Cercano Management LLC

Privacy Policy

CERCANO MANAGEMENT

CERCANO MANAGEMENT LLC
PRIVACY POLICY

Adopted as of January 1, 2022

A. General

Cercano Management LLC ("**Cercano**" or the "**Firm**"), its member, and their respective managers, directors, officers, and employees (each, a "**Supervised Person**" and collectively, "**Supervised Persons**") have adopted these policies and procedures ("**Privacy Policy**") to provide and identify administrative, technical and physical safeguards that establish standards for maintaining the security and confidentiality of nonpublic information ("**NPI**") collected from Cercano's clients (each, an "**Advisory Client**" and collectively, "**Advisory Clients**") and investors in private funds managed by Cercano or its affiliates (each, an "**Investor**" and collectively, "**Investors**") to protect against anticipated threats or hazards to the security or integrity of NPI, to protect against unauthorized access to or use of NPI in a manner that creates a substantial risk of identity theft or fraud, and to dispose of NPI in a secure manner. Cercano's regulatory responsibility to protect NPI is mandated by, among others, SEC Regulation S-P and CFTC Regulation 160 (the "**Privacy Rules**").

The Chief Compliance Officer ("**CCO**") or the designee of the CCO is responsible for overseeing this Privacy Policy and may consult with outside counsel and/or compliance consultants, as necessary.

The Firm will not disclose NPI of any current or former Advisory Clients or Investors to third parties other than to the Firm's affiliates, brokers, administrators, accounting support firms, compliance/operational support services providers, and other third-party firms that assist the Firm in providing advisory services or effecting client transactions.

NPI includes, but is not limited to, nonpublic personally identifiable financial information plus any list, description or grouping of Advisory Clients or Investors that is derived from nonpublic personally identifiable financial information. NPI may also include, without limitation, personal financial and account information, such as: names, addresses, contact details, or information that identifies a person as an Advisory Client or Investor; social security numbers or tax identification numbers; assets, net worth, income, or other information provided on a financial product application; bank account information; consumer report information; occupation; information acquired through an Internet "cookie"; or other information regarding Advisory Clients or Investors not available to the public. NPI also may include advice provided by the Firm to Advisory Clients, and data or analyses derived from NPI.

Certain states and foreign jurisdictions have adopted additional consumer privacy laws that may be applicable to investment advisers with clients who are residents of those states or countries. These include but are not limited to California and Massachusetts. To ensure compliance with state and non-US privacy laws, the CCO will, in consultation with outside counsel and external compliance consultants as he or she deems necessary or appropriate, periodically review state and foreign laws and determine whether the Firm's policies and procedures are adequate in light of those reviews. To the extent required, Cercano will revise its Privacy Policy in order to comply with those laws.

B. Privacy Notice

The Firm's Privacy Notice incudes a description of the types of NPI the Firm collects, a description of the manner in which the Firm collects such information, an explanation of the conditions under which the Firm may disclose NPI to third parties, and the Firm's policies and procedures for the protection and security of confidential information. The Privacy Notice is provided to new individual customers and on an annual basis thereafter.

C. Procedures for Compliance with Privacy Policy

So as to generally confirm that NPI from Advisory Clients and Investors is safeguarded, the Firm has adopted the following internal procedures:

1. The CCO or a designee will inventory all systems on which the Firm maintains NPI, as well as who has access to those systems;

2. Access to NPI will be restricted to Supervised Persons and service providers that need to access such information to engage in business activities on behalf of Cercano, and access rights will be terminated promptly if the Supervised Person or service provider no longer requires such access;

3. Supervised Persons are prohibited from storing NPI on their personal devices (e.g., personal desktop computers, laptops, tablets, smartphones);

4. Supervised Persons are prohibited from sending NPI to unsecured locations outside of the Firm's networks;

5. Files containing NPI will generally not be maintained in physical, hard copy form;

6. Cercano has established electronic systems protocols as discussed below; and

7. NPI is securely disposed of as set forth below.

D. Data Security

Cercano seeks to establish and maintain a security system that covers the use of the internet, its servers, its computers and other IT equipment (such as desktop computers, laptops, tablets and smartphones). In this regard, Cercano has adopted the following internal procedures:

1. Cercano's electronic systems are protected by security software, which software may include firewalls, anti-virus, anti-spam, malware and trojan protection, as well as reasonably up-to-date software patches and security 'definition' updates;

2. Access to systems will be limited to only active users and active user accounts only and access will be blocked to any user identification after multiple unsuccessful attempts to gain access or the limitation placed on access for the particular system;

3. Secure user authentication protocols (including control of user IDs and control of data security passwords) are implemented on all Cercano IT equipment;

4. All Cercano laptops' hard drives are encrypted;

5. All Cercano smartphones may be remotely wiped from the exchange server if any such equipment is lost or stolen; and

6. If Cercano IT equipment (including desktop computers, laptops, tablets, and smartphones) is lost or stolen, Supervised Persons are directed to immediately contact the CCO or the System Administrator, who shall render the data on such IT equipment unreadable.

E. Disposal of Nonpublic Personal Information

In order to protect Advisory Clients and Investors against the risks of fraud and fraud-related crimes, including identity theft, the Firm has also adopted the following internal procedures relating to the secured disposal of NPI:

1. To the extent not covered under Rule 204-2 under the Investment Advisers Act of 1940, as amended (the "**Advisers Act**"), hard copies of Advisory Clients' NPI (or any extra hard copies of Advisory Clients' NPI, whether or not covered by Advisers Act Rule 204-2) shall be destroyed in a manner so that the information cannot be practicably read or reconstructed;

2. To the extent not covered under Advisers Act Rule 204-2, Advisory Clients' NPI that is stored on disk, CD, tape or other electronic media (or any extra disks, CDs, tapes or other electronic media which contains advisory clients' NPI, whether or not covered by Advisers Act Rule 204-2) is required to be cleared, purged, declassified, overwritten and/or encrypted in such a manner so that any information contained therein cannot be restored or decrypted;

3. After the electronic media containing NPI is cleared, purged, declassified, overwritten or encrypted, the System Administrator is required to check that the original information is not backed-up or saved on a hard drive, recycle bin or other memories; and

4. If a Supervised Person has any doubt as to whether certain data constitutes NPI, that Supervised Person must consult with the CCO or outside counsel or dispose of the data in question as if it were, in fact, NPI.