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

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;
- 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 PC-Net Consulting, LLC, 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, PC-Net Consulting, LLC.

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	