capabilities to perform the functions it was contracted to perform for us.

10.6 TECHNOLOGY DATA BACK-UP AND DISASTER RECOVERY

10.6.1 HARD COPY AND ELECTRONIC FORMATS
The Firm maintains minimal hard copy books and records and its predominantly electronic records at: 631 O'Farrell Street, Suite 1202, San Francisco, CA 94104. Maya Philipson, Chief Compliance Officer, or their designee, is responsible for the maintenance of these books and records. The Firm maintains the following document types and forms that are not transmitted to our custodial firm(s):

- Client Files & Client Services (Agreements and Contracts)
- Firm Archives
- Human Resources (Labor Notifications, Payroll and Employee Benefits)
- Infrastructure & Strategy (Accounting, Banking, Bookkeeping, Corporate Minutes, Finance, Legal Disclosures and Licenses, Operating Business Practices, Regulatory Filings, Tax Statements and Third-Party Service Providers)
- Marketing & Communications

11.0 IRA ROLLOVER RECOMMENDATIONS AND ERISA PLANS

11.1 ROLLOVER RECOMMENDATIONS TO INDIVIDUAL RETIREMENT INVESTORS

11.1.1 DOCUMENTATION OF THE BEST INTEREST RATIONALE FOR ROLLING OVER RETIREMENT PLAN ASSETS.

If the Firm recommends that a client or potential client roll over assets from an ERISA plan to an IRA to be managed by the Firm, the SEC and the U.S. Department of Labor mandate that it document the specific reason(s) why the recommendation is in the best interests of the client.

In each instance when the Firm recommends any of the following strategies to a prospective or existing client:

- A switch from a 401k to an IRA;
- A switch from one IRA to another IRA; and/or
- A switch from a commission-based account to a level fee arrangement.

The documentation must include consideration of the following client-specific factors:

- The fees and expenses of the current plan or IRA and the proposed IRA
- Whether the employer pays some expenses
- Different levels of service and investments available under each option
- The ability to take penalty-free withdrawals
- Applicable required distribution rules
- Creditor protections not equally available for IRAs
- Specific needs of the client
- How the client prefers to invest their funds
- The client's individual risk tolerance, and
- Any other factors relevant to the client's specific situation.

A Retirement Plan Rollover or Transfer Recommendation Checklist for rollover recommendations is included in this Manual. An Annual Compliance Review of Retirement Plan Rollovers Checklist is also included in this Manual.

If the Firm's recommendation is that the client NOT roll over assets to an IRA (or to another IRA) but the client decides to go ahead with a rollover anyway, the Firm should document the recommendation, ask the client to acknowledge in writing that they have been so advised and they have decided to roll over regardless, and keep a record of the client's acknowledgment.

11.1.2 ERISA PLAN CLIENTS

Currently the Firm does not have client pension, retirement or other employee benefit plans that are governed by the Employee Retirement Income Security Act ("ERISA") nor are such client retirement plans a target client base for the Firm. At such time as ERISA-covered retirement plans become clients, if ever, the Firm will adopt required policies and procedures under applicable regulations.

12.0 Senior Citizen And Retirement Clients

Throughout this Manual, the Firm addresses its fiduciary duties and the policies and procedures it has adopted to effectively meet those duties with respect to *all* of its clients, not just senior and vulnerable clients.[4] Nevertheless, the following policies and procedures particularly should be observed with respect to senior and vulnerable clients.

12.1 BACKGROUND

Decline in financial capacity, mistakes in managing money, spendthrift consumption, excessive gift giving and susceptibility to fraud targeted at older people may be signs of cognitive decline or financial abuse and may occur long before an individual presents with clinically diagnosable dementia or disease. Further, clients suffering chronic medical conditions, psychological conditions or addictions may engage in spending behaviors that are harmful. Consequently, industry practices regarding senior and vulnerable clients generally are of increasing interest to the Firm's regulators, particularly as related to the following two categories:

- The prevention of fraud against seniors and retirement investors by financial industry representatives; and
- The financial professional's procedural responses to the cognitive decline of, the undue influence upon or the financial abuse of senior and vulnerable clients.

With respect to the first concern, the Firm is well-equipped to avoid fraudulent and misleading behavior. The Firm's status as a fiduciary to all of its clients and the totality of its compliance program dictate that all personnel avoid fraud, misleading marketing activities, conflicts of interest and the like. Moreover, as professionals, each investment decision must be made on the basis of the Firm's detailed understanding of the investment product and its suitability for each client. In the event of an SEC examination, staff should expect scrutiny in the following areas:

- Misrepresentations in advertising or in promoting the Firm's investment strategy;
- Disclosures to clients of the true costs of investing in any given investment product - the fees that a client pays and the compensation that each participating issuer and financial adviser receives, and how such costs are calculated;
- Mutual fund share classes—including adviser incentives, if any, to recommend a particular share class and whether that conflict was disclosed to investors.
- Wrap fee programs—specifically the best execution for clients and whether any trade-away costs are properly disclosed.
- Retirement products—the appropriateness of variable insurance products, target date funds, and retirement vehicles that serve employees of state and local governments and nonprofits.

With respect to the second concern, Firm personnel are not expertly trained in the medical, mental health, family counseling, criminal or legal fields and consequently, must closely balance a number of legal, fiduciary, client trust, client privacy and familial issues that have the potential to raise conflicts of interest between the various participants. Equally important, Firm personnel need to avoid encroaching into professional counseling in areas which it is neither competent to nor licensed to render services. Without expertise in identifying cognitive decline, mental health issues, physical health issues and elder abuse, the Firm is in a difficult position in dealing with suspected decline or abuse and making an incorrect assumption about a client's underlying circumstances can have serious implications in the following areas:

- The client's right to self-determination;
- The client's right to privacy;

[4] See forgoing policies and procedures related to marketing and advertising, conflicts of interest, suitability, investment due diligence, safeguarding client data, identity theft prevention and cyber security, amongst others.

- The Firm's fiduciary obligations to act in the best interests of the client;
- The Firm's legal liability for taking action without the clear legal authority to do so.
- Facilitating harm to the client by incorrectly assessing a possible problem.

For these reasons, in any case of suspected cognitive decline or undue influence/elder abuse, senior management and the Chief Compliance Officer will confer, review the circumstances of the situation and make all decisions regarding the Firm's course of action.

12.2 FRAUD PREVENTION
Adasina does not and will not engage in fraudulent or misleading behavior with respect to the marketing of its services, its investment strategy, individual securities to its senior and vulnerable clients.

The Firm discloses all conflicts of interest in its Form ADV Part 2A and makes certain that all new and existing clients are provided a copy of the Form ADV Part 2A or a Statement of Material Changes to the Part 2A with an offer to provide a full copy at least annually.

Adasina conducts appropriate due diligence on each client investment and makes a determination that in each case, an investment is suitable for each participating client's financial condition, risk profile and investment goals.

The Firm ensures that with respect to all client securities investments, all fees and costs are fully disclosed to the client.

12.3 CLIENT COGNITIVE DECLINE OR POTENTIAL ABUSE BY THIRD PARTIES
It is Firm policy for each of its advisors to encourage each client, regardless of age, to work with legal counsel to prepare, and regularly review and update, a comprehensive estate plan that includes some or all of the following:

- A revocable trust;
- A will;
- A power of attorney for health care;
- A springing/conditional[5] durable power of attorney.

12.3.1 RECOGNITION OF COGNITIVE DECLINE
Decreases in cognition are associated with decreases in financial literacy and yet an individual's confidence in his or her ability to manage finances and financial knowledge may not correspond to drops in cognition. A gap between a client's confidence in his or her ability to manage finances and the assessment of Firm personnel can be an early sign of cognitive decline.

Early stages of dementia include cognitive problems with:

- Basic orientation (such as not knowing the date)
- Judging distances

[5] A *general durable power of attorney* gives another person ("agent") broad powers over a client's financial (and possibly health care) decisions. A durable power of attorney can be in effect when the client has full cognitive and physical abilities and continue during a period when the client becomes physically or mentally incapacitated. For example, a client might give a child power over their finances or certain assets because they deem the child to be more experienced or "better" with financial matters. A *"conditional" or "springing" durable power of attorney* only comes into effect after certain conditions are met, typically when the client becomes severely physically disabled or mentally incompetent. (A springing power might equally be appropriate for someone in the military who is subject to sudden and immediate deployment overseas, which would give an agent powers in that specific situation only.) A *healthcare power of attorney* only grants the agent the ability to make choices about a client's medical treatment.

- Following a conversation
- Making decisions
- Performing the routine tasks of living
- Paying bills
- Recalling events
- Mood changes
- Suspiciousness
- Denial
- Poor judgment, and
- Loss of initiative

Mid-stage dementia symptoms include:

- Disorientation
- Restlessness and wandering
- More profound memory loss
- Hallucinations, and
- Language difficulty

Late stage dementia is recognized by:

- Inability to speak
- Inability to recognize family members
- Inability to engage, and
- Inability to eat, bathe, control bodily functions

12.3.2 RECOGNITION OF UNDUE INFLUENCE AND ELDER FINANCIAL ABUSE

Financial exploitation includes embezzlement, fraud, taking money under false pretenses, forgery, forced property transfers, purchasing expensive items with the client's money without the client's knowledge or permission or denying a client access to their own funds or home. It includes the improper use of legal guardianship arrangements, powers of attorney or conservatorships. It also includes a variety of internet, telephone and face-to-face scams perpetrated by salespeople (short-term lenders, mortgage lenders, home repair services etc.) or even by family members, friends or hired caregivers. Signs of potential elder abuse may include:

- Physical or emotional abuse (signs of fearfulness, uncharacteristic sadness, bruising, weight loss, injury)
- Neglect (hygiene, departure from usual standards of dress)

- Blocked access to belongings or assets (misappropriation or improper use of power of attorney)
- The client changes his or her regular spending habits.
- A previously uninvolved relative, caregiver, or friend speaks for or makes decisions on the client's behalf.
- A "new friend" appears that is quickly embedded in the client's personal life;
- The client becomes isolated from family and professional advisors.
- The client exhibits erratic behaviors, such as unpaid bills and changes in spending habits, unexplained asset transfers and/or atypical cash withdrawals/wire transfers, or
- There are unexplained changes in the client's professional advisors such as an accountant, doctor, attorney or other financial advisor.

12.3.3 FIRM RESPONSE TO SUSPECTED COGNITIVE DECLINE OR ABUSE

If senior management and the Chief Compliance Officer develop a reasonable belief that a client is, is about to or has suffered financial abuse or is exhibiting signs of undue influence in their financial decisions, the Firm will alert:

- The custodian(s) of the client's account(s);
- Any legal representative (trustee, power of attorney) established by the client's estate planning documents;
- Any Trusted Contact designated by the client (unless the contact themself is implicated); and as necessary
- Law enforcement.

If senior management and the Chief Compliance Officer develop a reasonable belief that a client is suffering physical or emotional abuse or neglect at the hands of a family member, caregiver or family friend or acquaintance, the Firm may contact all relevant social services and law enforcement agencies to look into the matter.

12.3.4 INFORM THE CHIEF COMPLIANCE OFFICER AND SENIOR MANAGEMENT
Senior management and the Chief Compliance Officer will meet with all staff members with knowledge of the facts regarding the client and the possibility that cognitive impairment and/or undue influence/abuse Is occurring and determine whether and what action is warranted. Documentation of the meeting will be maintained by the Chief Compliance Officer or their designee.

If Firm senior management and the Chief Compliance Officer determine that there is a reasonable basis for a determination that abuse of some kind is occurring or may occur and that escalation is warranted:

- The client's advisor may contact the client's Trusted Contact to gain any additional insight as to the physical/mental status of the client, and the possibility of abuse;
- Based upon that contact, the advisor may contact the custodian of the account(s) to notify it of the possible need for a freeze on assets;
- Based upon the circumstances, the advisor may contact the client and inform them of the possible freeze on the account by the custodian;

- Based upon the circumstances, the advisor may notify social services or law enforcement of possible abuse.

12.4 PREVENTION OF FRAUD WITH RESPECT TO SENIOR AND VULNERABLE CLIENTS
All Firm personnel are required at all times and with respect to each of the Firm clients (senior or otherwise) to follow the policies and procedures established by this Manual related to the Firm's fiduciary obligations, and to investment due diligence, investment standards (with particular emphasis on the full layers of cost of any particular investment or sub-advisory relationship), marketing and advertising restrictions, employee personal trading, conflicts of interest, Form ADV disclosures, identity theft prevention and cyber security planning and procedures, amongst others.

Fraudulent Investment Schemes, Telemarketing Scams, Internet Scams. Under the Senior Safe Act of 2017 (Public Law No. 115-174), "covered financial institutions" (and individuals working for and trained by them) are encouraged (but not mandated) to report suspected third-party fraud and the financial exploitation of seniors to one or more enumerated "covered agencies". The covered financial institution/individual making the report is granted immunity from civil liability and administrative proceedings as long as the covered financial institution has provided requisite staff training and the report is made by the reporting institution/individual in good faith and with reasonable care. Registered investment advisers and broker-dealers are "covered financial institutions" and the SEC and state securities authorities (along with law enforcement and adult protective services agencies) are "covered agencies".

The Senior Safe Act provides that the content of the training – used by either the financial institution or provided by a third-party training company must:

- Be maintained by the financial institution and made available to the covered agency with examination authority over the financial institution;
- Instruct those individuals subject to the program on how to identify and report the suspected financial exploitation of a senior citizen internally and to government officials or law enforcement authorities;
- Discuss the need to protect the privacy and integrity of each individual customer of the financial institution; and
- Be appropriate to the job responsibilities of the individual attending the training session.

Additionally, the training must be provided by the financial institution as soon as reasonably practical for current employees and individuals and must be provided for new employees within one year after the date the individual became employed. Finally, the financial institution must maintain certain records, including a record of each individual who has completed the training, whether employed or affiliated with the financial institution.

12.5 INVESTMENT STANDARDS FOR SENIOR AND VULNERABLE CLIENTS
The Firm meets its fiduciary duty to act in the best interests of each of its clients with respect to investment decisions by making certain that all decisions regarding investment strategy and securities transactions are in the best interests of the client. With respect to senior and vulnerable clients, client investment standards should be foremost in any investment due diligence and securities decisions.

12.6 UPDATE OF SENIOR AND VULNERABLE CLIENT FINANCIAL PROFILE
The responsible portfolio manager annually reviews the client profile of each senior and vulnerable client and update the following as required:

- Age
- Employment status
- Sources of income
- Liquid net worth

- Tax status, such as marginal tax rate;
- Investment objectives
- Risk tolerance
- Liquidity needs
- Investment time horizons
- Investment experience
- Other investments

The asset allocation and securities holdings of each senior and vulnerable client investment account should be reviewed and adjusted in light of any significant changes to the client's financial and risk profile.

The portfolio manager should inquire if the client's estate plan documents have changed in any way and if so, should obtain updated copies of the plan documents for the Firm's files.

12.7 CLIENT DESIGNATION OF TRUSTED CONTACT
It is Firm policy to discuss with each client about the issue of cognitive decline and financial abuse and endeavor to obtain from each client a designation of a trusted contact ("Trusted Contact") consistent with the client's estate plan designations for the Firm to contact should cognitive decline and/or suspected abuse become an issue for the client.

At the beginning of each new client relationship, regardless of the age of the client, and in connection with each existing Firm client, regardless of the age of the client, the responsible advisor will request and thereafter as necessary, update an "Add a Trusted Contact Person" form. The form allows the client to designate one or more persons authorized by the client to be contacted in order to:

- Address possible financial exploitation;
- Confirm client contact information;
- Confirm client health status;
- Confirm the identity of any legal guardian, executor, trustee, or holder of a power of attorney; or
- As otherwise permitted by applicable rules.

12.7.1 LIMITATION ON SHARING INFORMATION WITH TRUSTED CONTACTS
By its terms, the Schwab "Add a Trusted Contact Person" form agreement does not authorize designated Trusted Contact to view a client's account information, execute transactions, or inquire about any activity in the client's account. Simultaneously however, the agreement authorizes both Schwab and Firm to disclose private client information to the Trusted Contact, including financial account information and balances, recommendations for securities transactions, personally identifiable information such as social security numbers, dates of birth, account numbers and other highly sensitive client information.

Because the Firm is not a signatory or party to the "Add a Trusted Contact Person" agreement, in the event contact with a client-designated Trusted Contact is required, the Adasina advisor and staff should NOT share any of the client's personal financial condition, account holdings or other private data with the Trusted Contact and must NOT accept or act upon any requests or directions for financial transactions or investment recommendations with respect to the client's assets without specific Chief Compliance Officer approval.

In such cases, the Firm may contact the Trusted Contact *ONLY* to verify client status, health condition, mental condition, current whereabouts and/or to identify possible agents of financial abuse.

12.7.2 ADDITIONAL RECOMMENDATIONS TO CLIENT REPRESENTATIVE OR TRUSTED CONTACT

As appropriate under the circumstances and assuming the designated legal representative or Trusted Contact is not implicated in any abuse, the advisor may encourage a client's legal representative or Trusted Contact to consider one or more of the following actions, as warranted:

- Arrange a competency evaluation: Conducted by a healthcare professional, an evaluation relies upon interviews with the client and others to determine whether a client is impaired and in need of additional clinical evaluation and medical attention.

- Engage an attorney: An attorney can assist with ensuring that an individual's advance care directive reflects care choices and preferences, particularly if that person is unable to make decisions due to cognitive disorders.

- Engage a care management team**:** A care management team can be engaged to coordinate the many facets of medical, residential and other care required to assist a patient's quality of life in their day-to-day living.

- Identify an assisted living facility**:** Based upon the individual's unique needs and budgetary constraints, assisted living offers a safe, comfortable housing alternative with care from specially trained staff.

12.9 FIRM RESPONSE TO CLIENT CHANGES TO REPRESENTATIVES AND BENEFICIARIES
Clients often designate one or more representatives and/or beneficiaries in their custodial account agreements. Account representatives could include persons designated as trustee or co-trustee of a client trust account, a person designated with a durable power of attorney or, upon the death of a client, the executor of a client's estate. Designated representatives may have the authority to obtain or direct payment of client account assets. Designated beneficiaries stand to inherit the assets of an account upon the death of the client.

Because senior and vulnerable clients are particularly subject to the undue influence of persons seeking to take advantage of their vulnerabilities, all client requests to change account representatives and beneficiaries must be evaluated by the Firm for evidence of possible abuse and undue influence.

The following policies apply when any team member receives a request from a senior or vulnerable client to make changes to their representatives or beneficiaries:

- Client services staff/advisor receiving the client's request or notification from the client's custodian of changes in representative/beneficiary designations must notify the Chief Compliance Officer.

- The Chief Compliance Officer will consider the request with the advisor and senior management and evaluate the presence of undue influence/abuse in light of the factors discussed in Section 5, below.

    - If undue influence or abuse is suspected, the advisor should request an in-person meeting with the client to discuss the requested changes;

    - If not implicated in the undue influence/abuse, the advisor may contact the client's designated Trusted Contact to discuss the client's status; and/or

- The Chief Compliance Officer and senior management may authorize the Firm to notify the client's custodian of the suspected abuse in order that the custodian may consider placing a freeze on the account.

12.10 DEATH OR INCAPACITY OF A CLIENT
Upon notification of the death of a client, staff immediately must inform the responsible portfolio manager and the Chief Compliance Officer and the following restrictions must be observed:

- The Chief Compliance Officer will consider the request with the advisor and senior management and evaluate the presence of undue influence/abuse in light of the factors discussed in Section 5, below.
    - Current designated co-trustees of a client trust account may continue to authorize transactions, but estate representatives should be identified;
    - If the Firm does not have current estate planning documents identifying the authorized successor trustee and/or executor, such documents should be obtained and verified with the client's legal counsel prior to further account activity.
- The Chief Compliance Officer will consider the request with the advisor and senior management and evaluate the presence of undue influence/abuse in light of the factors discussed in Section 5, below.
    - Upon notification, the custodian may impose a freeze on the account until it receives formal notification from the estate representative and documentation of the representative's authority under the estate plan.

12.11 STAFF TRAINING
For all new Access Personnel and as otherwise required, the Chief Compliance Officer will arrange for staff to be trained regarding the recognition of signs of cognitive decline, undue influence, financial and other abuse, and the Firm's policies and procedures related to protecting its senior and vulnerable clients. This training is included in the Annual Firm-Wide Compliance Training session.

12.12 REGULATORY EXAMINATIONS OF THE FIRM'S POLICIES REGARDING SENIOR AND VULNERABLE CLIENTS
Regulator exams will focus on the following:

- Firm procedures addressing issues related to diminished capacity and elder abuse or financial exploitation);
- Training of investment adviser representatives with regard to senior-specific issues;
- Types of client account information required to open accounts for senior investors;
- Types of securities and suitability of securities sold to senior investors;
- Supervision of investment adviser representatives as they interact with senior investors
- Use of professional "senior" specialist designations;
- Marketing and communications to senior investors;
- Disclosures provided to senior investors; and
- Complaints filed by senior investors and the Firm's response to those complaints.

13.0 Investment Strategy, Investment Research & Investment Due Diligence

13.1 INDIVIDUALLY MANAGED ACCOUNTS
The Firm's investment advisors work with each client to determine the client's specific investment objectives to develop an investment policy statement that outlines the basic asset allocation for the client based upon the client's risk tolerance and investment goals. Investment and portfolio allocation software may be used to assist in the evaluation of the client's portfolio. The portfolio manager evaluates the client's existing investments and works with the client to develop a plan to transition existing holdings into a portfolio that is consistent with the Firm's investment strategy for the client's portfolio. The client's portfolio and asset allocation is routinely monitored.

13.2 TYPES OF SECURITIES
The security classes listed below are currently utilized by the portfolio manager in the management of client accounts although other security classes are permitted:

- Equity Securities
- Exchange Traded Funds
- Certificates of Deposit
- Municipal Securities
- Mutual Fund shares
- United States government securities
- Fixed income securities

13.3 SOCIAL JUSTICE INVESTING
The Firm works with socially responsible investors. In addition to financial analysis performed on portfolios, socially responsible investments ("SRI") also use a social screen, a collection of non-financial criteria that a SRI manager uses to include or exclude companies for investment (this often includes environmental impact, social impact, and corporate governance). The Adasina Investment Criteria is a responsive set of criteria that adjusts as needed and allows us to dynamically align with social justice movements.

13.4 INVESTMENT DECISIONS
The Firm's Public Equities Portfolio Management Team is led by Rachel Robasciotti, and is responsible for:

- Reviewing existing securities positions held in client accounts;
- Determining new securities for purchase for client accounts;
- Determining securities to sell from client accounts;
- Reviewing general market conditions and industry sectors;
- Conducting the Firm's annual best execution review; and
- Conducting the Firm's annual soft dollar review.

13.4.1 CLIENT INVESTMENTS MUST BE IN BEST INTEREST OF THE CLIENT
The investment decisions made by the Firm's portfolio managers or Public Equities Portfolio Management Team must be based upon a reasonable belief that each security transaction is in the best interests of the client, based upon the client's particular financial circumstances.

13.5 INVESTMENT DUE DILIGENCE
Prior to making an investment on behalf of any client or recommending a specific investment to a client, Firm portfolio managers or the Public Equities Portfolio Management Team must conduct sufficient due diligence as is appropriate to:

- Ensure that the nature of the security is fully understood, to assess the risk and operational characteristics of the security;
- Ensure that the security meets the firm's investment criteria; and
- Ensure that the security investment that is contemplated would be reasonable and consistent with the client's best interest given the client's financial condition and investment strategy.

13.5.1 INITIAL INVESTMENT DUE DILIGENCE
Prior to recommending any specific investment to a client, the portfolio manager or the Public Equities Portfolio Management Team conducts the due diligence necessary to assess the risk and operational characteristics of the security and ensure that the security meets the Firm's investment criteria. The Firm's due diligence consists of some or all of the following as is appropriate:

- Review of in-house or third-party research;
- Review of applicable financial statements and annual reports;
- Review of mutual fund prospectuses, current holdings, and relevant analytics;
- Review of bond indenture, credit rating, notice(s) of material events since issuance, and bond analytics;
- Review of private placement memoranda, offering memoranda, subscription agreements, partnership agreements, other agreements;
- Review of issuer/principals' backgrounds and experience;
- Review of disclosure brochures and statements;
- Review of ratings;
- Review of the past performance of the investment.

13.5.2 ON-GOING INVESTMENT DUE DILIGENCE
The responsible portfolio manager or the Public Equities Portfolio Management Team is responsible for supervising and conducting on-going due diligence on the securities the Firm recommends, by reviewing, as appropriate:

- Updated prospectuses;
- Changes to fund investment strategy;
- Rating changes;
- Changes resulting from the occurrence of material events.

Portfolio managers or the Public Equities Portfolio Management Team is responsible for conducting on-going due diligence of securities the Firm purchases for or recommends to clients, including reviewing and documenting updated versions of all due diligence materials listed above as is appropriate to the complexity, risk profile and/or liquidity of the investment.

13.6 MUTUAL FUND SHARE CLASSES
The Firm does not receive 12b-1 fees, or other compensation that would give the Firm incentive to choose one mutual fund share class over another. We make the determination of which share class of a mutual fund to

purchase solely on the best interests of our clients, based upon the circumstances of each individual client. The factors used to make the determination include:

- Mutual fund expense ratio
- Transaction fees
- Holding period
- Size of order
- Anticipated future liquidity needs of client
- Overall strategy for the client portfolio

Due to these varying factors, the Firm may purchase different share classes for different clients and the share class purchased may not always be the one with the lowest expense ratio for which the client qualifies.

The Firm recognizes that not holding the optimal share class of a mutual fund may lead to higher expenses for the client and so has adopted a policy to review share classes of mutual funds as part of the annual review of client account models. Each portfolio manager is responsible for reviewing the funds held in accounts that they review and will perform an inter-class exchange of share classes when deemed appropriate.

13.7 LENDING OF CLIENT SECURITIES
Adasina does not lend client securities.

13.8 WRAP FEE PROGRAM INVESTMENTS
It is not a part of the Firm's investment strategy to place client assets into wrap fee programs. The Firm does not sponsor or act as the investment manager for any wrap fee programs.

13.9 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer is responsible for maintenance of the Firm's investment strategy related records. Records may be kept electronically in a non-rewritable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- Documentation, if any, of the basis for individual investment management decisions.
- Documentation, if any, of the basis for any material deviations from the Firm's investment strategy or client investment guidelines.

14.0 Trade Execution And Settlement

It is the policy of the Firm to supervise all trade related activities and to prohibit personnel from executing trades on behalf of client accounts without the approval of a portfolio manager. Furthermore, the Firm has established the following execution guidelines.

14.1 TRADE EXECUTION
For Discretionary Accounts: The portfolio manager(s) are authorized to execute client trades that are consistent with the Firm's investment strategy, any client investment guidelines and restrictions and subject to the Firm's best execution policies.

For Non-Discretionary Accounts: The Firm's policy is not to accept these accounts.

For Clients Directing Use of Specific Executing Broker: Adasina generally does not accept clients that custody their assets or direct brokerage executions to a broker-dealer other than Schwab. If the Firm accepts direction

from a client to direct brokerage executions, the portfolio manager(s) are authorized to execute client trades consistent with the Firm's investment strategy, any client investment guidelines and restrictions and subject to the Firm's best execution policies and subject to the commission arrangement negotiated between the client and the broker.

Client Trading Instructions: Because the Firm cannot guarantee that a portfolio manager or other trade staff will be available to timely receive any email, voicemail, text or other message, clients should be informed that the Firm does not accept trade instructions from clients via any messaging system. All client-originated trade instructions should be made directly via direct phone contact or in person.

14.2 SELECTION OF EXECUTING BROKER
In most instances, client trade executions are directed to the custodian of the client's account to avoid the imposition of "trade away" fees. In cases where a desired security is not available through the custodial broker, or when lower pricing or execution parameters warrant, the portfolio manager(s) are authorized to execute client transactions with an approved broker-dealer other than the client's custodian subject to the alternative executing broker meeting the best execution guidelines established by the Firm.

14.3 PRINCIPAL AND AGENCY CROSS TRANSACTIONS PROHIBITED
It is the policy of the Firm to prohibit principal transactions between a Firm account (or an Access Person account) and a client account and to prohibit agency cross transactions between the accounts of two or more clients.

14.4 PROHIBITED TRADE ACTIVITIES
The Firm and its employees are prohibited from the following:

- Placing a securities order for fraudulent purposes
- Placing a securities order for an unsuitable transaction for a client
- Engaging in a manipulative transaction
- Engaging in inter-positioning
- Engaging in front-running (the practice of dealing on advance information provided by others, before their clients have been given the information)
- Engaging in scalping (a trading practice in equities/options/futures/foreign exchange markets whereby a trader holds a position for a very short period of time in an attempt to profit from the bid-ask spread)
- Allocating trades to favor one client over the interests of another client; or
- Allocating trades to compensate a client for services, gifts, or other benefits given to the Firm or any staff member or to induce such future services, gifts or benefits from the client.

14.5 EXECUTED TRADES REVIEW
On a monthly basis the portfolio manager(s) review the executed transactions executed the prior month as noted on the trade blotter.

The portfolio manager(s) or other trade staff download executed trade reports and review any exceptions or trade discrepancies as provided by the executing broker or a similar report as generated by a broker-dealer platform. If a discrepancy noted is clerical in nature, the portfolio managers or trade staff makes corrections as needed. The portfolio manager(s) or trade staff report discrepancy corrections to the broker either electronically or by telephone. If the discrepancy is non-clerical, the Chief Compliance Officer is alerted and follows the Firm's Trade Error procedures as required.

14.6 SETTLEMENT DATE
The custodian is responsible for settling all trades on behalf of the client accounts. If the custodian reports trade settlement problems, the portfolio managers are required to assist in the resolution of the problem.

14.7 TRADE AND PORTFOLIO ACCOUNTING SYSTEMS UTILIZED

- Schwab online trading platform
- Orion Portfolio Management software

15.0 Trade Aggregation And Allocation

The SEC has stated that when a transaction is suitable for more than one client, an advisor may aggregate trade orders and allocate purchase and sale opportunities on a fair and consistent basis.
The portfolio managers may aggregate orders of more than one client if it is determined that aggregation is in the best interests of the clients participating. In these cases, the Firm's aggregation and allocation policies are as follows.

15.1 AGGREGATION
Adasina has adopted the following trade aggregation policies:

- The Firm may aggregate multiple client trades into a single transaction when it is determined that aggregation is consistent with the Firm's duty to seek best execution, consistent with the investment objectives for the client accounts participating in the trade and that aggregation would be in the best interests of the participating clients.
- Client transactions may be aggregated according to custodial relationship in consideration of execution charges that may be imposed if trades are directed to a non-custodial broker-dealer for execution.
- In aggregated client transactions, clients may be aggregated according to Firm model portfolio categories or other groupings that treat all similarly situated clients equally
- Prices for securities purchased or sold in aggregated trades are averaged across the client accounts participating in the trade. Aggregated trades placed with different executing brokers may be priced differently; the trade sheet or trade blotter should indicate that the price was averaged.
- Transaction costs are allocated to each client account as determined by the client's custodian based upon the custodial agreement.

15.2 ALLOCATION
Adasina has adopted the following allocation policies:

- Trade allocation decisions are made by the portfolio manager.
- Trades may not be allocated in any manner that consistently favors one group of similarly-situated clients over another.
- If an aggregated order is not completely filled, a portfolio manager must allocate the partially filled order on a fair and consistent basis. The Firm's trade records must indicate that a transaction was aggregated and the method used to determine pricing and allocation.
- In allocating partial fills after execution, the security should be allocated *pro rata* to all client accounts eligible to participate in the order, with the following exceptions:

- If one or more accounts would be unable to meet an investment objective (which may include sector diversification, client guidelines, etc.), the portfolio manager may deviate from the *pro rata* formula;
- If a *pro rata* allocation results in a *de minimis* allocation to certain accounts, the portfolio manager may deviate from the *pro rata* formula; and/or
- If pro *rata* allocation results in a cash position that is different from the desired cash level, the portfolio manager may deviate from the pro rata formula.

- The Firm may continue to hold a security in one client account while selling it for another client account. This occurs when client guidelines or risk tolerances mandate a sale for a particular client. In some cases, consistent with client objectives and risk, the Firm may purchase a security for one client while selling it for another.
- Client trades may be executed at different times and at different prices consistent with specific client objectives and risk tolerance.

15.3 ALLOCATION OF EQUITY TRADES
The Firm uses the portfolio evaluation factors listed above in allocating partial fills of equity transactions.

15.4 ALLOCATION OF FIXED INCOME TRADES
The Firm may aggregate fixed income transactions. Partial fills of aggregated fixed income trades are allocated in accordance with the portfolio evaluation factors stated above.

15.5 TIMING OF TRADE ALLOCATION DECISIONS
The portfolio manager should allocate each transaction in writing prior to or at the time an order is transmitted to a broker for execution. If the portfolio manager is unable to allocate in writing before or at the time of transmission, the written allocation should be done as soon as practicable thereafter, but in no event later than the end of the business day. The written allocation records shall be maintained with the trading records.

15.6 EXCEPTIONS FROM ALLOCATION POLICY
The portfolio manager documents all exceptions from the stated allocation policies.

The method of allocation and determining price and participation for each aggregated/allocated trade must be noted on the trade blotter or trade allocation memorandum for each such trade. A form Aggregated Trade Order and Allocation Memorandum follows these procedures.

16.0 Trade Errors

16.1 POLICIES
It is the policy of Adasina that its personnel carefully implement investment management decisions. Nevertheless, if a trade error occurs, it is Firm policy that the error be corrected as soon as possible and in a manner that the client is not disadvantaged and bears no loss. The following specific policies are followed by the Firm:

- All trade errors are resolved such that no loss is assigned to the affected client account(s) as a result of the error.
- No client account may be used to correct a trade error made in another client's account;
- Clients need not be notified of a trade error if the affected account(s) suffer no loss or significant taxable gain;

- Clients are notified (via telephone, email or mail) of trade errors affecting their accounts if and when the account is reimbursed for a loss or is notified of a substantive taxable gain; and
- Firm personnel are prohibited from requesting a broker-dealer to accept financial responsibility for a trade error caused by the Firm in exchange for the promise of future compensation through commissions; however, client custodians/executing brokers may have internal policies related to absorbing trade losses due to errors for trade errors with minimal losses.

Implementation of these policies requires that:

- A trade error, once identified be immediately reported to the Chief Compliance Officer;
- The Chief Compliance Officer formulate and supervise the trade error correction process;
- The Chief Compliance Officer investigate the source of the error and institute preventive enhancements to operational procedures, if necessary; and
- A written record of all trade errors is maintained.

These policies and procedures apply only to trade errors made by Adasina and its employees. If an error is determined *not* to be the fault of Firm personnel, the Chief Compliance Officer resolves the error with the responsible party.

16.2 TYPES OF TRADE ERRORS
The following are some of the most common trade errors:

- Buying or selling a type of security that is not authorized for the client account;
- Buying or selling a security that results in the client account being managed outside of its investment guidelines or contrary to client instructions (for example, buying a stock that is on the client account's restricted list, or buying or selling a security that causes the client account to be improperly concentrated in a particular industry or asset class);
- Entering an order as a sell rather than a buy or vice versa;
- Entering a limit order as a market order;
- Buying a security when the client account has insufficient funds;
- Buying or selling the incorrect number of shares;
- Buying or selling the wrong security;
- Buying or selling the correct security/the correct amount, but for the wrong account;
- Incorrectly noting the price executed;
- Sending the trade to the wrong broker; and
- Incorrect allocation of an aggregated trade.

16.3 IDENTIFYING TRADE ERRORS
The timely correction of trade errors is critical in order to limit the Firm's market exposure. Most trade errors are identified through the:

- Review of the daily trade blotter by the Firm's portfolio managers and trade personnel; and

- Review of the daily download from Schwab, reconciling the data with the Firm's portfolio accounting system.

16.4 RESOLVING TRADE ERRORS
Once identified, a trade error must be brought to the attention of the Chief Compliance Officer immediately.

The Chief Compliance Officer will:

- Conduct research to determine the facts surrounding the error; and
- Gather the trade blotter, tickets and any other pertinent material.

Trades are either corrected within a client account or moved into a Firm error account as the specific circumstances dictate. The Chief Compliance Officer formulates a strategy for resolving the trade error.

The Chief Compliance Officer prepares a written Trade Error Report explaining the trade error and the steps taken to resolve it. Hard copies of the trade blotter, trade report, confirmations, executing broker correspondence and staff notes, if any, and documentation of the error correction are attached to the report.

16.5 TRADE ERROR COMPENSATION TO CLIENTS
Except as noted below, the Chief Compliance Officer directs personnel to calculate the gain or loss suffered by the client due to the error and if applicable, due to the correction of the error. Adasina will compensate losses only for those trade errors made by the Firm and will not be responsible for compensating clients for losses resulting from trade errors made by the client's custodian and/or the executing broker-dealer.

If an investment gain results from the correcting trade, the gain will remain in the account unless:

- The same error involved other client account(s) that should have received the gain; or it is not permissible for the client to retain the gain, or
- The client decides to forego the gain (e.g., due to tax reasons).

Each client custodian has adopted its own policies and procedures regarding the handling of gains earned and losses suffered in connection with erroneous trades. The Chief Compliance Officer contacts the custodian of the client account involved with the trade error and determines the custodian's internal policies with respect to trade error gains and losses.

Schwab's policy for trade error gains for accounts custodied there is that any gain of $100 or over either will be left in the client's account or donated by Schwab to a charity of its choosing. If a loss occurs that is greater than $100, the Schwab or the Firm is responsible for compensating the client for the loss. Schwab will take the loss or gain (if such gain is not retained in the client's account) if it is under $100 to minimize and offset its administrative time and expense. Generally, if related trade errors result in both gains and losses in a client's account, they may be netted.

Applicable law prohibits the Firm from requesting an executing broker to accept financial responsibility for a trade error caused by the Firm in exchange for the promise of future compensation through commissions.

All documents related to the computation and payment of the loss to the client are attached to the Trade Error Report and given to the Chief Compliance Officer for approval. The Report and attachments are maintained in a trade error file.

17.0 Proxy Voting

BACKGROUND

The Firm accepts and exercises voting authority over the securities held in client accounts and in certain of the funds under its management or advisement. Firm clients designate voting authority to the Firm over: (1) proxies solicited by issuers of securities beneficially owned by the client, and (2) all shareholder voting relative to any mergers, acquisitions, tender offers, bankruptcy proceeds, re-organizations or other types of events pertaining to the client's investment assets. This practice is stated both in the Firm's investment advisory agreement and in the Firm's Form ADV Part 2. The following policies and procedures are implemented by the Firm to ensure its compliance with all regulatory requirements.

All solicitations received are reviewed and voted by the Chief Compliance Officer, under her supervision, voted in a manner that is in the best interest of its clients and that follows the Firm's Proxy Voting Guidelines.

17.1 DISCLOSURE OF PROXY VOTING POLICIES IN FORM ADV PART 2
A summary of the Firm's proxy voting practices is disclosed in the Firm's Form ADV Part 2. Material changes to the policy must be made to the Form ADV Part 2 within *30 days* of any change.

17.2 BEST INTERESTS OF THE CLIENT
It is Firm policy that all solicitations are voted in accordance with the best interests of the client. For those Firm clients electing to follow a socially responsible investing strategy, an additional SRI analysis of proxy solicitations will be performed. In order to ensure that solicitations are voted in the best interests of the client, the Chief Compliance Officer or portfolio manager will:

- Monitor corporate actions by reviewing, prior to voting, all solicitations received on behalf of clients that have delegated voting authority.
- Vote all solicitations received on behalf of clients that have delegated voting authority unless it is determined that not voting would best serve client interests.
- Determine the social, environmental, corporate governance and other public policy impacts of the proposal for those clients following an SRI strategy.
- Disclose potential conflicts of interest that exist between the Firm (or its principals or employees) and the client's best interests and either obtain client consent to vote the proxy or delegate voting authority back to the client or a qualified third-party.

17.3 DETERMINING PROXY VOTES
In the absence of a conflict of interest, and to the extent consistent with the Firm's Proxy Voting Guidelines (see, appended forms) the portfolio manager, the Chief Compliance Officer, will vote on all solicitations received on behalf of clients. Prior to voting, the portfolio manager, the Chief Compliance Officer, will evaluate the following documents and information, as available:

- Proxy statements and other solicitation materials
- Published reports of the financial condition and current market position of the issuer
- Market conditions and social issues as publicly debated and discussed by reputable sources

17.4 VOTING CRITERIA
Prior to voting the portfolio manager, the Chief Compliance Officer, will evaluate the proxy ballot on the basis of one or more of the following factors:

- The possible impact on the value of the security
- The possible impact on shareholder rights and privileges
- The reasonableness of the proposal

- The social, environmental and corporate governance implications of the proposal
- The possible impact of any proposed mergers, acquisitions and/or corporate restructuring
- The possible impact of other issues particular to the proxy statement

17.5 UNSUPERVISED CLIENT ASSETS
Unsupervised assets are defined as securities specifically under the direction of the client for which the Firm has no discretionary authority. For these clients the investment advisory contract specifies that the Firm cannot vote solicitations on their behalf.

17.6 CLIENT DO NOT VOTE LIST
As the Firm is authorized to vote on most client solicitations, the Firm only maintains a list containing the names of those clients declining to authorize proxy voting on their behalf by the Firm.

17.7 NEW CLIENT ACCOUNTS
Clients are advised of the Firm's willingness to vote proxy solicitations when a new account is opened. At this time, clients make an election and are directed to inform their custodian whether or not they authorize the Firm to receive and vote corporate solicitations sent by companies whose securities are included in their portfolios.

Where provided by the client or custodian, a copy of the client's instructions to the custodian regarding proxy voting authority should be placed in the Firm's client account file.

Clients declining to authorize the Firm to vote solicitations are directed to forward instructions to their custodian advising them to direct all solicitations directly to them. Any proxy solicitations received on the clients' behalf will be immediately forwarded to them for voting. The Client Do Not Vote List is updated to include the new client, as applicable.

17.8 RECEIPT AND VOTING OF PROXY SOLICITATIONS

17.8.1 CONFLICTS OF INTEREST
The Chief Investment Officer reviews the Firm's employee conflict of interest and outside business activities disclosures and annual certifications and the relevant proxy statement received. In the event it is determined that a possible conflict of interest exists between the best interests of the client on whose behalf a proxy will be voted and the interests of the Firm or any of its employees, the conflict-of-interest procedures described below will be followed.

17.8.2 VOTING OF PROXIES IN ACCORDANCE WITH GUIDELINES
The Chief Investment Officer reviews the proxy package and votes the solicitations in accordance with the voting guidelines established under the policy and accompanying these policies and procedures. If any documents are created that memorialize the basis for a particular vote, they are kept with a copy of the voted ballot. The Chief Investment Officer or their designee processes and sends the voted ballots. The proxy materials are maintained in a file containing a copy of the ballot and voting documentation, if any, in a proxy voting file, kept chronologically by year.

17.9 REVIEW OF POTENTIAL CONFLICTS OF INTEREST
The Firm is sensitive to conflicts of interest that may arise in the proxy decision making process. For example, conflicts may arise under the following circumstances:

- Proxy votes regarding non-routine matters are solicited by a company that has an institutional separate account relationship with the Firm.
- A Firm employee has a personal interest in the outcome of a particular proxy proposal (which might be the case if, for example, a member of an employee's immediate family were a director or executive officer of the relevant company).

- A Firm employee (or a household member or related person of that owner, officer or employee) held a position on the board of directors or is 10% or greater shareholder of (or in the case of a household member or related person, is an officer of) a company, whose securities are held by a client and from whom the company is soliciting the client's proxy.

The Chief Investment Officer, in consultation with the Chief Compliance Officer, decides whether or not a conflict in fact exists and seeks to resolve all such conflicts in the client's best interest. Voting in accordance with the voting factors described above will generally prevent any conflicts that arise from influencing the Firm's exercise of its voting authority. The Chief Compliance Officer inquires whether the Firm has any interests that could be viewed as potentially conflicting with the interests of the clients. If there are any potential conflicts, the Chief Compliance Officer may consult, as appropriate, with an independent consultant or outside counsel to determine what votes on those proposals would be in the collective best interest of the clients.

A log of Proxy Voting Conflict Of Interest Determinations is maintained. A copy of this form is included with these procedures. Each time a conflict of interest is determined to exist, the log is updated to include the relevant security and the disposition of the solicitation.

17.11 UNSUPERVISED CLIENT ASSETS
All proxy ballots received for unsupervised assets held in client accounts are immediately forwarded to the client. Such assets should be reflected on the Client Do Not Vote List. A file containing the front page of the proxy statement forwarded to the client is maintained chronologically by year.

17.12 CLIENT REQUESTS FOR PROXY VOTING INFORMATION
All client requests for proxy voting information are brought to the attention of the Chief Compliance Officer who will send a response letter to the requesting client within *10 days* of the receipt of the request. A copy of the Proxy Voting Information Request is included with these procedures. The response letter includes all relevant information regarding the Firm's proxy voting procedures or the particular votes cast on behalf of the client, including:

- Name of security
- Date the proxy was voted
- How the proxy was voted; or if not voted
- When the proxy statement and ballot were forwarded to the client for voting, if applicable

17.13 MAINTENANCE OF BOOKS AND RECORDS
The Chief Investment Officer or their designee is responsible for compliance with applicable proxy voting recordkeeping requirements. The records may be kept electronically in a non-rewritable format. The Firm may rely upon the SEC's EDGAR electronic filing system which maintains corporate records and any other database that stores proxy solicitations on behalf of issuers. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- Proxy voting guidelines.
- Records of votes cast on behalf of clients.
    - The Firm keeps copies of each proxy ballot voted chronologically by year.
- Any documents prepared or reviewed that were material to making a decision on how to vote, or that memorialized the basis for the decision.
    - Any such documents are attached to the applicable proxy ballot and filed as above.

- Log of Conflict-of-Interest Determinations.
- Client Requests for Proxy Voting Information and the Firm's response.
    - A response letter to all client proxy information requests is sent to the client within *10 days*. Copies of all response letters are kept in a chronological file maintained by the Chief Investment Officer or their designee.

18.0 Privacy - Safeguarding Client Financial Information

BACKGROUND

The Firm's clients provide private financial information when opening an account that is subject to protection under Regulation S-P. The Firm collects non-public client information to facilitate the investment management services it provides, including executing authorized securities transactions, providing general client service and fulfilling other legal and regulatory requirements. The type of private information collected depends upon the nature of the financial services requested by each client, but generally includes:

- Personal information obtained at the time an account is opened such as name, address, social security number, family information, assets and income, liabilities, investment objectives, and the like; and
- Information about investment activity in a client's account.

Adasina safeguards non-public client information in accordance with industry standards and established security standards and procedures. Measures taken in this regard include implementation of physical, electronic and procedural safeguards.

18.1 SAFEGUARDING CLIENT INFORMATION

The Firm and each employee and any individuals servicing the Firm's clients must take appropriate steps to prevent the disclosure of non-public client information to third parties. The following precautions should be followed:

- Employees and any individuals servicing the Firm's clients should not access non-public information unless necessary as part of their duties and responsibilities;
- Employees and any individuals servicing the Firm's clients should not discuss non-public information unless necessary as part of their duties and responsibilities;
- Employees and any individuals servicing the Firm's clients must keep all paper copies of confidential and proprietary information that are not in use off computer screens, desktops, conference tables or any other place where such copies would be visible to persons who are not authorized to have access to such information;
- Employees and any individuals servicing the Firm's clients may not take documents containing confidential and proprietary information from the Firm's offices or download such documents to a local harddrive or device without the prior consent of the Chief Compliance Officer. Any copies removed from the Firm's offices must be returned promptly and any locally saved or downloaded documents must be securely deleted from all local or portable electronic storage devices;
- All appropriate electronic safeguards employed by the Firm to maintain the security of its computer data from unlawful intrusion such as anti-virus, firewall and spyware software, encryption software and similar safeguards are maintained and updated routinely;
- THE LOSS OF ANY ELECTRONIC DEVICE CONTAINING CLIENT DATA MUST BE REPORTED TO THE CHIEF COMPLIANCE OFFICER IMMEDIATELY;

- Employees and any individuals servicing the Firm's clients may photocopy confidential and proprietary information only if required to do so as part of their employment duties. All copies and originals of such documents that are not otherwise required to be maintained as Firm records must be disposed of by shredding, or if an electronic record, deleted securely;

- Access to any hardware and software for individuals servicing the Firm's clients is restricted by individual passwords which are updated on an as needed basis. Employees and any individuals servicing the Firm's clients should secure their computer at the end of each day. All employees must notify the Chief Compliance Officer of the logon and password to their work computer and neither login nor password should be changed without immediate notification to the Cybersecurity Compliance Team or their designee; and

- Client private information and Firm business may not be disclosed to any person, including any spouse or other household member, who is not an employee or any individual servicing the Firm's clients and who does not have a reason to know such information.

18.2 ACCESSING CLIENT INFORMATION
Access to non-public client information is granted only in connection with Firm business purposes and only to Firm employees and authorized third parties retained to assist the Firm in its provision of financial services to its clients. Access is based on a person's "need-to-know" the information in providing products or services to Firm clients and to allow the orderly and accurate execution and settlement of financial transactions. The Firm requires each of its employees and third-party providers who have access to client information to protect it and keep it confidential.

18.3 DISPOSAL OF CLIENT INFORMATION
Rule 30, enacted to regulate financial institutions under Regulation S-P requires that every investment adviser registered with the SEC that maintains or otherwise possesses consumer non-public information used for a business purpose must properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

When disposing of hard copy and electronic information related to its clients, the Firm will:
- Wipe clean or remove and destroy all hard drives of client information before disposing of any electronic devices;

- Adopt any further practices reasonably designed to safeguard client information during the disposal of documents and electronic records.

18.4 SECURITY BREACHES

18.4.1 RESPONDING TO PRIVACY BREACH
If any employee and any individual servicing the Firm's clients becomes aware of an actual or suspected privacy breach, including but not limited to any improper disclosure of client private information through a cyberattack, that person must promptly notify the Cybersecurity Compliance Team. Because most states require prompt specific notification to affected individuals of such a breach involving nonpublic personal information, the Firm must investigate an actual or suspected breach that may involve such information as quickly as possible and discuss the issue with legal counsel. The Firm's investigation and response will include the following, as appropriate:

- To the extent possible, identify the information that was disclosed and the improper recipients;

- Take any actions necessary to prevent further improper disclosures;

- Take any actions necessary to reduce the potential harm from improper disclosures that have already occurred;

- Consider discussing the issue with regulatory authorities or law enforcement officials;

- Evaluate the need to notify affected clients - The Firm is required by most states to provide notice as soon as possible to the affected client unless the investigation determines that the misuse of information about the client has not occurred and is not reasonably likely to occur;

- Make any required notifications promptly, and submit required documents to state and federal government agencies, if any of the foregoing is required by applicable law;

- Collect, prepare, and retain documentation associated with the inadvertent disclosure and the Firm's response; and

- Evaluate the need for changes to the Firm's privacy protection policies and procedures in light of the breach.

18.4.2 REQUIRED NOTICE OF BREACH

California law requires that any advisor that owns or licenses computerized data that includes personal information must disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. Only if the personal information was adequately encrypted and is unreadable (and there is no reasonable likelihood of harm to the affected client(s)), is notification not required.

Such notice must be made in good faith, in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement and with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the computerized data system. If Firm personnel or any individuals servicing the Firm's clients become aware of a breach of the security of the Firm's computer system or hard copy files, they should immediately inform the Cybersecurity Compliance Team who will conduct a prompt investigation to determine if personal information has been compromised and assess the risk of misuse. The Firm is required to provide notice as soon as possible to the affected client unless the investigation determines that the misuse of information about the client has not occurred and is not reasonably likely to occur. Such required notice to clients must be made without unreasonable delay.

California Civil Codes s. 1798.29(e) and s. 1798.82(e) require the Firm to notify any California resident whose *unencrypted personal information* was acquired, or reasonably believed to have been acquired, by an unauthorized person. The law requires the Firm to send to the State an electronic sample of the breach notification sent to California residents, *if the breach affected more than 500 residents*. The sample should exclude any personally identifiable personal information.

Notification must be made as soon as possible, in one of the following manners:

- Written notification to the affected client(s);

- Electronic, if this is the customary means of communication between the Firm and its client(s); or

- Telephone notice provided that the Firm can directly contact the affected client(s).

Notification may be delayed if a law enforcement agency determines that it will impede a criminal investigation. If an investigation into the breach or consultation with a federal, state or local law enforcement agency determines there is no reasonable likelihood of harm to consumers, notification is not required.

18.5 SHARING INFORMATION

The Firm does not sell or otherwise distribute client lists or non-public client information. In the course of conducting its business, and as allowed by law, the Firm may disclose necessary non-public information to non-affiliated third parties:

- If requested or authorized by the client;

- To provide client account services or account maintenance;
- To respond to subpoena/court order, law enforcement or regulator;
- To perform services for the Firm or on its behalf to develop or maintain proprietary trading or other software;
- In connection with a proposed or actual sale, merger, or transfer of all or a portion of the Firm's business or an operating unit;
- To help the Firm prevent fraud;
- With rating agencies, persons assessing compliance with industry standards, or to the attorneys, accountants and auditors of the Firm;
- To comply with federal, state or local laws and other legal requirements; and
- Pursuant to any other exceptions enumerated in the California Information Privacy Act.

18.6 IDENTITY THEFT PREVENTION

The increasing sophistication of technology hackers renders all electronic information sharing and storage open to the embezzlement and/or theft of client assets. It is Firm policy to take all reasonable precautions to protect its clients from identity theft by safeguarding the private client information in its records. It is Firm policy to safeguard client assets by implementing procedures to inhibit persons posing as clients or otherwise accessing client funds without authorization.

The Firm does not hold or maintain consumer transaction accounts or advance credit or funds to its clients. Therefore, it has not adopted an identity theft prevention program ("ITPP") under the "Red Flag Rules" and relies on the ITPP implemented by each of its clients' custodians. Nevertheless, because the Firm recommends to clients one or more qualified custodians to maintain their investment accounts, the Firm conducts appropriate due diligence with respect to the ITPPs adopted by the custodians it recommends.

The Firm's policy is to protect clients and their accounts from identity theft by implementing appropriate identity theft prevention procedures that limit the risk of identity theft in relation to Firm operational procedures. The Firm's Chief Compliance Officer is responsible for the oversight development and implementation of the Firm's identity theft prevention procedures.

18.7 IDENTITY THEFT PREVENTION – CLIENT FUNDS TRANSFERS

The Firm assists its clients with recurring and occasional payments to client-approved third parties (i.e. to a party other than the client or to an account that is not "identically titled"). In order to avoid taking custody of client funds, Firm employees are precluded from facilitating the transfer of funds out of client investment accounts to third parties without first obtaining specific client direction and satisfying all custodian requirements[6] for written client authorization. Written wire transfer authorizations or Standing Letters Of Authorization ("SLOAs") - executed by the client whose identity is confirmed by the Firm – are typical custodian transfer requirements. In its effort to assist clients with third-party transfers, the Firm implements the following identity theft prevention procedures to make certain that the identity of the client and the requests for a transfer are verified before implemented.

18.7.1 VERIFICATION OF CLIENT TRANSFER INSTRUCTIONS

If the client has specified in an SLOA that a given payment to an authorized third-party is to occur regularly on a set schedule, or periodically at the request of the client, the Firm may order the payment based upon the

[6] In the absence of an SLOA or written wire transfer instructions executed by the client, a custodian will not typically execute a third party transfer ordered by an investment advisor. In fact, in the absence of an SLOA or written transfer instructions executed by the client, such a transfer authorization by an investment advisor would confer custody on the advisor and invoke the surprise examination requirement of the SEC's Custody Rule.

prior written authorization granted by the SLOA without additional client verification. For such authorizations, the SLOA should specify the exact amount of the payment, the third-party recipient and the timing of the payment (i.e. first day of the month or the like).

For payments to third parties where an SLOA has not been written to provide timing and amount specifications, the client's custodian and the Firm will require that written authorization to the custodian for the transfer specifying the payment, timing, and third-party recipient account and routing information for each transfer. The Firm also will verify the identity of the client making the transfer request as follows:

- If the client makes the request via phone call, a portfolio manager or client services staff person that is familiar with the client's voice must speak to the client personally and verify the client's identity. If a portfolio manager or client services staff person is not familiar with the client's voice, the request should be confirmed by asking the client to verify their personal information, such as; social security number, address, children's names, Firm contact or other information that a person impersonating the client would not have. Once the client's identity has been confirmed, the staff member must also verbally verify details of the requested transfer including; dollar amount, receiving bank name, receiving account registration and the last four digits of the receiving account number.

In the event that the client's voice cannot be authenticated by a staff person, the client must be directed to the client's custodian for processing the transfer to a third-party.

- If the client request comes to the Firm via voicemail to authorize the request, a portfolio manager or client services staff person that is familiar with the client's voice must call the client at the client's telephone number of record and verify the client's identity. If a portfolio manager or client services staff person is not familiar with the client's voice, the request should be confirmed by asking the client to verify their personal information, such as; social security number, address, children's names, Firm contact or other information that a person impersonating the client would not have. Once the client's identity has been confirmed, the staff member must also verbally verify details of the requested transfer including; dollar amount, receiving bank name, receiving account registration and the last four digits of the receiving account number.

In the event that the client's voice cannot be authenticated by a staff person, the client must be directed to the client's custodian for processing the transfer to a third-party.

- If the client request comes to the Firm via email (or other non-oral communication), a portfolio manager or client services staff person that is familiar with the client's voice must telephone the client at the client's telephone number of record and verify the client's identity. If the portfolio manager or client services staff person who calls the client is not familiar with the client's voice, the portfolio manager or client services staff person must ask the client to verify their personal information, such as social security number, address, children's names, Firm contact or other information that a person impersonating the client would not have.

Once the client's identity has been confirmed, the staff member must also verbally verify details of the requested transfer including; dollar amount, receiving bank name, receiving account registration and the last four digits of the receiving account number.

In the event that the client's voice cannot be authenticated by a staff person, the client must be directed to the client's custodian for processing the transfer to a third-party.

- In all cases, a confirming email to the client's email address of record should be sent to the client at the time the Firm facilitates the transfer with the client's custodian.

18.8 ANNUAL VERIFICATION OF CUSTODIAN ITPP POLICIES AND PROCEDURES

At least annually, the Chief Compliance Officer will verify with each client custodian that it recommends to Firm clients, that the custodian has adopted and implemented an identity theft prevention program (ITPP) that meets applicable regulatory requirements by including provisions that allow the custodian to:

- Identify relevant red flags for the custodian's covered accounts;
- Detect red flags related to its customers' covered accounts;
- Respond appropriately to any red flags that are detected to prevent and mitigate identity theft; and
- Routinely review and update its ITPP to reflect changing identity theft risks.

18.9 WORKING IN PUBLIC PLACES

Employees and any individuals servicing the Firm's clients should be cautious when using laptops or reviewing documents that contain nonpublic personal information in public places, shared office spaces, or while using any non-private WiFi network to prevent unauthorized people from viewing the information. Employees are required to keep documents containing nonpublic personal information in lockable filing cabinets and are prohibited from leaving documents containing nonpublic personal information and other sensitive information unattended in public spaces or shared meeting rooms, such as lobbies or conference rooms. Employees must secure their computers when they leave the office for any extended period.

18.10 TEMPORARY STAFF AND OUTSIDE SERVICE PROVIDERS

All temporary staff and outside service providers with access to private client financial information are required to review these policies and procedures upon hire and to execute a Confidentiality Agreement.

18.11 DUE DILIGENCE CONDUCTED ON THIRD-PARTY SERVICE PROVIDERS

For any instance where client data may have nonpublic "personally identifiable financial information", the Firm conducts due diligence when hiring any third-party service providers and when subscribing to online services in order to form a reasonable belief that such provider is familiar with security issues and able to safeguard Firm client data to which it may have access. The Firm performs initial and on-going due diligence of each third-party service provider of services to the Firm where the services provider has access to private client information or the Firm's investment recommendations.

18.11.1 INITIAL DUE DILIGENCE

The Chief Compliance Officer or a Firm principal conducts and documents the following due diligence tasks, *as deemed appropriate to the contemplated relationship*, when considering a new third-party service provider relationship:

- Determines how much experience the service provider has in providing its services.
- Determines how long the service provider has been in business.
- Conducts an internet search of the service provider and its principals and the employees that would be assigned to work with the Firm.
- Determines if the service provider primarily services the investment management industry.
- Determines which processes the service provider follows to make certain its services and systems comply with industry requirements and standards.
- Determines if the service provider is familiar with federal and state securities laws.
- Determines if the service provider is familiar with federal and state privacy laws.
- Determines which background checks the service provider conducts on its employees.
- Determines if the service provider's principals and employees are bonded and insured.

- Verifies that the provider has policies and procedures in place for protecting the Firm's private client financial information and investment decisions.
- Determines whether the provider has an appropriate risk/compliance program.
- Determines whether the service provider has a business continuity plan.
- Determines whether the provider is a part of a regulated industry and inquires as to the results of any recent regulatory exams the service provider has undergone.

18.11.2 ONGOING DUE DILIGENCE

At least annually, the Chief Compliance Officer conducts and documents the following due diligence tasks, *as may be appropriate to the relationship*, when reviewing an existing third-party service provider relationship:

- Requires the service provider to sign a confidentiality agreement or certification of its own privacy and security procedures and practices.
- Periodically reviews the qualifications and oversight capabilities with respect to the specific services that the Firm has delegated to the service provider.
- Evaluates the effectiveness of the reports prepared by the service provider for the Firm (i.e., types of reports produced and conditions under which exceptions are raised to the Firm's attention) and the frequency with which the reports are produced.
- Ensures that the service providers are performing all contracted functions.
- Verifies that the service provider is creating and maintaining the documentation necessary to ensure that such records are compliant with the needs of the Firm.
- Makes on-site visits to the service provider's facilities to view operations in action, *as and if deemed necessary.*

18.11.3 OTHER THIRD-PARTY SERVICE PROVIDER CONSIDERATIONS

- The Firm may not represent that a service provider is "independent" when it is under common control or otherwise has a close connection with the Firm.
- Clients may not be charged excessive and/or duplicative fees for third-party administration and/or accounting services.
- The Firm must validate the accuracy of pricing provided by third parties when fees are charged directly to clients.
- The Firm may not participate in any arrangements whereby clients make payments to various third-party service providers and, in turn, the service providers make payments directly to the Firm ("quid pro quo" arrangements).
- The Firm may not use client funds to pay third-party consultant fees that should be paid by the Firm.
- Third-party contractors with access to client investment recommendations may require designation as an Access Person.

18.12 VIOLATIONS OF FIRM CLIENT PRIVACY PRACTICES

Each employee is required to notify the Chief Compliance Officer immediately if they learn of a breach of the Firm's client privacy policies or procedures.

18.13 STAFF TRAINING ON IDENTITY THEFT PREVENTION PROCEDURES
As necessary, the Cybersecurity Compliance Team will conduct staff training on the Firm's identity theft prevention procedures with new and existing employees.

18.14 UPDATE OF FIRM IDENTITY THEFT PROCEDURES
The Firm updates these identity theft procedures whenever there is a material change to our operations, structure or business or to those of client custodial firms, or in response to a material identity theft suffered by a client or related to a client account. The Firm's identity theft policies, procedures and internal controls are reviewed and updated at least annually by the Chief Compliance Officer to ensure they reflect changes both in identified threats, industry practices, applicable regulations and Firm operations.

18.15 TRANSMITTAL OF STATEMENT OF PRIVACY POLICY TO CLIENTS
A current version of the Firm's *Statement of Privacy Policy* accompanies these procedures. The Firm is required to provide each new client with a copy of the Statement of Privacy Policy at the time they become a client and to send the *Statement of Privacy Policy* to existing clients annually.

18.15.1 PROSPECTIVE CLIENTS
Prospective clients are provided a copy of the Statement of Privacy Policy along with the Firm's Form ADV Part 2 (brochure) during initial discussions with the prospective client, prior to the prospective client being asked to execute an investment management agreement.

18.15.2 EXISTING CLIENTS
A copy of the Firm's current Statement of Privacy Policy is sent to all existing clients at least annually. A list of all clients that were sent a copy of the privacy notice is kept by the Chief Compliance Officer along with the version of the privacy statement sent.

18.15.3 FIRM WEBSITE
A copy of the Firm's current Statement of Privacy Policy is provided to clients on the Firm's website.

18.16 REQUIREMENTS OF THE STATE OF CALIFORNIA
California regulations require:

- An affirmative opt-in before information can be shared with non-affiliated third parties;
- An opt-out for sharing amongst affiliates;
- And the provision of a self-addressed envelope with prepaid postage if there are not at least two free ways for the client to provide the opt-in authorization (e.g. toll-free telephone or email).

California adopted the 2019 California Consumer Privacy Act ("CCPA") that establishes strict notice and opt-out requirements for California businesses that collect private consumer data. The CCPA applies to any for profit business that collects and accesses the personal data of California residents:

- That has an annual gross review of $25M or more, or
- That derives more than half of its annual revenue from selling consumers' personal data, or
- That buys, sells, or shares the personal data of more than 50,000 consumers, households or devices (computer IP addresses, cellphone numbers etc.).

In order to avoid inadvertently collecting the personal data of more than 50,000 California consumers, the Firm should disable any of the data collection protocols on the Firm website.

The Chief Compliance Officer is responsible for informing all temporary employees and outside service providers of the Firm's privacy procedures with respect to safeguarding client nonpublic information.

18.17 AFFILIATES AND THIRD-PARTY ARRANGEMENTS
No employee and any individual servicing the Firm's clients may enter into a third-party arrangement without the review of the Chief Compliance Officer and the approval of senior management. Any affiliate or third-party arrangement that would necessitate the sharing of non-public client information beyond the scope of the Firm's client privacy policies would require the Firm to notify its affected clients ahead of time and provide them with the opportunity to "opt out" of any transfer of non-public information to such non-affiliated third-party. Any such arrangement may necessitate the revision of these policies and procedures and other Firm documents.

18.17.1 USE OF DATA MANAGEMENT SERVICES
The Firm is aided in its ongoing client account monitoring and management services by the use of third-party portfolio and trade data management software and services provided by Custodians, as well as other software providers.. Such third-party services provide linked access to client custodial accounts and trade activity and provide "cloud" storage of such data on their secure, internal computer servers on behalf of the Firm.

The Firm's Statement of Privacy Policies should disclose any sharing of private client data with third-party service providers.

Contracts with third-party service providers should include a CCPA provision if there is, or could be, sharing of personal information. Vendors that process personal data should have contracts updated to comply with the CCPA and restrict the vendor's right to use data.

18.18 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer supervises the Firm's compliance with applicable privacy recordkeeping requirements. Records may be kept electronically in a non-rewritable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- All client funds transfer requests and communications verifying the legitimacy of such requests.
- Documentation of verification of custodian and broker-dealer ITPP.
- Executed temporary employee and outside service provider acknowledgements and certifications.
- Lists of current clients receiving annual copy of Privacy Policy statement.
- Current and historic versions of the Statement of Privacy Policy.
    - A chronologic file or report is maintained by the Chief Compliance Officer. With respect to each year's annual mailing of the Statement of Privacy Policy to clients, the file copy bears a notation of the date the statement was sent to clients and a list of clients to whom it was sent.
- Copies of all regulatory, law enforcement or judicial subpoenas requiring the Firm to disclose client non-public information.
    - A chronologic file of subpoenas served on the Firm is maintained by the Chief Compliance Officer.
- Copies of third-party service provider due diligence.

19.0 Referral Arrangements

The Firm currently is not a party to any third-party marketing relationships with outside solicitors. The Firm may enter into such relationships in the future whereby the Firm would pay a referral fee to persons or entities that

refer clients to it. Such relationships may only be approved by the Chief Compliance Officer, must be documented in writing, and are subject to specific solicitor qualification and client disclosure rules. At such time, if ever, as the Firm enters into any third-party solicitation or marketing arrangements, appropriate policies and procedures will be instituted.

The following referral fee practices are prohibited:

- Any rebate of fees to clients as a means of paying a referral fee;
- Payment of referral fees to anyone or any company pursuant to any arrangement that has not met all regulatory disclosure requirements and been properly documented; and
- Payment of excess fees to anyone or any company as a means of paying a referral fee.

20.0 Regulatory Reporting: Form ADV, Rule Filings, IARD Maintenance

Adasina is committed to the timely and accurate filing of all regulatory forms, statements and reports required of it.

20.1 DETERMINING NEW SEC REGULATORY REQUIREMENTS

The Chief Compliance Officer will identify new regulatory requirements from the SEC and other regulatory agencies as needed, and update this Manual with new or amended policies and procedures, as required by the regulations.

20.2 IARD, WEBCRD AND THE SUPER ACCOUNT ADMINISTRATOR

The Firm's IARD files and WebCRD records are accessible on the internet at https://crd.finra.org/iad through use of the Firm's login name and password. The Firm has designated an IARD Super Account Administrator ("SAA") by completing an IARD Entitlement Form and filing it with IARD. The Firm's IARD SAA is Maya Philipson. The SAA is responsible for designating any other account administrators at the Firm. At least annually, usually in June or July (when FINRA sends a reminder), the Firm's SAA must log onto IARD/WebCRD and certify all of the Firm's current user accounts and entitlements. Any changes to the Firm's electronic entitlements must be made through the filing of an amended IARD Entitlement Form. This Form is also used to entitle additional users.

20.3 FORM ADV PART 1

20.3.1 ANNUAL AMENDMENT

The Firm is obligated to file a Form ADV Part 1 Annual Amendment within 90 days of the end of its fiscal year. As the Firm's fiscal year end is December, the annual update is due by the end of March of each year.

20.3.2 STATE NOTICE FILINGS

In order to avoid having federally registered investment advisors register with the individual states in which their clients reside, the IARD system allows advisors to "Notice File" with each state where an advisor has more than an exempted minimum of clients by paying an annual notice filing fee to the applicable state through IARD. The notice and the fee are then transmitted to each state designated and the advisor's Form ADV Part 1 is made available to the state regulators through IARD.

The Firm may have client accounts for clients who live outside of California. As the Firm acquires clients who live in other states, it is required to track these clients and, if exceeding the individual state's exemption requirement (known as the "*de minimis*'' exemption – each state sets its own *de minimis* exemption level but generally, it is at least five clients in the state), to notice file in those states by amending its Form ADV Part 1 and paying annual state notice filing fees through the Firm's IARD account.

IARD conducts an annual Renewal Program for investment advisors in November and December of each year whereby investment advisors are required to deposit their state notice filing fees for all state jurisdictions for

the following year. As the fees assessed are based on the current year's notice filings, the Firm must amend its Form ADV Part 1 at this time to delete any state jurisdiction whose *de minimis* exemption is no longer exceeded due to loss of clients or clients having moved to another jurisdiction.

Some states do not provide a *de minimis* exemption and the Firm will have to file notice on acquiring even one client in the state. The notice filing must be made immediately upon exceeding the exemption or in cases where a state does not provide an exemption, upon the acquisition of the first client in that state.

On no less than an annual basis, the Firm reviews its list of client accounts to determine if a notice filing should be made.

20.4 FORM ADV PART 2

The Form ADV Part 2 is the Firm's primary client disclosure document and is considered the Firm's "brochure" under applicable SEC Rules. Among other things, it must contain all required disclosures to clients regarding the Firm's existing and potential conflicts of interest. The Form ADV Part 2 is amended at least annually and is required, in part, to be uploaded as a PDF attachment to the Form ADV Part 1 annual amendment filed on the IARD system.

The ADV 2 is comprised of two sections. Part 2A is the Firm's primary disclosure statement regarding the Firm's organization and business structure and any disciplinary information regarding the Firm itself. The Part 2B Supplement(s) describes each of the Firm's investment advisory personnel and provides disclosures related to their qualifications, business experience and regulatory event or other disciplinary history.

20.4.1 ANNUAL AMENDMENT TO FORM ADV PART 2A

At least annually, in conjunction with the Firm's annual amendment to Form ADV Part 1, the Chief Compliance Officer reviews and updates the ADV Part 2A.

20.4.2 SUPERVISED PERSONS REQUIRING A PART 2B SUPPLEMENT

Each person who formulates investment strategies for clients, determines the investment advice to be given to clients or has discretionary authority over client assets is required to have a Part 2B Supplement setting forth their qualifications, all conflicts of interest and regulatory disclosures.

20.4.3 CLIENT-SPECIFIC DISTRIBUTION OF PART 2B SUPPLEMENTS

Each new and existing client must be given a copy of the Part 2B Supplement only for those supervised persons that provide advice to that client, formulate investment strategy for that client or have discretion over that client's assets.

20.4.4 TIMING OF DISTRIBUTION OF PART 2B SUPPLEMENTS

The Firm must deliver each required Part 2B Supplement to a new or existing client before or at the time the supervised person begins to provide services for that client.

20.4.5 ANNUAL AMENDMENT OF FORM ADV PART 2B

The Chief Compliance Officer reviews each supervised person's Part 2B Supplement at least annually and determines if any revisions need to be made.

20.4.6 DISTRIBUTION OF ADV PARTS 2A AND 2B

20.4.**6**.1 DISTRIBUTION TO PROSPECTIVE CLIENTS

The Part 2A and each required Part 2B Supplement must be distributed to all new clients prior to the time they enter into an investment advisory agreement with the Firm.

20.4.6.2 DISTRIBUTION OF PART 2A TO EXISTING CLIENTS

In addition, the Firm is required to distribute a current Part 2A – or a Statement of Material Changes and an offer to distribute - to all of its existing clients within 120 days of the Firm's fiscal year end (April 30th) and to provide a current copy to any client on request.

The Chief Compliance Officer directs the distribution of the Firm's current ADV Parts 2A to all existing clients.. The Chief Compliance Officer must keep a copy of the distributed amended ADV Part 2A along with a list of all clients that were sent the document and noting the method of delivery for each client.

20.4.6.3 DISTRIBUTION OF PART 2B SUPPLEMENT TO EXISTING CLIENTS

The Part 2B Supplement does not need to be sent to existing clients annually unless it has been updated with material changes.

20.4.6.4 ELECTRONIC DISTRIBUTION

For those clients that have authorized the Firm to deliver materials to them electronically, the Firm may email a non-rewritable PDF of the ADV Part 2 via email. The Chief Compliance Officer must keep a copy of the distributed amended ADV Part 2 along with a list of all clients that were sent the document and noting the method of delivery for each client.

20.5 FORM ADV CLIENT RELATIONSHIP SUMMARY

The Form CRS Relationship Summary is a maximum two-page narrative summary of the full description of services, fees conflicts and other disclosures contained in each RIA's current Form ADV Part 2A. It is a short-form disclosure document to inform, distributed to clients and prospective clients about:

- the types of client and customer relationships and services the Firm offers;
- the Firm's fees, costs, conflicts of interest, and required standard of conduct associated with those relationships and services;
- whether the Firm and its financial professionals currently have reportable legal or disciplinary history; and
- how a client or prospect may obtain additional information about the Firm.

20.5.1 DISTRIBUTION OF FORM CRS TO NEW CLIENTS

The Firm must deliver a copy of the Form CRS to each prospective new client at the time he/she/it enters into an investment management/financial consultation arrangement with the Firm.

If the relationship summary is delivered on paper and not as a standalone document, the Firm must ensure that it is the first among any documents that are delivered at that time.

20.5.2 DISTRIBUTION TO EXISTING CLIENTS

The Firm must deliver Form CRS to each existing client within 30 days of its initial upload to IARD and:

- before or at the time a new account is opened for the client that is different from the client's existing account(s);
- when changes are made to the client's existing account(s) that would materially change the nature and scope of the Firm's relationship with the retail investor (e.g., if the Firm recommends that a client transfers from an from a brokerage account to an investment advisory account, or to rollover assets from one type of account to another in a transaction not in the normal, customary or already agreed course of dealing with the client);
- upon client request;

- within 30 days of any material update of the Form CRS.

Form CRS may be delivered via email to all existing clients that have authorized the Firm to send documents electronically.

20.5.3 FORM CRS MUST BE POSTED TO THE FIRM'S WEBSITE
The Firm must post its current Form CRS prominently on its public website and make it easily accessible for client and prospects to review.

20.5.4 AMENDMENT OF FORM ADV PART 3
Form CRS must be updated within 30 days if it becomes materially inaccurate and each update must be uploaded to IARD, uploaded to the Firm's website and distributed to all existing clients within 30 days.

Firms may, but are not required, to submit amended versions of the Form CRS as part of the Firm's annual updating amendment.

20.6 STATE-REQUIRED REGISTRATION OF INVESTMENT ADVISOR REPRESENTATIVES
Although the SEC does not require the registration of individual investment advisor employees, certain states require registration of each employee that qualifies as an investment advisor representative ("IAR").

Registration of IARs is accomplished by filing a Form U-4. The individual Form U-4 records of registered investment advisor representatives are maintained electronically on WebCRD, rather than IARD

20.6.1 CALIFORNIA REGISTRATION REQUIREMENT

20.6.1.1 DEFINITION OF INVESTMENT ADVISOR REPRESENTATIVE
California requires registration of the following employees of SEC registered advisors:

"Investment advisor representative" is defined in Corporations Code Section 25009.5(b) as any person defined as an investment advisor representative by Rule 203A-3 of the Securities and Exchange Commission and who has a place of business in California. An investment advisor representative is defined in Rule 203A-3 as a supervised person of the investment advisor who has more than five clients who are natural persons (other than "excepted persons") and more than ten percent of whose clients are natural persons (other than "excepted persons").

"Excepted person'' means a natural person who is a qualified client as described in Sec. 275.205-3(d)(1) of the Act as a natural individual/couple or company that:

- Has $1,100,000 under management with the advisor; or
- The advisor reasonably believes has a net worth of at least $2.2 million, exclusive of any primary residence; or
- Has a total of at least $5 million of investments (a "qualified purchaser").

A qualified client also includes both a "qualified purchaser" as defined in section 2(a)(51)(A) of the Investment Company Act of 1940, and an investment adviser's "knowledgeable employees".

Employees are not IARs if they do not, on a regular basis solicit clients, or in an unsupervised manner, conduct investment research, analyze client financial condition, investment suitability or risk tolerance, provide financial consulting services, make investment recommendations, or otherwise communicate with clients of the investment advisor on an non-administrative basis or provides only impersonal investment advice.

20.6.2 REQUIRED QUALIFICATIONS

Unless otherwise exempted from the examination requirement, registered IARs must have successfully passed the FINRA Series 65 exam or both the Series 7 and Series 66 exams.

20.6.2.1 EXAM EXEMPTION FOR PROFESSIONAL DESIGNATIONS

Although still required to register and file a Form U-4, IARs are exempted from taking the Series 65 exam if they maintain any of the following designations:

- Chartered Financial Analyst ("CFA")
- Chartered Financial Consultant ("ChFC")
- Certified Financial Planner ("CFP")
- Chartered Investment Counselor ("CIC")
- Personal Financial Specialist ("PFS")

20.6.2.2 GRANDFATHER PROVISION

California regulations exempt from the examination requirement any IAR who has been actively and continuously engaged in the securities business as a broker-dealer, an agent of a broker-dealer, an investment advisor, or an IAR without substantial interruption (2 or more years) since passing the:

- Series 2 (SEC/FINRA Nonmember General Securities Examination) or Series 7 before February 1, 1998, or
- Series 65 or Series 66 before February 1, 2000 and the Series 7 Examination

20.6.3 NEWLY HIRED INVESTMENT ADVISOR REPRESENTATIVES

Any time a new employee is hired, the Chief Compliance Officer will determine if that person is required to register as an IAR. Upon hiring a new employee that is required to register as an IAR, the Chief Compliance Officer will:

20.6.3.1 EMPLOYEES WITH EXISTING FORM U-4 REGISTRATION

- Transitions the employee's existing Form U-4 noting Firm as the new employer, making other changes as necessary and requesting state jurisdiction registration as applicable
- Files a copy of the employee's U-4 in the employee's personnel file
- Saves a copy of employee's exams and files it in the employee's personnel file
- Subsequently monitors WebCRD to ensure registration follow-through

20.6.3.2 EMPLOYEES WITHOUT PRIOR FORM U-4 REGISTRATION

- Creates an initial Form U-4 filing online on WebCRD/IARD for the employee.
- Files a copy of the employee's U-4 in the employee's personnel file.
- Coordinates the employee's Series 65 exam schedule;
- Saves a copy of employee's exams and files it in the employee's personnel file.
- Subsequently monitors WebCRD to ensure registration follow-through.

20.6.4 AMENDMENT OF REGISTERED EMPLOYEES' FORMS U-4
Registered employees are required to notify the Chief Compliance Officer of changes in home address and the Chief Compliance Officer amends the employees' Form U-4s, as necessary.

20.6.5 REVIEW OF FIRM AND EMPLOYEE DISCLOSURES
At least annually, the Chief Compliance Officer reviews each registered employee's U4 information to ensure it is up to date.

20.6.6 TERMINATED INVESTMENT ADVISOR REPRESENTATIVES
The Chief Compliance Officer files a Form U-5 within 30 days of any registered IAR leaving the Firm. A copy of the completed and filed Form U-5 must be sent to the former employee within the 30-day period at his or her last known address.

20.7 FORM FILINGS UNDER SEC RULE 13 - EDGAR FILINGS

20.7.1 FORM 13F – REPORTS BY INSTITUTIONAL INVESTMENT MANAGERS

Form 13F must be filed when the Firm's discretionary account holdings of specified Section 13(f) equity securities have an aggregate fair market value on the last trading day of any month of any calendar year of at least $100,000,000. The Firm must file its first Form 13F for the December quarter of the calendar year during which it first reaches the $100 million threshold. The initial Form 13F must be filed within 45 days after the last day of the calendar year. Subsequent filings must be submitted within 45 days after the last day of each of the first 3 calendar quarters of the subsequent calendar year (March, June and September), even if the market value of the 13(f) securities falls below $100 million.

See Form 13F -—Reports Filed by Institutional Investment Managers | Investor.gov for the filing of forms on the EDGAR database. Once the Firm sets up its initial Form 13F filing, subsequent filings are a simple matter of updating the initial filing. Information for filing an initial Form 13F and quarterly amendments on the EDGAR system is here, including instructions regarding the filing of forms on the EDGAR database. Once the Firm sets up its initial Form 13F filing, subsequent filings are a simple matter of updating the initial filing. Information for filing an initial Form 13F and quarterly amendments on the EDGAR system may be found on the above webpage under the heading "Form 13F."

Form 13F filings must include:

- The name of the issuer and the title, class, and CUSIP number of the security;
- The number of shares or principal amount of each class held of the security;
- Whether the holdings are put or call options;
- The market value of each class of the security held;
- The investment discretion held by the Firm for each class
- Whether the investment discretion is shared with another person or manager; and
- Such other related information as the SEC, by rule, may prescribe.

20.7.1.1 QUALIFYING SECTION 13(f) SECURITIES DEFINED

Section 13(f) securities are equity securities as described in Section 13(d) (1) of the Securities Exchange Act. The list includes exchange-traded or NASDAQ-quoted stocks, equity options and warrants, shares of closed-end investment companies, and certain convertible debt securities.

The SEC's Division of Investment Management webpage provides a link to the current official list of Section 13(f) Securities http://www.sec.gov/divisions/investment/13flists.htm. It is updated at the end of each calendar quarter.

Shares of open-end investment companies, i.e., mutual funds, are not included and, therefore, should not be listed on Form 13F. Shares of exchange-traded funds ("ETFs"), however, are on the Official List and should be reported. Securities that are not on the Official List should not be reported on Form 13F.

20.7.2 Forms 13d And 13g – Reports Of Holders Of 5% Or More Beneficial Ownership Of Qualifying Equity Securities

Form 13D is filed if the Firm, an employee or a client acquires beneficial ownership of more than 5% of a class of publicly-traded equity securities of a single issuer. [Check the Official List of 13F Securities.] Form 13D identifies background information about the acquirer, their or its past legal or disciplinary proceedings, the aggregate amount of shares beneficially owned, the percentage of the class represented the source/amount of funds and the purpose of the transaction. Form 13D presumes the intent of the holding is to influence control of the issuer.

Form 13G is an alternative to Form 13D and is used if the Firm, employee or a client acquires a greater than 5% (but not over 20%) beneficial ownership of shares as a "passive investor," in the ordinary course of business and not for the purpose of influencing control of the issuer. Form 13G requires disclosure of the identity of the acquirer, the aggregate amount of shares beneficially owned and the percent of the class represented.

An advisor must file a Form 13D if, subsequent to filing a Form 13G, it holds or acquires securities with the purpose or effect of influencing control of the issuer or acquires more than a 20% interest. Form 13D must be filed within 10 days of acquiring greater than 5% beneficial ownership. Amendments for material changes filing must be filed promptly. Changes to investment purpose must be made within 10 days.

A Form 13G must be filed within 45 days after the end of the calendar year in which the Firm, employee or client acquired a greater than 5% beneficial ownership in the security. If the relevant beneficial ownership exceeds 10 percent, prior to the end of the calendar year, the initial Form 13G has to be filed within 10 days after the end of the first month in which the beneficial ownership exceeds 10 percent, computed as of the last day of the month.

20.7.3 FORM 13H – LARGE TRADER

Form 13H identifies market participants engaged in substantial trading activity, collects information on their trading, and analyzes trading activity. A "large trader" is defined as a person, including an investment adviser, whose transactions in exchange-listed or over-the-counter securities equal or exceed two million shares or $20 million during any calendar day, or 20 million shares or $200 million during any calendar month.

Form 13H securities include exchange-listed equity securities and standardized options, but do not include exchange-listed debt securities, securities futures, or open-end mutual funds. Upon receipt of the initial Form 13H filing, the SEC assigns the Firm a unique large trader identification number (LTID). A firm is required to disclose to its broker-dealers its LTID and specify all of the accounts at the broker-dealer through which it trades.

An initial Form 13H filing must be made within 10 days after first meeting the filing criteria. The annual Form 13H filing must be made within 45 days after the end of the calendar year in which the Firm first meets the criteria of a Large Trader. The annual filing is required regardless of whether the information on the 13H has changed.

A previously registered large trader who has not conducted the identifying amount of trading activity as measured by volume or market value may file for "Inactive Status" and can remain inactive and exempt from the filing requirements until the large trader trading level is made again.

The Chief Compliance Officer is responsible for verifying that information provided on Form 13H is consistent with that provided on the Firm's Form ADV, Parts 1 and 2. Amended Filings – if any of the information contained in a Form 13H filing becomes inaccurate for any reason, a Large Trader (other than those on Inactive Status) must file an amended filing no later than the end of the calendar quarter in which the information becomes stale.

20.8 FORM FILINGS UNDER SECTION 16 OF THE 1934 ACT

Section 16 of the Securities and Exchange Act of 1934 applies to any person who is the beneficial owner, directly or indirectly, of more than ten percent of any class of equity securities. Section 16 rules apply to any class of equity securities of an issuer whether or not registered. The rules under Section 16 also apply to non-equity securities as provided by the Public Utility Holding Company Act of 1935 and the Investment Company Act of 1940. Under Section 16, Forms 3, 4 and 5 must be filed (electronically via EDGAR) as follows:

- Form 3: In general, an advisor that exercises investment discretion or voting power over more than ten percent (10%) of a class of equity securities of a publicly traded company (and thus is a "beneficial owner" of such securities) may be required to file with the SEC an initial ownership report on Form 3 within ten days after exceeding the ten percent threshold.

- Form 4: Changes in an advisor's/beneficial owner's ownership of securities must be reported on Form 4 before the end of the second business day following the day on which the change occurred. Due to the changes in the filing timeframe for the Form 4, it is possible that a Form 4 may be due before the Form 3 is due. In these situations, the SEC encourages the filer to submit both forms at the same time.

- Form 5: An annual report on Form 5 must be filed by an advisor/beneficial owner within 45 days after the fiscal year, by every person who was an insider of a publicly traded company during the entire year, to report previously unreported transactions during the year that should have been reported on Form 4 but were not, and certain other transactions that may be reported.

20.9 HART-SCOTT-RODINO FILINGS

Under the Hart-Scott-Rodino Antitrust Improvements Act of 1976, the Firm may be required to file a confidential notice with the Federal Trade Commission ("FTC") and the Department of Justice ("DOJ") before acquiring for itself or a client a substantial amount of voting securities or assets of an issuer (whether the securities are publicly-traded or not). After the notice is filed, the acquisition cannot be consummated until the FTC and DOJ have reviewed the transaction and consented.

20.9.1 APPLICABLE THRESHOLDS

Various thresholds trigger a filing requirement under the HSR Act, and the computation of each threshold is complicated and depends on the individual circumstances of the situation. The application of the thresholds to investment advisers' securities purchases is not always clear. The Chief Compliance Officer should consult outside counsel immediately if the Firm and its client accounts together intend to engage in a transaction that will result in their collectively owning the following threshold amounts *These dollar thresholds and the other thresholds under the HSR Act change annually based on changes to the GNP:*

HSR Threshold	2022 Threshold	2022 Fee
Size-of-Transaction	$20.2 million	
	$101 million	$45,000
	$202 million	$125,000
	$222.2 million	"

	$403.9 million	“
	$1.009 billion	$280,000
	$2.019 billion	“

Alternative Size-of-Transaction	$403.9 million	
Size-of-Person	$20.2 million and $202 million	

20.9.2 EXEMPTIONS
Certain types of acquisitions are exempt from the HSR Act filing requirements, even if they exceed the $94 million threshold. For example, an acquisition of voting securities is exempt from the HSR Act filing requirements if it is made "solely for the purpose of investment" and if, as a result of such acquisition, the securities acquired or held do not exceed 10% of the outstanding voting securities of the issuer. Securities are acquired "solely for investment purposes" if the acquirer does not intend to participate in formulating or directing the basic business decisions of the issuer. The "solely for the purpose of investment" exemption is not available to an acquirer who intends to obtain a seat on the issuer's board of directors. Acquisitions of convertible voting stock also are exempt from the HSR Act filing requirements, as are acquisitions of voting stock of non-U.S. issuers whose U.S. assets and sales are below specified thresholds.

20.10 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer supervises the Firm’s compliance with applicable recordkeeping requirements. Records may be kept electronically in a non-writable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- Forms ADV Parts 1 and 2.
    - A chronological file is maintained by the Chief Compliance Officer of superseded versions of the Firm’s Form ADV Parts 1 and 2.
- Employee Forms U-4 and U-5.
    - Employee Forms U-4 and U-5 are maintained in the employee’s file.
    - Employee files are kept for five years after the end of the year of termination.
- Regulatory filings under Rule 13 and Section 16.
- Hart-Scott-Rodino filings.

21.0 Soft Dollar Arrangements

BACKGROUND
Adasina is not currently a party to any formal arrangements whereby it accepts third-party research or brokerage services from a broker-dealer in exchange for placing a minimum number of commissionable client transactions with the broker-dealer.

Adasina does however accept research and brokerage services from Schwab, the custodian of its clients’ investment accounts.. While this institution offers Adasina investment research, practice management and

compliance advice, discounts and/or other services primarily without charge, they do so because the Adasina recommends that its clients custody their investment assets with them. Such research, advice and brokerage services, provided to Adasina without charge, create a conflict of interest in that Adasina is motivated to recommend Schwab to some extent on the basis of these free services as well as on the quality of their custody and brokerage execution quality. As its fiduciary duty is to only act in the best interests of its clients, Adasina remains mindful of this conflict of interest and the best interests of its clients when it accepts research and brokerage services from these institutions and routinely evaluates the quality of their services to its clients in relation to the value of the benefits bestowed on the Firm.

21.1 POLICIES

The Firm's acceptance of research and brokerage services is limited by its fiduciary obligation to act in the best interests of its clients. Only bona fide research and brokerage products and services that provide assistance to the Firm in the performance of its investment management obligations are permitted. The Firm limits its acceptance of investment research and brokerage services from client custodians to those products and services that, if otherwise subject to a formal soft dollar arrangement, would fall within the safe harbor of Section 28(e) of the Securities and Exchange Act of 1934.

The research or brokerage products or services the Firm will accept must meet the following established criteria:

- They must be brokerage and/or research related;
- They must be provided by a qualified custodian at which the Firm's clients custody investment accounts; or
- They must be provided by an executing broker-dealer at which the Firm executes client securities transactions.

21.2 IDENTIFYING ALLOWED BROKERAGE SERVICES AND RESEARCH

21.2.1 ACCEPTABLE BROKERAGE SERVICES

Brokerage services are those that begin from the point at which Firm personnel communicate with a broker to execute an order through the point at which the funds or securities are delivered or credited to the client's account. Permissible services begin when the Firm communicates with the executing broker-dealer for the purpose of transmitting an order for execution and ends when funds or securities are delivered or paid to clear and settle the transaction in the client's account. Services or advice provided by the broker-dealer before the communication of an order do not constitute brokerage services, although they may constitute allowable research. The following brokerage services are allowed:

- Execution, clearing and settlement services;
- Post trade matching services;
- Exchange of messages among broker-dealers, custodians and institutions;
- Electronic communication of allocation instructions between institutions and broker-dealers;
- Routing settlement instructions to custodian banks and clearing agents;
- Electronic confirmation and affirmation of institutional trades;
- Trading software to route orders and algorithmic trading software; and
- Communication services related to the execution, clearing and settlement of securities transactions and other incidental services (i.e., connectivity service between the Firm and the broker-dealer and other relevant parties such as custodians), such as:

- Dedicated lines between the broker-dealer and the Firm's order management system;
- Dedicated lines between a broker-dealer and the order management system of a third-party;
- Dedicated direct dial lines with the trading desk of a broker-dealer; or
- Message services used to transmit orders to broker-dealers for execution; and
- Order management systems that include trading software or provide connectivity to trading software.

21.2.2 PROHIBITED BROKERAGE "SERVICES"
The following should not be accepted:

- Software used for recordkeeping or administrative purposes, including software used to manage portfolios and quantitative analytical software used to test "what if" scenarios (including such functionality provided by order management systems and trade analytic software);
- Products or services used to meet a client's specific investment parameters or for internal compliance, including analysis of best execution, portfolio turnover rate or performance of similarly-managed accounts, creation of trade parameters and portfolio stress testing;
- Trade financing/stock lending fees;
- Long-term custody costs;
- Hardware, such as telephones and computer terminals;
- Error correction services, capital introduction services, margin services or other services related to error correction;
- Office equipment, including furniture, supplies, telephone systems, salaries, rent, accounting fees and software, website design, email software, internet service, legal expenses, personnel management, marketing, utilities, membership dues, professional licensing fees, software to assist with the administrative functions (back-office functions, operating systems and word processing); or
- Operations overhead.

21.2.3 ACCEPTABLE INVESTMENT RESEARCH
In order for research to be accepted, it must constitute "specialized advice, analyses and reports that: 1. contain expressions of "reasoning" or "knowledge" by the author; and 2. be used by the Firm in its investment decision-making processes" (as opposed to its administrative or marketing functions.) Only those research products and services that constitute the following may be accepted:

- Traditional research reports analyzing a company or stock;
- Discussions with analysts and meetings with corporate executives to obtain reports on company financial data and economic data;
- Data services that provide market data, company financials and economic data;
- Financial newsletters and trade journals;
- Research related to the market for securities (such as pre-trade and post-trade analytics, software and other products that depend on market information to generate market research, research on optimal execution venues and trading strategies, and advice from broker on order execution, execution strategies, market color and the availability of buyers and sellers);

- Corporate governance research and rating services if used to make investment decisions;
- Market data reports, including stock quotes, last sale price reports, trading volume – whether or not the data has been analyzed or manipulated by the provider;
- Quantitative analytical software and software that provides analyses of the performance of securities portfolios (unless it is used exclusively for marketing purposes)(may be a mixed use product if used for both);
- Economic data such as unemployment reports, inflation rates or gross domestic product figures; and
- Tuition for seminars and conferences where the content satisfies the above requirements.

21.2.4 PRODUCTS AND SERVICES NOT CONSTITUTING "RESEARCH"
The following products and services should not be accepted by the Firm:

- Mass marketed publications (low cost publications that are intended for and marketed to a broad, public audience rather than intended to service the specialized interests of a small readership);
- Travel associated with attending conferences or seminars;
- Entertainment associated with attending conferences or seminars;
- Extravagant meals associated with attending conferences or seminars, occurring outside the hours of the seminar or conference; and
- Computer hardware and computer accessories.

21.3 DISCLOSURES TO CLIENTS
The Firm's research and brokerage services disclosures are contained in its Form ADV Part 2. The Chief Compliance Officer reviews these disclosures at least annually during the Form ADV update occurring during the first calendar quarter of each year. In addition, the disclosures are updated each time a new soft dollar arrangement is entered into that renders the current disclosures inadequate.

21.4 REVIEW OF EXISTING ARRANGEMENTS
On an annual basis the Chief Compliance Officer reviews the investment research, practice management and compliance advice, discounts and/or other services accepted by the Firm and determines the following:

- Does the product, service, compliance advice, discounts and/or other service accepted by the Firm remain within the guidelines outlined above?
- Is the product or service still desired?;
- Is there another product or service that would better meet the Firm's needs?
- Is the broker-dealer continuing to perform capably based on the Firm's best execution standards?

21.5 MAINTENANCE OF BOOKS AND RECORDS
The Chief Compliance Officer supervises the Firm's compliance with applicable soft dollar recordkeeping requirements. Records may be kept electronically in a non-rewritable format. The following records are kept by the Firm for at least 5 years from the end of the fiscal year in which they were last used and must be readily accessible to regulator examination:

- A list of all benefits and services accepted by the Firm by any client custodian or executing broker-dealer.

22.0 Succession And Transition Planning

22.1 POLICIES
In light of the Firm's fiduciary duties to its clients, it is Firm policy to properly prepare for a possible transition of Firm ownership precipitated by sudden loss of key personnel. The Firm principals have adopted the following procedures so that if the Firm must cease operations, it can do so in an orderly manner, with minimal impact on the confidentiality of client private information.

These procedures are reasonably designed to address operational and other risks related to a business transition or succession undertaken in response to a determination that the Firm is unable to continue providing investment advisory services due to an unexpected loss of key personnel, a merger with another advisor, a sale of the Firm to another advisor or a business failure resulting in bankruptcy. Because the Firm maintains important client private information, any transition of client relationships to a new advisory firm would need to be effected securely.

Because all client assets are held at qualified custodians and are segregated from the Firm's assets, transitioning accounts from the Firm to another advisor will follow a streamlined process that will not involve the physical movement or sale of assets, but rather a de-linking of the Firm's advisory authority by the client's custodian and a re-designation of advisory authority by the custodian to another, client-appointed advisor.

22.2 SUCCESSION PLAN
Adasina Social Capital, Inc., dba Adasina, is a California corporation with two shareholders: Rachel J. Robasciotti and Maya Philipson. The principals have entered into a buy-out agreement that covers the retirement, death or incapacity of either one of the principals. In the event of the retirement, death or incapacity of either principal, the remaining principal will be responsible for the management of the Firm. In the event of the simultaneous death or incapacity of both principals, the Chief Compliance Officer or designee(s) will be responsible for notifying estate attorney Deb L. Kinney, at Johnston, Kinney & Zulaica, 101 Montgomery Street, Suite 1600, San Francisco, 94104, 415-693-0550, deb@jkzllp.com and other legal or regulatory counsel as required.

22.3 TRANSITION PLANNING
Firm principals have no current intention to sell the Firm's advisory practice or to merge with another advisory firm. Any unexpected business failure will be treated in the same manner as described in the Firm's succession plan outlined above.

23.0 Record Maintenance and Retention

23.1 POLICIES
The Firm maintains all books and records required under the Investment Advisers Act. A copy of the SEC's Books and Records Rule is provided in the attached Forms. Generally, all of the Firm's securities transactions, portfolio reporting, billing and client relationship records are maintained electronically, backed up regularly or stored on a third-party Cloud storage service. In a few cases, hard copy records are also maintained. In some instances, records are maintained by a third-party service provider such as an executing broker-dealer, a client custodian, portfolio management system, a portfolio analytics software application or the Firm's electronic communications archiving service.

23.2 HARD COPY AND ELECTRONIC FORMATS
The Firm maintains minimal hard copy books and records and its predominantly electronic records at:
631 O'Farrell Street, Suite 1202, San Francisco, CA 94109. Maya Philipson, Chief Compliance Officer, or her designee, is responsible for the maintenance of these books and records. The Firm maintains the following document types and forms:

- Client Files & Client Services (Agreements and Contracts)

- Corporate Records and Archives
- Human Resources (Labor Notifications, Payroll and Employee Benefits)
- Infrastructure & Strategy (Accounting, Banking, Bookkeeping, Corporate Minutes, Finance, Legal Disclosures and Licenses, Operating Business Practices, Regulatory Filings, Tax Statements and Third-Party Service Providers)
- Marketing & Communications

Hard copy records are kept in locked filing cabinets; electronic copies are made of all paper records. Electronic records are stored and backed up in the Cloud. In the event that there is no internet connection, files can be accessed and used locally on individual computers. Once the internet connection is restored, these files can be synced to the Cloud.

23.3 RETENTION REQUIREMENTS
The Investment Advisers Act requires all Firm records to be maintained for five years past the end of the year in which the document was created or last relied upon. All records must be maintained in a readily accessible format, available for near immediate production to an SEC examiner.

The Chief Compliance Officer is responsible for conducting sufficient due diligence on all service providers to determine:

- The sufficiency of the service provider's security protocols
- The retention policies of the service provider and their consistency with SEC retention requirements
- The ability of the service provider to readily produce all records upon request.

Please refer to the Firm's Record Retention Checklist in the Forms section following.

23.4 SPECIAL REQUIREMENTS FOR PERFORMANCE DATA
For as long as the Firm disseminates performance results, it must maintain all accounts, books, internal working papers, and any other records or documents that are necessary to demonstrate the calculation of the performance or rate of return. With respect to the performance of managed accounts, the retention of all account statements, if they reflect all debits, credits, and other transactions in a client's account for the period of the statement, and all worksheets necessary to demonstrate the calculation of the performance or rate of return of all managed accounts shall be deemed to satisfy the requirements of this paragraph.

FORMS - ALPHABETICAL

1. Access Person Certification - Initial
2. Access Person Certification - Quarterly
3. Access Person Request for Trade Approval
4. Annual Best Execution Evaluation Checklist
5. Annual Compliance Program Review Checklist
6. Annual Senior Management Risk Assessment Checklist
7. Communications Review Compliance Checklist
8. Confidentiality Agreement With Third-Party Service Provider
9. Entertainment and Gift Log
10. IRA Rollover Procedure Checklist
11. Notice of Outside Business Activity and Request for Approval Form
12. Notice Of Participation In Private Securities Transaction And Request For Approval
13. Political Contribution Pre-Approval Form
14. Proxy Voting Conflict of Interest Determinations
15. Proxy Voting Information Request
16. Trade Error Report Template

ANCILLARY POLICIES AND PROCEDURES

1. Communications & Compliance Approval Process - Interdepartmental Procedures
2. Communications Review Request Process
3. Proxy Voting Guidelines

DEFINITIONS

Access Person. Regardless of Firm employment status (full time, part time, temporary, independent contractor, W-2 or 1099), all persons who have access to non-public client information and information regarding client securities transactions, persons who are involved in making securities recommendations to clients or have access to client recommendations and/or who are owners or control persons of the advisor.

Advertisement. Under SEC Rule 206(4)-1(b), An Advertisement is any direct or indirect communication an investment adviser makes that: (i) offers the investment adviser's investment advisory services with regard to securities to prospective clients or private fund investors, or (ii) offers new investment advisory services with regard to securities to current clients or private fund investors. The definition includes any endorsement or testimonial of any kind, including those for which an adviser provides cash and non-cash compensation directly or indirectly (e.g., paid solicitors, directed brokerage, awards or other prizes, and reduced advisory fees).[7]

Beneficial Interest. Any direct or indirect ownership, future ownership, control or authority interest in an investment account or security, including beneficiary, heir, trustee, executor, investment advisor or other status over trust accounts, estate assets, custodial accounts or other accounts in which the employee has an interest or exercises authority or investment discretion. For purposes of these policies, the term is considered to include securities held by members of an Access Person's Household Membershousehold members; provided however, this presumption may be rebutted.

Consumer. An individual or that individual's personal trust, estate or pension account and not an entity such as a partnership, corporation, limited liability company, limited partnership or other similar entity.

Covered Accounts. Accounts held by consumers: 1) that are offered primarily for personal, family or household purposes and involve multiple payments such as credit cards, margin accounts, checking or savings accounts; or 2) that involve a reasonably foreseeable risk from identity theft to consumers or to the security of the financial institution itself.

FACT Act / Red Flag Rules. The Red Flag Rules were adopted by the SEC in 2010, as amended, which was enacted and implemented to combat identity theft in connection with covered consumer accounts. The regulations require covered financial institutions to adopt an identity theft prevention program ("ITPP").

Financial Institution. A firm is a "financial institution" under the FACT Act and related Federal Trade Commission regulations if it provides, either directly or indirectly consumer transaction accounts that allow account holders to make withdrawals for payment or transfer of funds to third parties by telephone transfers, checks, debit cards or similar means.

Household Member. An Access Person's spouse, domestic partner, children, parents, siblings, other relatives and any other member of the person's immediate household, a trust or estate in which any member of his or her immediate household has a beneficial interest or over which the immediate household member has control.

[7] This definition excludes most one-on-one communications and contains certain other exclusions. Further, a written communication by an investment advisor that does no more than respond to an unsolicited request by a client, prospective client or consultant for specific information about the advisor's investment history, performance, past recommendations and the like, is not an "advertisement."

Household members include adopted and foster children, stepchildren, grandchildren, parents, stepparents, grandparents, siblings and in-laws.

Insider. Insiders are owners, officers, directors and employees of a company and the Firm's attorneys, accountants, consultants, bank lending officers, and the employees of such organizations.

Insider Trading. Insider trading is buying or selling securities by an "insider" while he or she is in possession of material non-public information; or trading by a non-insider while he or she is in possession of material non-public information, if the information either was disclosed to the non-insider in violation of an insider's duty to keep it confidential or was misappropriated; or communicating material non-public information to others in violation of one's duty to keep such information confidential

Non-public. Information is non-public until it has been effectively communicated to the marketplace and made available to the general public. Information found in filings with the Securities and Exchange Commission, or appearing in the *Dow Jones*, *Reuters Economic Services, the Wall Street Journal, Bloomberg Financial* or other publications of general circulation would be considered public.

Nonpublic Personal Information. Includes nonpublic "personally identifiable financial information" plus any list, description or grouping of customers that is derived from nonpublic personally identifiable financial information. Such information may include personal financial and account information, information relating to services performed for or transactions entered into on behalf of clients, advice provided by/to clients, and data or analyses derived from such nonpublic personal information.

Personal Information. An individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not secure and/or encrypted:

- Social security number;
- Driver's license number or California Identification Card number;
- Account number, credit or debit card number, in combination with any required security code, access code, or password to an individual's financial account;
- Medical information; and
- Health insurance information.

Regulation S-P. Requires investment advisors and the client services team(and other financial institutions) to adopt policies and procedures limiting the disclosure to third parties of non-public personal financial information about the advisor's clients and to safeguard such client information as collected by the advisor in the course of its advisory business.

Tipping. The act of communicating material non-public information to others or recommending a securities transaction to others while in possession of material non-public information about the security or the company in question.