RIMROCK
CAPITAL MANAGEMENT, LLC

PRIVACY NOTICE

Maintaining the confidentiality and security of your personal financial information is very important to us at Rimrock Capital Management, LLC ("Rimrock").

INFORMATION WE COLLECT. To provide you with superior service, we may collect several types of nonpublic personal information about you, including:

- Information from forms you fill out and send to us in connection with your investment in one of our Funds (such as your name, address, and social security number).
- Information you give us verbally.
- Information you submit to us in correspondence, including emails.
- Information about the amounts you have invested in our Funds (such as your initial investment and any additions to and withdrawals from your capital account).
- Information about any bank account you use for transfers between your bank account and your capital account in any of our Funds, including information provided when effecting wire transfers.

INFORMATION WE SHARE. We do not sell your personal information and we do not disclose it to anyone except as permitted or required by law. For example, we may share information we collect about you with our independent auditors in the course of the annual audit of the Fund in which you have an investment. We may share this information with our legal counsel as we deem appropriate and with regulators. Additionally, we may disclose information about you at your request (for example, by sending duplicate account statements to someone you designate), or as otherwise permitted or required by law.

INFORMATION SECURITY. Within Rimrock, access to information about you is restricted to those employees who need to know the information to service your account. Rimrock employees are trained to follow our procedures to protect your privacy and are instructed to access information about you only when they have a business reason to obtain it.

CHANGES TO OUR PRIVACY POLICY. We reserve the right to change our privacy policy in the future, but we will not disclose your nonpublic personal information as required or permitted by law without giving you an opportunity to instruct us not to.

QUESTIONS. For questions about our privacy policy, or additional copies of this notice, please call us at (949) 381-7800 or ir@rimrockcapital.com.

PRIVACY NOTICE FOR DATA SUBJECTS WHOSE PERSONAL INFORMATION MAY BE COLLECTED IN THE EUROPEAN UNION:

EU GENERAL DATA PROTECTION REGULATION ("GDPR"). With regard to personal information collected in the European Economic Area (EEA), Rimrock lacks an office in any EEA country and offers investment management products and services only to institutional investors in the EEA. However, through its investor subscription forms, websites, emails, and other communications with investors, Rimrock collects and stores personal information on officers, employees, and representatives of entity investors.

Because Rimrock has no established office in the EEA, it must potentially deal with local supervisory authorities in all E.U. states where it has business. In addition, information that we collect may be transferred outside of the EEA, including to countries, such as the United States and the Cayman Islands, which have not been deemed as having "adequate" security measures by the European Commission. Therefore, we have executed or intend to execute Model Clauses in our contracts, pursuant to European Commission Decision 2010/87/EC, to facilitate the legitimate, secure transfer of personal information outside the EEA as necessary.

CAYMAN ISLANDS DATA PROTECTION ACT, 2021 ("DPA"). By virtue of investing in a Cayman Islands Fund and your associated interactions with us, you will provide us (including by submitting subscription documents, tax forms, and associated documents and in correspondence and discussions with us) certain information that constitutes "personal data" under the DPA.

PERSONAL INFORMATION. Personal information that may be collected by us from data subjects in the EEA, and information that constitutes "personal data" under the DPA, includes, without limitation:

- Name
- Address
- Phone Number
- Email Address
- Names of Beneficial Owners
- Tax ID Number
- Place of Birth or Incorporation
- Whether an Investor is an "Accredited Investor" and "Qualified Purchaser"
- Contact Information for Individuals Receiving Duplicate Reports and "Interested Parties."

LAWFUL GROUNDS TO PROCESS AND OBTAIN CONSENT. As a regulated financial services entity, Rimrock is required to collect, review, and store private information about investors, clients, and their representatives. Based on our obligations and business needs, we may collect information for a variety of reasons, including, but not limited to, the following:

- Determining whether a prospective investor is eligible to invest in the Fund under applicable law;
- Determining the identity and beneficial ownership of investors and clients to comply with requirements seeking to prevent money laundering, tax evasion, terrorism and violation of foreign sanctions, and identity theft;
- Determining the persons authorized to act on behalf of an investor or client who can give instructions to Rimrock.
- Determining whether an investor or client is subject to specific investment regulations related to a specific type of person or organization (e.g., ERISA plans, governmental entities);
- Communicating with clients and investors about their existing and prospective investments or accounts.

Data subjects whose data is collected in the EEA or whose data is subject to the DPA may withdraw consent at any time where consent is the lawful basis for processing his/her information. However, if a data subject withdraws consent for processing or otherwise objects to processing that impedes Rimrock's ability to comply with applicable regulations, a data subject may be unable to avail him/herself of the services that Rimrock provides.

Rimrock keeps the above-referenced client and investor information for as long as its relationship with the client or investor continues and for a minimum of five years after termination.

DATA SUBJECTS' RIGHTS. All individuals whose personal information is held by Rimrock have the right to:

- Ask what information Rimrock holds about them and why;
- Ask for a copy of such information or access to such information;
- Be informed on how to correct or keep that information up to date;
- Be informed on how Rimrock is meeting its data protection obligations.

Furthermore, for data collected in the EEA, or data which is subject to the DPA, data subjects have the right to:

- Ask for a copy of such information to be sent to a third party;
- Ask for data to be erased if possible and required under the GDPR or the DPA, as applicable;
- Ask for processing of personal information to be restricted if possible and required under GDPR or the DPA, as applicable;
- Object to processing of personal information if possible and required under GDPR or the DPA, as applicable;
- Object to automated decision-making where applicable;
- Contact a supervisory authority in the EEA or the Cayman Islands to lodge a complaint regarding Rimrock's processing of your data.

RESPONSIBILITY. Rimrock's Chief Compliance Officer (the "CCO") is also Rimrock's Data Protection Officer, responsible for reviewing, maintaining, and enforcing these policies and procedures to ensure meeting Rimrock's client privacy goals and objectives while at a minimum ensuring compliance with applicable federal, state, and foreign laws and regulations. The CCO reports directly to Rimrock's Principals and the Board of Directors of the Funds. The CCO is also responsible for distributing these policies and procedures to employees and conducting appropriate employee training to ensure employee adherence to these policies and procedures.

All Supervised Persons are responsible for helping to ensure that investor and client private information is collected, used, stored, and handled in accordance with Rimrock policy.

PROCEDURE. Rimrock has adopted these various procedures, applicable to its business practice and those of its affiliates, including each Fund's general partner or directors. These procedures are designed to (1) ensure the confidentiality of customer records and information, (2) protect against any anticipated threats or hazards to the security of customer records and information, and (3) protect against unauthorized access or use of customer records or information that could result in substantial hardship or inconvenience to any consumer.

NON-DISCLOSURE OF INFORMATION. Rimrock and its affiliates maintain safeguards to comply with federal and state standards to guard each client's and investor's nonpublic personal information. The Firm does not share any nonpublic personal information with any nonaffiliated third parties, except in the following circumstances:

- As necessary to provide the service that the client or investor (by virtue of subscribing to the Fund's interests) has requested or authorized, or to maintain and service the client's or investor's account;
- As required by regulatory authorities or law enforcement officials who have jurisdiction over Rimrock and its affiliates or as otherwise required by any applicable law; and
- To the extent reasonably necessary to prevent fraud and unauthorized transactions.

Employees are prohibited, either during or after the termination of their employment, from disclosing nonpublic personal information to any person or entity outside Rimrock, including family members, except under the circumstances described above. An employee is permitted to disclose nonpublic personal information only to other employees who need to have access to such information to deliver our services to the client or investor.

SECURITY AND DISPOSAL OF INFORMATION. Rimrock restricts access to nonpublic personal information to those employees who need to know such information to provide services to our clients or investors. Any employee who is authorized to have access to nonpublic personal information is required to keep such information in a secure compartment or receptacle daily as of the close of business each day.

All electronic or computer files containing such information shall be secured and protected from access by unauthorized persons. Any conversations involving nonpublic personal information, if appropriate at all, must be conducted by employees in private, and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations. Electronic and paper records used for business purposes must not be left in places where they are visible to unauthorized persons. Data printouts and files must be disposed of securely when no longer needed.

Safeguarding standards encompass all aspects of Rimrock's business that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures. Important safeguarding standards the Firm has adopted include:

- Access controls on information systems, including controls to authenticate and permit access only to Supervised Persons and procedural controls to prevent employees from providing client/investor information to unauthorized individuals who may seek to obtain this information through fraudulent means (e.g., requiring employee use of user ID numbers and passwords, etc.);
- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals (e.g., key card entry system);
- Encryption of electronic customer information, including while in transit or in storage on networks or systems to which unauthorized individuals may have access;
- Monitoring systems and procedures to detect actual and attempted attacks on or intrusions into customer information systems (e.g., data should be auditable for detection of loss and accidental and intentional manipulation);
- Policy to respond as appropriate when the Firm suspects or detects that unauthorized individuals have gained access to customer information systems, including, as appropriate, notifying applicable regulatory and law enforcement agencies;
- Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards, such as fire and water damage or technological failures (e.g., use of fire-resistant storage facilities and vaults; backup and store off-site key data to ensure proper recovery); and
- Information systems security should incorporate the security of physical facilities and personnel, the use of commercial or in-house services (such as networking services), and contingency planning.

RIMROCK CONTACT INFORMATION FOR PERSONS LOCATED WITHIN THE EEA.

If you are located in the European Economic Area ("EEA") or Switzerland and have questions or concerns regarding the processing of your personal information, you may contact our EU Representative at:

Rimrockcapital@sallbergco.se

Or write to us at:

Attn: Sällberg & Co
Bankgatan 1A, 223 52 Lund, Sweden

CONTACT INFORMATION FOR THE CAYMAN ISLANDS OMBUDSMAN

Under the DPA, you have the right to complain to the Cayman Islands Ombudsman, who may be contacted by email (info@ombudsman.ky), telephone (+1 345 946 6283), or post (PO Box 2252, Grand Cayman KY1-1107, Cayman Islands).