NOTICE OF PRIVACY POLICY

We consider privacy to be fundamental to our relationship with our investors. We are committed to maintaining the confidentiality, integrity and security of our current and former investors' non-public information. Accordingly, we have developed internal policies to protect confidentiality while allowing investors' needs to be met.

We respect your right to privacy. We also know, however, that you expect us to conduct our investment program in an accurate and efficient manner. To do so, we must collect and maintain certain non-public information about you and our other investors. We collect this information from sources such as subscription agreements and other documents.

We will not disclose any non-public personal information about investors who are individuals, except to our affiliates and service providers as allowed by applicable law or regulation. In the normal course of serving our investors, information we collect may be shared with companies that perform various services such as our accountants, auditors, attorneys, broker-dealers and fund administrator.

Any party that receives this information must agree to use it only for the services required and as allowed by applicable law or regulation and is not permitted to share or use this information for any other purpose. To protect the personal information of individuals, we permit access only by authorized employees who need access to that information to provide services to us and our investors. In order to guard investors' non-public personal information, we maintain physical, electronic and procedural safeguards that comply with U.S. federal standards. An individual investor's right to privacy extends to all forms of contact with us, including telephone, written correspondence and electronic media, such as the Internet.

We note, however, that notwithstanding the foregoing, we reserve the right to disclose non-public personal information about investors to any person or entity, including without limitation any governmental agency, regulatory authority or self- regulatory organization having jurisdiction over us or our affiliates, if (i) we determine in our discretion that such disclosure is necessary or advisable pursuant to or in connection with any United States federal, state or local, or non U.S., law, rule, regulation, executive order or policy, including without limitation any anti-money laundering law and the USA PATRIOT Act of 2001 and (ii) such disclosure is not otherwise prohibited by law, rule, regulation, executive order or policy.

Regulation S-P

Regulation S-P is a set of privacy rules that govern the treatment of customer information about consumers of certain financial institutions.

Under Regulation S-P, the Firm is required to properly maintain and protect the customer information that it collects from any individual who becomes a client or investor of the Firm.

This customer information includes but is not limited to:

- Taxpayer ID number (e.g., Social Security number);
- Other National, State/provincial identification number (e.g., driver's license number, passport number);
- Financial account numbers;
- Personal contact details (e.g., home address, telephone number, mobile number);
- Date of birth;
- Income; and
- Assets (including assets under management at the Firm).

The Firm maintains policies and procedures reasonably designed to safeguard the security and confidentiality of customer information and prevent against unauthorized access or use.

The Firm has identified all customer information that it retains internally including the data which may be received from other financial institutions. The Firm has controls in place to physically and electronically safeguard such customer information and to dispose or delete of such data, when required.

All customer information held by the Firm will be kept confidential and only disclosed to non-affiliated third parties as set out in the Firm's privacy notice.

The Firm will maintain documentation evidencing compliance with Regulation S-P safeguards and disposal rules.

Incident Response

Regulation S-P requires that the Firm maintain an incident response plan including, but not limited to, the below key components:

- Assessment of the nature and scope of any data breach;
- Containment and control of the incident to prevent further unauthorized access; and
- Notice to affected individuals.

The Firm has a written incident response program that details procedures related to the detection, response, and recovery from unauthorized use or access of customer information.

Privacy Notice

A privacy notice describing the Firm's policies must be provided to each individual investor prior to entering into an advisory contract with the Firm.

The Firm's privacy notice must be clear and conspicuous and include, among other things:

- Categories of customer information collected;
- Categories of information the Firm shares and with whom; and
- The Firm's policies and procedures for protecting the confidentiality and security of the information.

If changes are made to the policies and procedures through which the Firm safeguards or discloses customer information, the Chief Compliance Officer will ensure an updated privacy notice is delivered to all individual investors.

Safeguarding Customer Information

Regan restricts access to customer information to those who need to know such information for the performance of their roles within the Firm. All employees with which the Firm shares such information are required to keep such customer information confidential.

The Firm may share customer information:

- With service providers of the Firm such as administrators, auditors, and attorneys;
- With affiliated entities (e.g. general partners) that assist the Firm in the running of its day- to-day business;
- To respond to a request from regulators or law enforcement;
- To protect against fraud and unauthorized transactions; and
- If provided consent by the investor to share for other purposes.

No employee is permitted to share customer information outside the scope of what is required to properly perform their duties at the Firm.

At a minimum, the Firm will maintain the below safeguards.

Administrative Safeguards:

- Comply with this policy and other applicable Firm policies, e.g. Incident Response Plan, Cybersecurity Policy and Business Continuity Plan;
- Assign and maintain appropriate access rights and reasonable controls on applications, databases, shared drives, and other systems containing customer information; and
- Consider privacy and data protection issues during due diligence of third party service providers.

Physical Safeguards:

- Require all visitors to sign into the building at the security desk;
- Limit office access to employees who have electronic access cards, authorized building personnel, and approved guests;
- Lock or log off computers when unattended for any extended period of time;
- Lock file cabinets and desks holding Firm confidential information;
- Shred hard copy confidential information after use;
- Avoid discussions referencing confidential information in public spaces; and
- Report any loss or theft of mobile devices and laptops to the Chief Compliance Officer immediately.

Technical Safeguards:

- Adhere to applicable IT risk policies and standards, regarding the use of passwords, removable storage devices and other security measures;
- Remain vigilant in monitoring for suspicious emails, attachments and websites; and
- Access Firm network remotely only by approved means.

Employees are to contact the Chief Compliance Officer immediately should it be suspected that confidential Firm or customer information has been or may be lost, stolen, accessed, destroyed, modified or disclosed in

an unauthorized manner.

At least annually, the Chief Compliance Officer provides training on various policies that assist in the protection of individual customer information.

Regan Capital will keep records of:

(i) written policies and procedures about compliance with Regulation S-P, including the incident response program;

(ii) written policies, procedures, or contracts with service providers adopted under or applicable to requirements of this rule;

(iii) incidents, investigations, related determinations, and subsequent notification processes, including procedures designed to revisit notification determinations where appropriate in light of new facts or developments and Attorney General requests for delays in notice.

Where applicable, the CCO will promptly notify Boards, Trust Officers or General Partners of any of the funds or vehicles under its management of any incidents relating to this policy, when practicable.

Customer Information Breach Notifications

Where sensitive customer information has been or is reasonably likely to have been used or accessed without authorization, the Firm is required to make a notification to the affected individuals. Sensitive customer information is any component of customer information (alone or in conjunction with any other information), the compromise of which could create a reasonably likely risk of substantial harm or inconvenience to an individual identified with the information. Examples include social security numbers, passport or identification numbers, address amongst other identifying information.

The notification will be made in writing and provided to the affected individuals as soon as possible, and no later than 30 days, after the Firm became aware of the unauthorized use or access.

At a minimum, the breach notification will provide:

- Detail about the incident, including the date or estimated date of the data breach (or date range if applicable);
- Information on the breached data;
- How affected individuals can respond to the breach to protect themselves; and
- Contact information for an individual at the Firm who affected individuals can contact for further information.

The Firm will maintain records of investigations undertaken, including our basis for determining whether a notification was required to be made.

Third Party Service Providers

The Firm is required to establish, maintain and enforce policies and procedures reasonably designed to oversee and monitor service provider relationships. A service provider is defined as "any person or entity (including affiliates of a covered institution) that receives, maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to a covered institution," such as the Firm. An appropriate level of due diligence is required to be completed prior to engaging a service provider that will have access to customer information and the Firm will perform ongoing monitoring and review.

Service providers must inform the Firm as soon as possible, but no later than 72 hours after becoming aware of a security breach involving customer information systems. On notification the Firm will initiate its incident response program.

The Firm is ultimately responsible for ensuring that a data breach notification is made to any affected individual but may enter into a written agreement with a service provider to delegate such notification.

The Firm will review to ensure that any notifications are delivered within the required timeframe.

Disposal of Data

Documents and information not required to be maintained under the Advisers Act may be deleted or destroyed. Prior to disposing of any document that may be considered a book or record of the Firm, employees should consult with the Chief Compliance Officer. Employees may never destroy documentation or any information that is a part of a pending legal or regulatory matter.

The destruction of records containing customer information or other confidential information must be conducted in a manner so that others will not be able to retrieve such data. The Firm will shred paper documents or utilize a service such as Iron Mountain for destruction. Electronic records will be permanently deleted or erased.

Getting In Touch

Should you have any queries or wish to discuss your data protection rights with us, please contact Regan's COO; Sujit Sahadevan at +1 (214) 550-1714 or IR@regancapital.com.