PRIVACY POLICY AND PROCEDURES

Introduction

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. Although Reg S-P does not explicitly apply to the records of companies, investors in a Private Fund, or individuals acting in a business capacity, the Firm is committed to protecting the confidentiality of all information of all Investors and prospects ("**Nonpublic Personal Information**").

Reg S-P requires registered investment advisers to provide its natural person Investors with notices describing the Firm's privacy policies and procedures. These privacy notices must be delivered to all new natural person Investors upon inception of a subscription, and at least annually thereafter. Reg S-P does not require the distribution of privacy notices to companies or to individuals representing legal entities.

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.

In addition to Reg S-P, certain states have adopted consumer privacy laws that may be applicable to investment advisers with natural person Investors who are residents of those states.

Policies and Procedures

Guiding Principles

The Firm will seek to limit its collection of Nonpublic Personal Information to that which is reasonably necessary for legitimate business purposes. The Firm 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 Investor to whom the information pertains, including authorizations contained in subscription materials. The Firm will never sell Nonpublic Personal Information.

With respect to Nonpublic Personal Information, the Firm 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 Firm recognizes the threat posed by cyber-attacks. Accordingly, the Firm's investment technology team and outside service providers seek to protect such information and the Firm from such incidents in accordance with the Firm's Cybersecurity Policy attached as Appendix 9.2.7 to the Compliance Manual.

The Chief Compliance Officer is responsible for administering these policies and procedures. LL Ultra Team Members are required to notify the Chief Compliance Officer 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, LL Ultra Team Members must be careful to protect all of the Firm's proprietary and confidential information.

Non-Public Personal Information includes all personally identifiable financial information about a current or former Supervised Person, Client or Investor that is not publicly available, including, but not limited to:

- Social security number, tax ID number, etc.;

- Driver's license number;
- State-issue identification card number;
- Financial account number such as a bank or brokerage account number;
- Name, address and contact details;
- Age, employment and marital status;
- Financial information such as assets or income; and
- Information related to a Fund Investor's capital account, such as profit and loss allocations and capital additions or withdrawals.

Protecting Confidential Information

LL Ultra Team Members will maintain the confidentiality of information acquired in connection with their employment, with particular care being taken regarding Nonpublic Personal Information. Improper use of the Firm'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.

The overall security standards that must be upheld are:

- Seek to ensure the security and confidentiality of Nonpublic Information;
- Protect against any anticipated threats or hazards to the security or integrity of Fund Investor and Fund Client records and information; and
- Protect against unauthorized access to or use Nonpublic Personal Information.

All requests by third-parties to review this Compliance Manual, compliance testing results, correspondence between the Firm and regulators and other compliance-related documents should be forwarded to the Chief Compliance Officer. LL Ultra Team Members are not authorized to respond to such requests without the prior approval of the Chief Compliance Officer.

Disclosure of Nonpublic Personal Information

Nonpublic Personal Information may be disclosed:

- to the extent the Privacy Notice procedures (described below) have been complied with and the clients and Fund Investors, as applicable, have not opted out of disclosure;
- to the extent necessary to administer or effect a transaction that the client or Fund Investor has requested or authorized, including as necessary to facilitate investment in a Fund Client;
- to service providers or joint marketers who agree to limit their use of such information;
- with the consent or at the direction of the Fund Client or the Fund investor;
- to protect the confidentiality or security of a client or Fund Investor's records;

- for required institutional risk control or for resolving client/investor disputes or inquiries;
- to persons holding a legal or beneficial interest relating to the client or Fund Investor;
- to persons acting in a fiduciary or representative capacity on behalf of the client or Fund Investor;
- to accountants, lawyers, and others as directed or authorized by the Fund Client or Fund Investors; and
- to the extent required or specifically permitted by law or regulation or reasonably necessary to prevent fraud, unauthorized transactions or liability.

Nonpublic Personal Information may be reviewed by outside service providers, such as accountants, lawyers, consultants, and administrators. To the extent both reasonably feasible and applicable, the Firm will review third party service providers' privacy policies to ensure that Nonpublic Personal Information is not used or distributed inappropriately.

LL Ultra Team Members should take reasonable precautions to confirm the identity of individuals requesting Nonpublic Personal Information. LL Ultra Team Members 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 LL Ultra Team Member to divulge additional information. Any contacts with suspected identity thieves must be reported promptly to the Chief Compliance Officer.

To the extent practicable, LL Ultra Team Members 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.

Information Obtained from or Provided to Affiliates

The Firm does not use information about individuals that was obtained from affiliates for any marketing purposes. In addition, the Firm does not provide information about individuals to affiliates for any marketing purposes.

Access to the Firm's Premises

The Firm's premises will be locked outside of normal business hours.

From time to time, the Firm may share office space with other individuals and business (including other investment advisers) (each, "**Co-Tenant**"). In addition to the other privacy policies and procedures set forth in this Compliance Manual, the Firm has adopted the following policies and procedures to ensure the privacy protection of records and information relating to clients and Fund Investors.

- The Co-Tenants will be physically segregated from the Firm.
- All records, information and documents relating to Fund Clients and Fund Investors that are available in hard copy shall be stored in secured file cabinets that are accessible only by the Firm's Supervised Persons.
- From time to time Co-Tenants may share a server with the Firm. However, all records, information and documents relating to Fund Clients and Fund Investors that are available in electronic copy shall be stored on a secured server and shall be accessible only by the Firm's Supervised Persons except in limited circumstances as described below.

Information Stored in Hard Copy Formats

Nonpublic Personal Information stored in hard copy formats should be kept in lockable filing cabinets, that are locked at the end of each workday, and must never be left unattended in public spaces.

LL Ultra Team Members may only remove documents containing Nonpublic Personal Information from the Firm's premises for legitimate business purposes. Any documents taken off premises must be handled with appropriate care and returned as soon as practicable. LL Ultra Team Members will exercise due caution when mailing or faxing documents containing Nonpublic Personal Information to ensure that the documents are sent to the intended recipients.

Electronic Information Systems

Policies regarding electronic information systems can be found in the Firm's Cybersecurity Policy attached as Appendix 9.2.7 to this Compliance Manual.

Discarding Information

LL Ultra Team Members may only discard or destroy Nonpublic Personal Information in accordance with the Document Destruction policy contained in the Books and Records portion of this Manual.

LL Ultra Team Members are reminded that electronic and hard copy media containing Nonpublic Personal Information must be destroyed or permanently erased before being discarded.

Privacy Policy Notices

The Firm will provide a Privacy Notice to all Clients at the onset of a new relationship and to Fund Investors upon investment in a Fund Client. The Firm will also provide a copy of the Privacy Notice to all Clients and Fund Investors annually in the event of a material change. The Chief Compliance Officer oversees the distribution of both the initial and annual Privacy Notices (if required), which will be mailed or emailed as required. The Chief Compliance Officer will maintain a record of the dates and recipients of Privacy Notices.

Responding to Privacy Breaches

If any LL Ultra Team Member becomes aware of an actual or suspected privacy breach, including any improper disclosure of Nonpublic Personal Information, or a "**breach of security**", that LL Ultra Team Member must promptly notify the Chief Compliance Officer. For purposes of these procedures, "breach of security" means the unauthorized acquisition or unauthorized use of unencrypted data or, encrypted electronic data and the confidential process or key that is capable of compromising the security, confidentiality, or integrity of Nonpublic Personal Information, maintained by a person or agency that creates a substantial risk of identity theft or fraud. A good faith but unauthorized acquisition of Nonpublic Personal Information by a person or agency, or employee or agent thereof, for the lawful purposes of such person or agency, is not a breach of security unless the Nonpublic Personal Information is used in an unauthorized manner or subject to further unauthorized disclosure.

Upon becoming aware of an actual or suspected breach, the Chief Compliance Officer will investigate the situation and take appropriate action(s). For example, if the breach involves a breach of security systems and other data housing Nonpublic Personal Information (including Personal Information), the Chief Compliance Officer will take the following steps in connection with a breach of security of computer systems and other data medium housing personal information:

- assess the breach of security, including ascertaining the data stolen or otherwise lost;
- attempt to retrieve stolen and/or lost data;

- take immediate action to cure the breach of security;
- investigate the cause of the breach;
- set up a post-security breach incident review;
- based on the findings contained in the post-incident review, develop and implement procedures or protocols designed to prevent similar future breaches of data;
- take the appropriate disciplinary actions with respect to Supervised Persons involved in the incident; and
- document all actions taken in response to the breach.