CODE OF ETHICS

Background

Investment advisers are fiduciaries that owe their undivided loyalty to their clients. Investment advisers are trusted to represent clients' interests in many matters, and advisers must hold themselves to the highest standard of fairness in all such matters.

Rule 204A-1 under the Advisers Act requires each registered investment adviser to establish, maintain and enforce a written code of ethics that contains, at a minimum, provisions regarding:

1. A standard of business conduct required of supervised persons that reflects fiduciary obligations of the adviser and supervised persons;

2. Compliance with all applicable Federal Securities Laws;

3. Reporting and review of personal Securities transactions and holdings;

4. Reporting of violations of the code; and

5. Distribution of the code and any amendments to each supervised person and a written acknowledgment of their receipt.

Risks

In developing these policies and procedures, Maven considered the material risks associated with administering the *Code of Ethics*. This analysis includes risks such as:

- Employees do not understand the fiduciary duty that they, and Maven, owe to Clients;

- Employees and/or Maven fail to identify and comply with all applicable Federal Securities Laws;

- Employees do not report personal Securities transactions;

- Employees trade personal accounts ahead of Client accounts;

- Employees allocate profitable trades to personal accounts or unprofitable trades to Client accounts;

- Violations of the Federal Securities Laws, the *Code of Ethics*, or the policies and procedures set forth in this Manual, are not reported to the CCO and/or appropriate supervisory personnel;

- Maven does not provide its *Code of Ethics* and any amendments to all Employees; and

- Maven does not retain Employees' written acknowledgements that they received the *Code of Ethics* and any amendments.

Maven has established the following guidelines to mitigate these risks.

Policies and Procedures

Code of Conduct, Fiduciary Standards, and Compliance with the Federal Securities Laws

At all times, Maven and its Employees must comply with the spirit and the letter of the Federal Securities Laws and the rules governing the capital markets. The CCO administers the *Code of Ethics* (or the "*Code*"). All questions regarding the *Code* should be directed to the CCO. Employees must cooperate to the fullest extent reasonably requested by the CCO to enable (i) Maven to comply with all applicable Federal Securities Laws and (ii) the CCO to discharge his duties under the Manual.

All Employees will act with competence, dignity, integrity, and in an ethical manner, when dealing with Clients, the public, prospects, third-party service providers and fellow Employees. Employees must use reasonable care and exercise independent professional judgment when conducting investment analysis, making investment recommendations, trading, promoting Maven's services, and engaging in other professional activities.

Maven expects all Employees to adhere to the highest standards with respect to any potential conflicts of interest with Clients. As a fiduciary, Maven must act in its Clients' best interests. Notify the CCO promptly about any practice that creates, or gives the appearance of, a material conflict of interest.

Employees are generally expected to discuss any perceived risks, or concerns about Maven's business practices, with their direct supervisor. However, if an Employee is uncomfortable discussing an issue with their supervisor, or if they believe that an issue has not been appropriately addressed, they should bring the matter to the CCO's attention.

Reporting Violations

Improper actions by Maven or its Employees could have severe negative consequences for Maven, its Clients and Investors, and its Employees. Impropriety, or even the appearance of impropriety, could negatively impact all Employees, including people who had no involvement in the problematic activities.

Employees must promptly report any improper or suspicious activities, including any suspected violations of the *Code of Ethics* or the Federal Securities Laws to the CCO. Issues can be reported to the CCO in person, or by telephone, email, or written letter. Reports of potential issues may be made anonymously. Any reports of potential problems will be thoroughly investigated by the CCO, who will report directly to the Managing Partners on the matter. Any problems identified during the review will be addressed in ways that reflect Maven's fiduciary duty to its Clients.

An Employee's identification of a material compliance issue will be viewed favorably by the Company's senior executives. Retaliation against any Employee who reports a violation of the *Code of Ethics* in good faith is strictly prohibited and will be cause for corrective action, up to and including dismissal. If an Employee believes that he or she has been retaliated against, he or she should notify the Managing Partners directly.

Violations of this *Code of Ethics*, or the other policies and procedures set forth in the Manual, may warrant sanctions including, without limitation, requiring that personal trades be reversed, requiring the disgorgement of profits or gifts, issuing a letter of caution or warning, reporting to the Employee's supervisor, suspending personal trading rights, imposing a fine, suspending employment (with or without compensation), making a civil referral to the SEC, making a criminal referral, terminating employment for cause, and/or a combination of the foregoing. Violations may also subject an Employee to civil, regulatory or criminal sanctions. No Employee will determine whether he or she committed a violation of the *Code of*

Ethics, or impose any sanction against himself or herself. All sanctions and other actions taken will be in accordance with applicable employment laws and regulations.

For the avoidance of doubt, nothing in this Manual prohibits Employees from reporting potential violations of federal law or regulation to any governmental agency or entity, including but not limited to the Department of Justice, the SEC, or any agency's inspector general, or from making other disclosures that are protected under the whistleblower provisions of federal law or regulation. Employees do not need prior authorization from their supervisor, the Managing Partners, the CCO, or any other person or entity affiliated with Maven to make any such reports or disclosures and do not need to notify Maven that they have made such reports or disclosures. Additionally, nothing in this Manual prohibits Employees from recovering an award pursuant to a whistleblower program of a government agency or entity.

Distribution of the Code and Acknowledgement of Receipt

Maven will distribute this Manual, which contains the Company's *Code of Ethics*, to each Employee upon the commencement of employment, annually, and upon any change to the *Code of Ethics* or any material change to another portion of the Manual.

All Employees must use the Employee Compliance solution within ComplianceAlpha to acknowledge that they have received, read, understood, and agree to comply with the Company's policies and procedures described in this Manual, including this *Code of Ethics*.

Conflicts of Interest

Conflicts of interest may exist between various individuals and entities, including Maven, Employees, and current or prospective Clients and Investors. Any failure to identify or properly address a conflict can have severe negative repercussions for Maven, its Employees, and/or Clients and Investors. In some cases the improper handling of a conflict could result in litigation and/or disciplinary action.

Maven's policies and procedures have been designed to identify and properly disclose, mitigate, and/or eliminate applicable conflicts of interest. However, written policies and procedures cannot address every potential conflict, so Employees must use good judgment in identifying and responding appropriately to actual or apparent conflicts. Conflicts of interest that involve Maven and/or its Employees on one hand, and Clients and/or Investors on the other hand, will generally be fully disclosed and/or resolved in a way that favors the interests of Clients and/or Investors over the interests of Maven and its Employees. If an Employee believes that a conflict of interest has not been identified or appropriately addressed, that Employee should promptly bring the issue to the CCO's attention.

In some instances conflicts of interest may arise between Clients and/or Investors. Responding appropriately to these types of conflicts can be challenging, and may require robust disclosures if there is any appearance that one or more Clients or Investors have been unfairly disadvantaged. Employees should notify the CCO promptly if it appears that any actual or apparent conflict of interest between Clients and/or Investors has not been appropriately addressed.

It may sometimes be beneficial for Maven to be able to retroactively demonstrate that it carefully considered particular conflicts of interest.

Personal Securities Transactions

Employee trades should be executed in a manner consistent with our fiduciary obligations to our Clients: trades should avoid actual improprieties, as well as the appearance of impropriety. Employee trades must

not be timed to precede orders placed for any Client, nor should trading activity be so excessive as to conflict with the Employee's ability to fulfill daily job responsibilities.

Accounts Covered by the Policies and Procedures

Maven's *Personal Securities Transactions* policies and procedures apply to all accounts holding any Securities over which Employees have any beneficial ownership interest, which typically includes accounts held by immediate family members sharing the same household, or non-Clients over which Employees exercise investment discretion. Immediate family members include children, step-children, grandchildren, parents, step-parents, grandparents, spouses, domestic partners, siblings, parents-in-law, and children-in-law, as well as adoptive relationships that meet the above criteria. For purposes of this *Personal Securities Transactions* section, the term "Employee" includes: (1) any employee who has access to nonpublic information regarding any Client's trading or any Reportable Fund's holdings, who is involved in making securities recommendations to Clients, or who has access to nonpublic securities recommendations; (2) all of Maven's directors, officers, and partners; (3) any other person so designated by the CCO by notice to such person; and (4) any consultant, intern, or independent contractor hired or engaged by Maven that has access to Maven's nonpublic securities recommendations.

It may be possible for Employees to exclude accounts held personally or by immediate family members sharing the same household if the Employee does not have any direct or indirect influence or control over the accounts, or if the Employee can rebut the presumption of beneficial ownership over family members' accounts. Employees should consult with the CCO before excluding any accounts held by immediate family members sharing the same household.

Reportable Securities

Maven requires Employees to provide periodic reports regarding transactions and holdings in all "Reportable Securities," which include any Security, **except**:

- Direct obligations of the Government of the United States;
- Bankers' acceptances, bank certificates of deposit, commercial paper and high-quality short-term debt instruments, including repurchase agreements;
- Shares issued by money market funds;
- Shares issued by open-end investment companies registered under the Investment Company Act of 1940, other than investment companies advised or underwritten by Maven or an affiliate;
- Interests in 529 college savings plans; and
- Shares issued by unit investment trusts that are invested exclusively in one or more open-end investment companies registered under the Investment Company Act of 1940, none of which are advised or underwritten by Maven or an affiliate.

Exchange-traded funds, or ETFs and exchange traded notes, or ETNs, are somewhat similar to open-end registered investment companies. However, ETFs and ETNs are Reportable Securities and are subject to the reporting requirements contained in Maven's *Personal Securities Transactions* policy.

Any Employee who wishes to purchase, acquire or sell any asset that is issued and transferred using distributed ledger or blockchain technology, including, but not limited to, virtual currencies,

cryptocurrencies, digital "coins" or "tokens" ("Digital Assets"), should consult with the CCO as to whether such Digital Asset would be considered a Security, and specifically a "Digital Security", for purposes of this policy. A Digital Asset is likely to be considered a Digital Security if it is offered and sold as an investment contract. On April 3, 2019, the SEC published a framework for investment contract analysis of Digital Assets.[1] The CCO may use this framework, among other relevant SEC guidance, to determine whether a Digital Asset would be considered a Digital Security for the purposes of this policy. If the CCO determines that such Digital Asset should be considered a Digital Security, the Digital Asset will be considered a Reportable Security for purposes of this policy.

Pre-clearance Procedures

Employees must have written clearance for all transactions involving IPOs, Private Placements, or securities on the Restricted List (discussed below) before completing the transactions. Maven may disapprove any proposed transaction, particularly if the transaction appears to pose a conflict of interest or otherwise appears improper. If clearance is granted for a specified period of time, the Employee receiving the approval is responsible for ensuring that his or her trading is completed before the clearance's expiration. Employees should be cautious when submitting good-until-cancelled orders to avoid inadvertent violations of Maven's pre-clearance procedures.

Employees must use the Employee Compliance solution within ComplianceAlpha to seek pre-clearance.

Maven's investment management personnel will maintain a Restricted List of Securities that Maven is actively evaluating for purchase or sale in Client accounts, or about which Maven might have received Material Nonpublic Information. The CCO will not pre-clear any personal transactions in Securities that are associated with any issuers on the Restricted List.

Reporting

Maven must collect information regarding the personal trading activities and holdings of all Employees. Employees must submit quarterly reports regarding Securities transactions and newly opened accounts, as well as annual reports regarding holdings and existing accounts.

Quarterly Transaction Reports

Each quarter, Employees must report all Reportable Securities transactions in accounts in which they have a Beneficial Interest. Employees must also report any accounts opened during the quarter that hold any Securities (including Securities excluded from the definition of a Reportable Security). Reports regarding Securities transactions and newly opened accounts must be submitted to the CCO using the Employee Compliance solution within ComplianceAlpha, within 30 days of the end of each calendar quarter.

If an Employee did not have any transactions or account openings to report, this should be indicated through the Employee Compliance solution within ComplianceAlpha within 30 days of the end of each calendar quarter.

Initial and Annual Holdings Reports

Employees must periodically report the existence of any account that holds any Securities (including Securities excluded from the definition of a Reportable Security), as well as all Reportable Securities holdings. Reports regarding accounts and holdings must be submitted to the Employee Compliance solution

[1] https://www.sec.gov/files/dlt-framework.pdf

within ComplianceAlpha on or before February 14th of each year, and within 10 days of an individual first becoming an Employee. Annual reports must be current as of December 31st; initial reports must be current as of a date no more than 45 days prior to the date that the person became an Employee. Initial and annual holdings reports should be submitted through the Employee Compliance solution within ComplianceAlpha.

Initial and annual reports must disclose the existence of all accounts that hold any Securities, even if none of those Securities fall within the definition of a "Reportable Security."

If an Employee does not have any holdings and/or accounts to report, this should be indicated using the Employee Compliance solution within ComplianceAlpha within 10 days of becoming an Employee and by February 14th of each year.

Exceptions from Reporting Requirements

There are limited exceptions from certain reporting requirements. Specifically, an Employee is not required to submit:

- Quarterly reports for any transactions effected pursuant to an Automatic Investment Plan; or
- Any reports with respect to Securities held in accounts over which the Employee had no direct or indirect influence or control, such as an account managed by an investment adviser on a discretionary basis.

Any investment plans or accounts that may be eligible for either of these exceptions should be brought to the attention of the CCO who will, on a case-by-case basis, determine whether the plan or account qualifies for an exception. In making this determination, the CCO may ask for supporting documentation, such as a copy of the Automatic Investment Plan, a copy of the discretionary account management agreement and/or a written certification from the unaffiliated investment adviser, and may provide Employees with the exact wording and a clear definition of "no direct or indirect influence or control" that the adviser consistently applies to all Employees. On a sample basis, the CCO may request reports on holdings and/or transactions made in the trust or discretionary account to identify transactions that would have been prohibited pursuant to Maven's *Code*, absent reliance on the reporting exception. Employees who claim they have no direct or indirect influence or control over an account are also required to request an exception using the Employee Compliance solution within ComplianceAlpha upon commencement of their employment and on an annual basis thereafter.

Reliance on this independent or separately managed account exception is conditioned on approval of the request through the Employee Compliance solution within ComplianceAlpha and other satisfactory documentary evidence (e.g., copy of advisory agreement, certification from adviser, etc.) as directed by the CCO. Employees should consult with the CCO before excluding any accounts, especially those held by immediate family members sharing the same household.

Personal Trading and Holdings Reviews

Maven's *Personal Securities Transactions* policies and procedures are designed to mitigate any potential material conflicts of interest associated with Employees' personal trading activities. Accordingly, the CCO will closely monitor Employees' investment patterns to detect the following potentially abusive behavior:

- Frequent and/or short-term trades in any Security, with particular attention paid to potential market-timing of mutual funds;

- Trading opposite of Client trades;
- Trading ahead of Clients; and
- Trading that appears to be based on Material Nonpublic Information.

The CCO will review all reports submitted pursuant to the *Personal Securities Transactions* policies and procedures for potentially abusive behavior, and will compare Employee trading with Clients' trades as necessary. Upon review of the report, the Code of Ethics module will automatically record the date and time of the review, and the CCO or a designee will record any notes and/or identify any items of interest for resolution. Any personal trading that appears abusive may result in further inquiry by the CCO and/or sanctions, up to and including dismissal.

The Managing Partners will use the Employee Compliance solution within ComplianceAlpha monitor the CCO's personal Securities transactions for compliance with the *Personal Securities Transactions* policies and procedures.

Disclosure of the Code of Ethics

Maven will describe its *Code of Ethics* in Part 2 of Form ADV and, upon request, furnish Clients and Investors with a copy of the *Code of Ethics*. All Client requests for Maven's *Code of Ethics* should be directed to the CCO.

INSIDER TRADING

Background

Section 204A of the Advisers Act requires every investment adviser to establish, maintain, and enforce written policies and procedures reasonably designed, taking into consideration the nature of such investment adviser's business, to prevent the misuse of Material Nonpublic Information by such investment adviser or any associated person. In the past, the Federal Securities Laws have been interpreted to prohibit the following activities:

- Trading by an insider while in possession of Material Nonpublic Information;
- Trading by a non-insider while in possession of Material Nonpublic Information, where the information was disclosed to the non-insider in violation of an insider's duty to keep it confidential;
- Trading by a non-insider who obtained Material Nonpublic Information through unlawful means such as computer hacking; and
- Communicating Material Nonpublic Information to others in breach of a fiduciary duty.

What Information is Material?

Many types of information may be considered material, including, without limitation, advance knowledge of:

- Dividend or earnings announcements;
- Asset write-downs or write-offs;
- Additions to reserves for bad debts or contingent liabilities;
- Expansion or curtailment of company or major division operations;
- Merger, joint venture announcements;
- New product/service announcements;
- Discovery or research developments;
- Criminal, civil and government investigations and indictments;
- Pending labor disputes;
- Debt service or liquidity problems;
- Bankruptcy or insolvency;

- Tender offers and stock repurchase plans;
- Recapitalization plans; and
- Major developments in litigation or events that could lead to litigation (e.g., a cyber breach or a data leak).

Information provided by a company could be material because of its expected effect on a particular class of securities, all of a company's securities, the securities of another company, or the securities of several companies. The prohibition against misusing Material Nonpublic Information applies to a wide range of financial instruments including, but not limited to, equities, bonds, warrants, options, futures, forwards, swaps, commercial paper, government-issued securities, and Digital Securities. Material information need not relate to a company's business. For example, information about the contents of an upcoming newspaper column may affect the price of a security, and therefore be considered material. Advance notice of forthcoming secondary market transactions could also be material.

Employees should consult with the CCO if there is any question as to whether nonpublic information is material.

What Information is Nonpublic?

Once information has been effectively distributed to the investing public, it is no longer nonpublic. However, the distribution of Material Nonpublic Information must occur through commonly recognized channels for the classification to change. In addition, there must be adequate time for the public to receive and digest the information. Non-public information does not change to public information solely by selective dissemination. The confirmation by an insider of unconfirmed rumors, even if the information in question was reported as rumors in a public form, may be nonpublic information. Examples of the ways in which nonpublic information might be transmitted include, but are not limited to:

- In person;
- In writing;
- By telephone;
- During a presentation;
- By email, instant messaging, or Bloomberg messaging;
- By text message or through Twitter; or
- On a social networking site such as Facebook or LinkedIn.

Employees must be aware that even where there is no expectation of confidentiality, a person may become an insider upon receiving Material Nonpublic Information. Employees should consult with the CCO if there is any question as to whether material information is nonpublic.

Penalties for Trading on Material Nonpublic Information

Severe penalties exist for firms and individuals that engage in Insider Trading, including civil injunctions, disgorgement of profits and jail sentences. Further, fines for Insider Trading may be levied against individuals and companies in amounts up to three times the profit gained or loss avoided (and up to $1,000,000 for companies). Maven is not obligated to pay legal fees, penalties, or other costs incurred by Employees found guilty of insider trading.

Risks

In developing these policies and procedures, Maven considered the material risks associated with insider trading. This analysis includes risks such as:

- Employees place trades in personal and/or Client accounts based on Material Nonpublic Information;
- Employees pass Material Nonpublic Information on to others;
- Employees are not aware of what constitutes Material Nonpublic Information;

Maven has established the following guidelines to mitigate these risks.

Policies and Procedures

Employees are strictly forbidden from engaging in Insider Trading, either personally or on behalf of Maven's Clients. Maven's Insider Trading Policies and Procedures apply to all Employees, as well as any transactions in any securities by family members, trusts, or corporations, directly or indirectly controlled by such persons. The policy also applies to transactions by corporations in which the Employee is an officer, director, or 10% or greater stockholder, as well as transactions by partnerships of which the Employee is a partner unless the Employee has no direct or indirect control over the partnership.

Procedures for Recipients of Material Nonpublic Information

If an Employee has questions as to whether they are in possession of Material Nonpublic Information, they should inform the CCO as soon as possible. The CCO will conduct research to determine if the information is likely to be considered material, and whether the information has been publicly disseminated.

Given the severe penalties imposed on individuals and firms engaging in Insider Trading, an Employee:

- Must immediately report the potential receipt of Material Nonpublic Information to the CCO;
- Must not trade the securities of any company about which they may possess Material Nonpublic Information, or derivatives related to the issuer in question;
- Must not discuss any potentially Material Nonpublic Information with colleagues, except as specifically required by their position; and
- Must not conduct research, trading, or other investment activities regarding a security for which they may have Material Nonpublic Information until the CCO dictates an appropriate course of action.

If the CCO determines that the information is material and nonpublic, the CCO will prepare a written memorandum describing the information, its source, and the date that the information was received. The CCO may also maintain a list of these restricted securities (the "Restricted List"). Maven and its Employees will not place any trades in securities for which it has Material Nonpublic Information. Depending on the relevant facts and circumstances, the CCO may also take additional steps as appropriate

Trading in affected securities may resume, and other responses may be adjusted or eliminated, when the CCO determines that the information has become public and/or immaterial. At such time, the CCO will amend the memorandum noted above as well as the Restricted List, as applicable to indicate the date that trading was allowed to resume and the reason for the resumption.

Selective Disclosure

Non-public information about Maven's investment strategies, trading, and Client holdings may not be shared with third parties except as is necessary to implement investment decisions and conduct other legitimate business. Employees must never disclose proposed or pending trades or other sensitive information to any third party without the prior approval of the CCO. Federal Securities Laws may prohibit the dissemination of such information, and doing so may be considered a violation of the fiduciary duty that Maven owes to its Clients.

Relationships with Potential Insiders

Maven's Clients, Investors, third-party research providers, portfolio companies, and advisory board members may possess Material Nonpublic Information. Access to such information could come as a result of, among other things: being employed by an issuer (or sitting on the issuer's board of directors); working for an investment bank, consulting firm, supplier, or customer of an issuer; sitting on an issuer's creditors committee; or a personal relationships with connected individuals.

Individuals with access to Material Nonpublic Information may have an incentive to disclose the information to Maven due to the potential for personal gain. Employees should be extremely cautious about investment recommendations, or information about issuers, that it receives from Clients, Investors, third-party research providers, and advisory board members. Employees should inquire about the basis for any such recommendations or information, and should consult with the CCO if there is any appearance that the recommendations or information are based on Material Nonpublic Information.

Rumors

Creating or passing false rumors with the intent to manipulate securities prices or markets may violate the antifraud provisions of Federal Securities Laws. Such conduct is contradictory to Maven's *Code of Ethics*, as well as the Company's expectations regarding appropriate behavior of its Employees. Employees are prohibited from knowingly circulating false rumors or sensational information that might reasonably be expected to affect market conditions for one or more securities, sectors, or markets, or improperly influencing any person or entity.

This policy is not intended to discourage or prohibit appropriate communications between Employees of Maven and other market participants and trading counterparties. Employees should consult with the CCO regarding questions about the appropriateness of any communications.

Value Added Investors

The Private Funds may accept investments from so-called "value-added" investors. Although the term value-added investor is not defined in the Advisers Act or elsewhere, it is generally understood to refer to an investor who may provide some benefit to the adviser (such as industry expertise or access to individuals in the investor's network) beyond just the value of their investment. Examples of such investors could include, without limitation, executive-level officers or directors of a company or personnel that are affiliated with other investment advisers and/or private funds.

Due to the nature of their position, such investors may possess Material Nonpublic Information. Therefore, Employees should always remain alert to the possibility that they could inadvertently come into possession of Material Nonpublic Information when communicating with such Investors. Employees should refrain from discussing potentially sensitive topics (e.g., specific information about the investor's employer) with a known value-added investor.

If there is any question as to whether information received from an Investor could be Material Nonpublic Information, Employees are expected to notify the CCO immediately, and otherwise to act in accordance with the procedures described above.

ANTI-MONEY LAUNDERING

Background

The USA PATRIOT Act does not currently require anti-money laundering ("AML") policies or procedures for registered investment advisors or private funds. Nonetheless, many advisers implement AML policies and procedures because of the potential consequences of becoming associated with money laundering. Additionally, investment advisers that are affiliated with other financial institutions or offshore private funds may be subject to AML statutes because of those affiliations.

AML policies and procedures typically involve:

- Designating an individual to oversee the policies and procedures;
- Implementing internal controls designed to detect and prevent money laundering;
- Conducting periodic testing to ensure that the internal controls are functioning as intended; and
- Conducting periodic training to help Employees identify suspicious activities and respond appropriately.

Risks

In developing these policies and procedures, Maven considered numerous risks associated with money laundering. This analysis includes risks such as:

- Law enforcement officers suspect that a Client or Investor is engaged in illegal money laundering activities, resulting in significant disruptions to Maven's operations;
- Clients or Investors maintain accounts with shell banks or foreign financial institutions that lack strong AML policies and procedures;
- Maven accepts Clients or Investors that are identified by the Treasury Department's OFAC list as being involved in terrorism or other illegal activities;
- Maven invests Client assets in companies that engage in money laundering or other illegal activities, causing law enforcement officers to question whether Maven or its Clients are financing such activities; and
- Maven lacks AML policies and procedures.

Maven has established the following guidelines as an attempt to mitigate these risks.

Policies and Procedures

Maven intends to comply with the spirit of certain provisions of the USA PATRIOT Act regarding the prevention of money laundering, as described below.

Investor Reviews

Maven will require all Investors in the Private Funds to affirmatively make certain representations in a subscription agreement or similar document. Maven will also check Investor names against applicable regulatory watch lists at the time of initial investment and upon any approved transfer of a Private Fund interest. To the extent that there is a match or possible match between the Investor and the regulatory watch lists, Maven will document this and may consult with legal counsel or outside compliance consultants to determine whether any regulatory filings need to be made or other steps need to be taken.

Contacts from Regulatory Authorities

Any communications from regulatory authorities regarding suspected money laundering or other potentially illegal activities must immediately be reported to the CCO. The CCO will coordinate Maven's response to the communication and will involve Outside Counsel as necessary.

Suspicious Activities and Arrangements

Employees should report any activities or arrangements that appear suspicious or indicative of money laundering to the CCO, even if the account in question is held in custody by a reputable bank or broker-dealer.

The CCO, with the assistance of Outside Counsel, will determine whether Maven should report potentially suspicious activity to the Treasury Department's Financial Crimes Enforcement Network.

Controls Instituted by Third Parties

Accounts under Maven's management are typically held in custody by reputable banks and broker-dealers that have instituted their own robust customer identification and AML policies and procedures. Before commencing management of an account at a new bank or broker-dealer, the CCO may request a summary of the bank or broker-dealer's customer identification and AML procedures. If these procedures appear reasonable to the CCO, then Maven will not take additional AML steps unless an Employee identifies suspicious activities or arrangements.

Portfolio Management

Maven will seek to avoid investing in companies that engage in money laundering, terrorist financing, or other illegal activities in order to avoid the appearance that Maven supports or is financing such activities. Maven's investment professionals must take reasonable steps to evaluate the risk that the issuer of a security is participating in money laundering, terrorist financing, or other illegal activities. Investment professionals should consult with the CCO if they perceive a material risk in connection with any current or prospective investment.

CUSTODY AND SAFEGUARDING OF CLIENT ASSETS

Background

Definition of Custody

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

- Actual possession of client funds or securities;
- Any arrangement (including a general power of attorney) under which an adviser is authorized or permitted to withdraw client funds or securities upon instruction to a custodian;[4]
- Any capacity (such as general partner of a limited partnership, a comparable position for another type of pooled investment vehicle, or a trustee of a trust) that gives an adviser or any supervised person legal ownership of, or access to, client funds or securities; and
- Custody by a related person in connection with advisory services provided to the adviser's clients.

General Requirements for Advisers with Custody

An investment adviser with custody of client funds or securities must implement certain procedures to safeguard those assets. The requirements imposed by the Custody Rule generally apply only to those funds or securities over which an adviser has custody, rather than all of the funds or securities under the adviser's management. The Custody Rule generally requires an adviser with custody to:

- Provide information in Part 1A of Form ADV about its custodial arrangements;
- Maintain the clients' funds and securities at a Qualified Custodian in the clients' names, or in the adviser's name as agent or trustee for the clients;
- Upon opening or changing an account on behalf of a client, notify the client in writing of the account's custodian, the custodian's address, and the manner in which the client's funds or securities are maintained;[5]

[4] In some cases, the terms of an agreement between a client and qualified custodian might permit the client's adviser to instruct the custodian to disburse, or transfer, funds or securities.

[5] An adviser that is required to provide written notices about account openings or changes made on behalf of clients, and that separately sends its own account statements to the affected clients, must include language in the adviser's written notice and subsequent account statements urging the affected clients to compare the adviser's statements to those issued by the custodian.

- Have a reasonable basis, after "due inquiry,"[6] to believe that the Qualified Custodian sends account statements to clients at least quarterly;[7] and

- Arrange for an independent public accountant to conduct a surprise verification of funds and securities at least annually, unless an exception is available.

Privately Offered Pooled Investment Vehicles

An investment adviser to a privately offered pooled investment vehicle that is audited by an independent public accountant need not:

- Notify clients or investors about changes to the vehicle's custodial arrangements;

- Ensure that a Qualified Custodian is sending account statements to the investors; or

- Arrange for an independent surprise verification of the vehicle's funds and securities.

However, these exceptions to the Custody Rule's requirements are only available if:

- The independent public accountant is registered with, and subject to regular inspection by, the PCAOB;

- The audits are conducted annually in accordance with generally accepted auditing standards, and the audit reports are issued in accordance with generally accepted accounting principles;

- The audited financial statements are distributed to all investors within 120 days of the vehicle's fiscal year end;[8] and

- The vehicle is audited upon liquidation, and the audit is distributed to all investors promptly after its completion.

If an investment adviser establishes or controls a special purpose vehicle ("SPV") for certain investments of private funds it advises, the adviser must either treat the SPV as a separate client for purposes of complying with the Custody Rule or include the SPV's assets as part of the applicable fund's audits. If the SPV is deemed to be a Client of Maven and it has owners other than Maven, its Private Funds, or its related persons, Maven must treat the SPV as a separate Client for purposes of the Custody Rule.

Privately Offered Securities

The Custody Rule states that securities need not be held by a Qualified Custodian if they are:

---

[6] The SEC has not prescribed a specific method for conducting "due inquiry." However, the Commission indicated that receiving and, on a sample basis, testing the integrity of the addresses on duplicate statements received from a custodian would be considered due inquiry. Conversely, the Commission indicated that simply accessing account statements on a custodian's website would not be considered due inquiry.

[7] Account statements for a privately offered pooled investment vehicle must be delivered to the vehicle's underlying investors unless the vehicle is audited and the audits are distributed to investors in accordance with paragraph (b)(4) of the Custody Rule.

[8] A fund of funds, which is defined as a pooled investment vehicle that invests 10% or more of its assets in unaffiliated pooled investment vehicles, may distribute its audited financial statements within 180 days of its fiscal year end. A fund of funds of funds may distribute its audited financial statements within 260 days.

- Acquired from the issuer in a transaction not involving any public offering;

- Uncertificated and ownership thereof is recorded only on books of the issuer or its transfer agent in the name of the client; and

- Transferable only with prior consent of the issuer or holders of the issuer's outstanding securities.

Although securities that meet the preceding criteria need not be held by a Qualified Custodian, they can nonetheless trigger the Custody Rule's independent surprise verification provisions if an adviser is deemed to have custody of the securities. Also, privately offered pooled investment vehicles that hold privately offered securities must be audited, as described above, in order to rely on this exception.

In August 2013 the SEC's Division of Investment Management extended the Custody Rule's exception for privately offered securities to include certificated securities as long as all of the following conditions are met:

- The client must be a pooled investment vehicle subject to audits as described in the Custody Rule;

- The security must be transferrable only with prior consent of the issuer or holders of the issuer's outstanding securities, and the private stock certificate must contain a legend restricting transfer;

- Ownership of the security must be recorded on the books of the issuer or its transfer agent in the name of the client; and

- The private stock certificate must be appropriately safeguarded by the adviser, and must be able to be replaced upon loss or destruction.

Independent Surprise Verifications

If an adviser is deemed to have custody of client funds or securities, and is unable to rely on the exceptions described above, then the adviser must arrange for an independent public accountant to conduct a surprise verification of the funds and securities over which the adviser has custody. The verification must be conducted at least once during each calendar year at a time that is irregular from year to year, and that is chosen by the accountant without prior notice to the adviser. The independent surprise verification must also be conducted pursuant to a written agreement between the adviser and the accountant that includes specific provisions regarding filings that the accountant will make with the SEC.[9]

Books and Records Requirements

A registered investment adviser with custody of client funds or securities must maintain certain books and records, as described in the *Maintenance of Books and Records* section of this Manual.

Account Statements Sent to an Independent Representative

A client, or an investor in a pooled investment vehicle, may designate an independent representative to receive notices and statements on the client or investor's behalf. Any such independent representative must

[9] The particular provisions that must be included in the written agreement between the adviser and the accountant are described in paragraph (a)(4) of the Custody Rule.

not be affiliated with the adviser, and must not have had a material business relationship with the adviser during the past two years.

Inadvertent Receipt of Client Funds or Securities

An adviser will not be deemed to have custody solely because it inadvertently receives client funds or securities, so long as the adviser returns the funds or securities to the sender promptly, but in any case within three business days of receipt. In an SEC staff letter issued to the Investment Adviser Association on September 20, 2007, the Division of Investment Management noted that it would not recommend enforcement action against an adviser that has inadvertently received client funds or securities despite its use of reasonable best efforts to direct third parties to deliver client funds or securities to its clients or Qualified Custodians, and that has promptly forwarded such client funds or securities to the appropriate client or Qualified Custodian, rather than to certain senders.[10] For example, a class action settlement inadvertently delivered to an adviser could be forwarded to the appropriate client or Qualified Custodian, rather than being returned to the settlement administrator. An investment adviser relying on this SEC staff letter must adopt and implement policies and procedures to:

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

Also, an adviser will not be deemed to have custody of client funds or securities because of its inadvertent receipt of a check made out to a Qualified Custodian or other unaffiliated third party. Nonetheless, an adviser should promptly forward any checks made out to third parties to the appropriate recipient.

Risks

In developing these policies and procedures, Maven considered numerous risks associated with the Custody Rule and the protection of Client assets. This analysis includes risks such as:

- Client assets are lost or misappropriated;
- Maven is deemed to have custody of Client funds or securities, but the Company and/or its Employees are unaware of the associated compliance obligations imposed by the Custody Rule; and

[10] The SEC staff notably limited the relief to the following three specific circumstances: (1) when the Internal Revenue Service or a state or other governmental tax authority sends client tax refunds to the adviser; (2) when administrators of funds established to distribute the settlement proceeds of class action lawsuits or other legal actions send client settlement assets to the adviser (including fair funds distributions); and (3) when the adviser receives stock certificates or dividend checks in the name of their client, including in connection with certain class action lawsuits involving bankruptcy or as a result of business reorganizations.

- Maven lacks internal controls that are reasonably designed to prevent and detect any loss or misappropriation of Client assets.

Maven has established the following guidelines to mitigate these risks.

Policies and Procedures

Custody by Maven and Qualified Custodians

Maven is deemed to have custody of the Private Funds' assets because of the authority that Maven and its affiliated entities have over those assets. The CCO is responsible for overseeing the audits of the Private Funds and any associated special purpose vehicles, as well as the distribution of the audited financial statements to all Investors within 120 days of the Private Funds' fiscal year ends.

If Maven establishes or controls an SPV for certain investments of a Private Fund, it will make a determination with Outside Counsel whether it needs to either i) treat the SPV as a separate client for purposes of complying with the Custody Rule or ii) include the SPV's assets as part of the applicable Private Fund's audits.

Maven will maintain Client cash and securities at unaffiliated Qualified Custodians.

Maven may have physical custody of, or access to, certain privately offered stock certificates. Should this occur, the CCO will ensure that these certificates meet the exemption discussed above.

Inadvertent Receipt of Client Funds or Securities

If any Employee inadvertently receives Client funds or securities, such as a stock certificate or a check incorrectly made out to Maven, the Employee must deliver the assets to the Controller who will notify the Managing Partners and the CCO by the close of business. The CCO will promptly, but in any case within three business days, send the funds or securities to the Client, the Client's Qualified Custodian, or the sender, as appropriate to most effectively protect Client funds or securities. The CCO may void out checks incorrectly made out to Maven prior to returning them to the sender. The CCO will instruct the sender that any future deliveries of Client funds or securities should be made directly to the Client or to the Client's Qualified Custodian. The CCO will use a log or similar documentation to document the receipt and forwarding or return of any such assets.

Private Fund Capital Controls

Maven maintains a *Cash and Related Accounting Policies* document as well as an *Accounts Payable Memo*. These documents contain controls to ensure that Client assets are sufficiently protected.

PRIVACY PROTECTION AND CYBER SECURITY

Background

Privacy Protection

Regulation S-P ("Reg S-P") requires registered investment advisers to adopt and implement policies and procedures that are reasonably designed to protect the confidentiality of nonpublic personal records. Reg S-P applies to "consumer" records, meaning records regarding individuals, families, or households. Reg S-P does not explicitly apply to the records of companies, investors in a private fund, or individuals acting in a business capacity, but corresponding Federal Trade Commission ("FTC") rules may impose similar disclosure and safeguarding obligations. Maven is committed to protecting the confidentiality of all nonpublic information regarding its Clients, Investors, prospects, and Employees ("Nonpublic Personal Information").

Privacy Notices

Reg S-P requires investment advisers to provide their customers with certain notices describing their privacy policies and procedures ("Privacy Notice"). Among other requirements, Reg S-P requires financial institutions to send initial Privacy Notices to "consumers" and provide both customers and consumers the opportunity to opt out of the disclosure of any Nonpublic Personal Information about a consumer to a nonaffiliated third-party. The Fixing America's Surface Transportation Act (the "FAST Act") clarifies investment advisers' obligations with regard to Reg S-P. Under the FAST Act, investment advisers are not required to send annual Privacy Notices to "customers" if the adviser (i) only shares Nonpublic Personal Information with nonaffiliated third-parties in a manner that does not require an opt-out right be provided to customers; and (ii) has not changed its policies and procedures with regard to disclosing Nonpublic Personal Information since it last provided a Privacy Notice to customers. For purposes of Maven's privacy policies and procedures, "consumers" are potential and current Clients and Investors and "customers" are current Clients and Investors.

Although Reg S-P does not require the distribution of Privacy Notices to companies, to investors in a private fund, or to individuals acting in a business capacity, the Company provides initial Privacy Notices, revised Privacy Notices, and, when appropriate, annual Privacy Notices to all Clients and Investors as a best practice.

Information Sharing with Affiliates

Regulation S-AM ("Reg S-AM") prohibits a registered investment adviser from using information about an individual consumer that has been obtained from an affiliated entity for marketing purposes unless the information sharing practices have been disclosed and the consumer has not opted out.

Cyber Security

The staff of the SEC is concerned by the risk of cyber-attacks against registered investment advisers because of the potential for direct harm against advisers' clients, as well as potential disruptions to market stability that could be intentional or incidental results of a cyber-attack.

State Privacy Requirements

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

Risks

In developing these policies and procedures, Maven considered the material risks associated with privacy protection and the prevention of identity theft. This analysis included risks such as:

- Nonpublic Personal Information is not recorded accurately or protected from inadvertent alteration or destruction;
- Nonpublic Personal Information is not protected from unauthorized access by Employees or third-party service providers;
- Nonpublic Personal Information can be accessed, copied, or destroyed by physical or electronic intrusions;
- False or misleading disclosures are made to Clients or Investors about the use or protection of Nonpublic Personal Information;
- Third-party service providers have adopted inadequate policies and procedures to protect Nonpublic Personal Information;
- Maven fails to comply with applicable state privacy laws;

Maven has established the following guidelines to mitigate these risks.

Policies and Procedures

Guiding Principles

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

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

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

Protecting Confidential Information

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

Nonpublic Personal Information will be restricted to Employees who have a need to know such information.

All requests by third-parties to review this Manual, compliance testing results, correspondence between Maven and regulators and other compliance-related documents should be forwarded to the CCO. Employees are not authorized to respond to such requests without the prior approval of the CCO.

Disclosure of Nonpublic Personal Information

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

- To accountants, lawyers, and others as directed in writing by Clients or Investors;
- To specified family members as directed in writing by Clients or Investors, or as authorized by law;
- To third-party service providers, as necessary to service Client or Investor accounts, assess Maven's compliance with industry standards, protect the confidentiality and security of Maven's records, and protect against or prevent actual or potential fraud, unauthorized transactions, claims, or other liability; and
- To regulators and others, as required by law.

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

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

Nonpublic Personal Information may be reviewed by Maven's outside service providers, such as accountants, lawyers, consultants, and administrators. Maven will review such service providers' privacy policies to ensure that Nonpublic Personal Information is not used or distributed inappropriately.

Access to Maven's Premises

Maven's premises will be locked outside of normal business hours. Meetings with Investors or other third parties should be held in conference rooms or other locations where Nonpublic Personal Information is not available or audible to others. Visitors will not be left in Maven's office unattended.

Information Stored in Hard Copy Formats

Generally, Maven does not maintain hard copy documents with Nonpublic Personal Information. In the event there are hard copy documents with such information, Maven has implemented the following procedures to protect Nonpublic Personal Information stored in hard copy formats:

- To the extent practicable, Nonpublic Personal Information will be kept in lockable filing cabinets or other secure locations;
- Documents containing Nonpublic Personal Information must never be left unattended in public spaces, such as lobbies or conference rooms;
- Employees will exercise due caution when mailing or faxing documents containing Nonpublic Personal Information to ensure that the documents are sent to the intended recipients; and
- Employees may only remove documents containing Nonpublic Personal Information from Maven's premises for legitimate business purposes. Any documents taken off premises must be handled with appropriate care and returned as soon as practicable.

Cyber-Security Practices for All Employees

Maven has implemented the following procedures to protect proprietary and Nonpublic Personal Information stored on electronic systems:

- Employees must never share their passwords or store passwords in a place that is accessible to others;
- Employees should avoid using the same password for different applications or websites;
- Employees should not use the same password for Company accounts as for non-Company accounts;
- Multi-factor authentication is best practice, and where MFA is not feasible, passwords should be changed periodically;
- Employees must shut down or lock their computers when they leave the office for any extended period of time;
- Employees must not include Nonpublic Personal Information in unencrypted emails sent outside of Maven's network;
- Any computers not issued by the Company that Employees use for business purposes must be configured to comply with Maven's information security policies;
- Any theft or loss of electronic storage media or equipment/devices containing Company data must immediately be reported to the CCO; and
- Employees must consult with the CCO before using any removable or mobile media to store sensitive Maven data, including Nonpublic Personal Information;

Cyber-Security Controls Implemented by Information Technology Professionals

The CCO oversees the development and implementation of Maven's cyber-security controls, with assistance from hiTech, Ingalls Information Security, and KnowBe4, Inc.

On at least an annual basis, the CCO and/or Maven's information technology provider will seek to conduct a cyber-security risk assessment. Additionally, on an annual basis, Maven's information technology service providers will seek to report to the CCO that Maven has:

- Inventoried its computers, system hardware, and other IT devices such as smart phones;
- Monitored for unauthorized devices accessing Maven's networks;
- Inventoried its software applications, and ensured that software patches are being applied in a timely manner;
- Evaluated likely types of attack, including through penetration testing and vulnerability scans, where appropriate;
- Implemented appropriate protections, such as anti-malware software, firewalls and data loss prevention software;
- Provided cybersecurity training to all Maven staff on at least an annual basis;
- Conducted mock phishing tests and phishing training to all employees;
- Tested Maven's ability to restore critical systems, data and software in a timely manner;
- Implemented standardized secure configurations for user hardware, software, operating systems, and network infrastructure;
- Periodically tested to confirm that hardware, software, operating systems and network infrastructure continue to operate according to their standardized secure configurations;
- Appropriately tested software applications prior to implementation;
- Encrypted any wireless data transmissions in Maven's offices that could contain sensitive data, as well as hardware and mobile devices that contain sensitive data;
- Mapped its network resources, and ensured that Maven has appropriately limited access to drives and applications that host sensitive data;
- Mapped personally identifiable information and implemented tools to detect, prevent, and monitor data loss;
- Mapped external access points to Maven's network;
- Evaluated the cyber-security programs of vendors or other third parties that have independent access to Maven's networks or proprietary data, and, where appropriate, ensured that third party contracts or statements of work include appropriate provisions governing cyber-security;

- Implemented adequate access logging capabilities, as well as automated exception reporting capabilities that are reasonably designed to detect malicious activity or unauthorized access to sensitive data or systems;
- Tested the functioning of Maven's access logging and exception reporting systems;
- Required relatively strong user passwords that must be changed from time to time;
- Encrypted all laptops and portable storage devices containing Nonpublic Personal Information;
- Allowed only a select few administrators to assign "domain administrator" privileges to accounts on the system;
- Restricted administrative and privileged access to systems and data;
- Used preventative and detective controls to prevent unauthorized access or alteration of systems and/or data;
- Assigned unique user IDs;
- Documented any change in access for a specific user and had such changes approved by the appropriate person;
- Monitored and logged remote access sessions;
- Used multi-factor authentication and encryption to secure remote access communications;
- Applied multi-factor authentication requirements to customers with online access;
- Restricted the ability of Employees to connect removable and mobile media to Company systems;
- Used multi-factor authentication and encrypted the transmission and storage of authenticators;
- Updated anti-virus and web security software;
- Secured access to the operating system and all system components;
- Used automatic software patching and update tools for all systems and applications;
- Backed up systems and data at least monthly using cloud or physical backup systems;
- Secured configurations for network devices, such as firewalls, routers, and switches;
- Used email and web browser protection tools such as web filtering and SPAM/phishing email filtering; and
- Promptly disabled access for any terminated Employees.

Working in Public Places

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

Discarding Information

Employees may only discard or destroy Nonpublic Personal Information in accordance with the *Document Destruction* policy contained in the *Maintenance of Books and Records* portion of this Manual. Employees are reminded that electronic and hard copy media containing Nonpublic Personal Information must be destroyed or permanently erased before being discarded.

Privacy Policy Notices

Maven will provide a Privacy Notice to all Clients and Investors upon establishment of an advisory relationship or investment in a Private Fund. A copy of Maven's *Privacy Notice* is attached.

Maven will provide Investors with prompt notice of any change to the Company's privacy policies, and will give Investors sufficient opportunity to opt out of any new disclosure provisions. On an annual basis, the CCO will review the Company's privacy policies and confirm that the Company (i) only shares Nonpublic Personal Information with nonaffiliated third-parties in a manner that does not require an opt-out right be provided to Investors; and (ii) has not changed its privacy policies with regard to disclosing Nonpublic Personal Information since it last provided a Privacy Notice to the Company's Investors. If the Company cannot confirm the aforementioned two conditions, Maven will provide a copy of the Privacy Notice to all Investors describing the Company's privacy policies. The CCO will retain a copy of the Privacy Notice sent and will make and retain a record of its distribution.

Information Obtained from, or Provided to, Affiliates

Maven does not use information about individuals that was obtained from affiliated entities for any marketing purposes. Maven does not provide information about individuals to affiliate entities for any marketing purposes.

Responding to Privacy Breaches

Maven maintains a *Cyber Risk Policy*, maintained separate from this Manual, that functions as the Company's incident response plan. In the event of a cyber incident or breach, Employees should follow the policies and procedures outlined in the *Cyber Risk Policy,* which is maintained with the assistance of Maven's IT provider, hiTech.

Privacy Protection Training

The CCO will ensure that all new Employees have received, reviewed, and understand their obligations to protect Nonpublic Personal Information. The CCO will also periodically remind all Employees of their privacy protection obligations. If the privacy protection program appears to be functioning well and has not undergone material changes, then this reminder might appropriately take the form of a broadly-distributed annual email. The CCO may provide training more frequently and/or in person to individuals or groups if:

- Maven's policies and procedures, or the threats to Nonpublic Personal Information, change in a material way;
- Maven experiences a privacy breach; and/or
- One or more Employees do not appear to understand their obligations regarding privacy protection.

Privacy Notice

FACTS	**WHAT DOES MAVEN ROYALTY PARTNERS, LLC ("Maven") DO WITH YOUR PERSONAL INFORMATION?**
WHY?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
WHAT?	The types of personal information we collect and share depend on the product or service you have with us. This information can include: ▪ Social security number ▪ Income ▪ Assets ▪ Risk tolerance ▪ Wire transfer / ACH instructions ▪ Transaction history When you are no longer our customer, we continue to share information about you as described in this notice.
HOW?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Maven chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	**Does Maven Share?**	**Can you limit this sharing?**
For our everyday business purposes - such as to process your transactions, maintain your accounts(s) or respond to court orders and legal investigations.	Yes	No
For our marketing purposes - to offer our products and services to you	Yes	No
For joint marketing with other financial companies	No	We don't share
For our affiliates' everyday business purposes - information about your transactions and experiences	No	We don't share
For our affiliates' everyday business purposes – information about your creditworthiness	No	We don't share
For nonaffiliates to market to you	No	We don't share

Questions?	Visit: https://www.mavenroyalty.com/

Page 2	
Who we are	
Who is providing this notice?	Maven Royalty Management LLC and Maven Royalty Partners
What we do	
How does Maven protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings.
How does Maven collect my personal information?	We collect your personal information, for example, when you complete a subscription document for our funds, and when you are receiving a distribution from such funds.
Why can't I limit all sharing?	Federal law gives you the right to limit only ▪ sharing for affiliates' everyday business purposes - information about your creditworthiness ▪ affiliates from using your information to market to you ▪ sharing for nonaffiliates to market to you State laws and individual companies may give you additional rights to limit sharing.
Definitions	
Affiliates	Companies related by common ownership or control. They can be financial and nonfinancial companies. ▪ *Maven does not share with our affiliates*
Nonaffiliates	Companies not related by common ownership or control. They can be financial and nonfinancial companies. ▪ *Maven does not share with nonaffiliates so they can market to you*
Joint Marketing	A formal agreement between nonaffiliated financial companies that together market financial products or services to you. ▪ *Maven does not jointly market.*
Other important information	
N/A	