



PRIVACY NOTICE

Overview

Evergreen Advisors, LLC's primary client goal is to protect your privacy.

To conduct regular business, we may collect nonpublic personal information from sources such as:

- Information reported by you on applications or other forms you provide to us

As the Firm shares nonpublic information solely to service our client accounts, we do not disclose any nonpublic personal information about our customers or former customers to anyone, except as permitted by law.

- Information the firm receives from clients on applications (name, social security number, address, assets, etc.)

At times, we may disclose nonpublic personal information to affiliated third parties. We may share any of the information that we collect as described above. We may disclose nonpublic personal information about you to the following types of affiliated third parties:

- Financial service providers such as mortgage brokers, insurance companies, or broker dealers

Evergreen Advisors, LLC will internally safeguard your nonpublic personal information by restricting access to only those employees who provide products or services to you or those who need access to your information to service your account. In addition, we will maintain physical, electronic and procedural safeguards that meet federal and/or state standards to guard your nonpublic personal information.

Policy

As a registered investment adviser, Evergreen Advisors, LLC must comply with SEC Regulation S-P (or other applicable regulations), which requires registered advisers to adopt policies and procedures to protect the "nonpublic personal information" of natural person consumers and customers and to disclose to such persons policies and procedures for protecting that information. Nonpublic personal information includes nonpublic "personally identifiable financial information" plus any list, description or grouping of customers that is derived from nonpublic personally identifiable financial information. Such information may include personal financial and account information, information relating to services performed for or transactions entered into on behalf of clients, advice provided by Evergreen Advisors, LLC to clients, and data or analyses derived from such nonpublic personal information.

Background

The purpose of these privacy policies and procedures is to provide administrative, technical and physical safeguards which assist employees in maintaining the confidentiality of nonpublic personal information collected from the consumers and customers of an investment adviser. All nonpublic information, whether relating to an adviser's current or former clients, is subject to these privacy policies and procedures. Any doubts about the confidentiality of client information must be resolved in favor of confidentiality.

Responsibility

Michael O'Donnell is responsible for reviewing, maintaining and enforcing these policies and procedures to ensure meeting Evergreen Advisors, LLC's client privacy goals and objectives while at a minimum ensuring compliance with applicable federal and state laws and regulations. Michael O'Donnell may recommend to the President any disciplinary or other action as appropriate. Michael O'Donnell 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.

Procedure

Evergreen Advisors, LLC has adopted various procedures to implement the firm's policy and reviews to monitor and insure the firm's policy is observed, implemented properly and amended or updated, as appropriate, which include the following:

Non-Disclosure of Client Information

Evergreen Advisors, LLC maintains safeguards to comply with federal and state standards to guard each client's nonpublic personal information. Evergreen Advisors, LLC 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 has requested or authorized, or to maintain and service the client's account;
- As required by regulatory authorities or law enforcement officials who have jurisdiction over Evergreen Advisors, LLC, 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 termination of their employment, from disclosing nonpublic personal information to any person or entity outside Evergreen Advisors, LLC, including family members, except under the circumstances described above. An employee is permitted to disclose nonpublic personal information only to such other employees who need to have access to such information to deliver our services to the client.

Safeguarding and Disposal of Client Information

Evergreen Advisors, LLC restricts access to nonpublic personal information to those employees who need to know such information to provide services to our clients.

Any employee who is authorized to have access to nonpublic personal information is required to keep such information in a secure compartments or receptacle on a daily basis as of the close of business each day. All electronic or computer files containing such information shall be password secured and firewall protected from access by unauthorized persons. Any conversations involving non public personal information, if appropriate at all, must be conducted by employees in private, and care must be taken to avoid any authorized persons overhearing or intercepting such conversations.

Safeguarding standards encompass all aspects of the Evergreen Advisors, LLC that affect security. This includes not just computer security standards but also such areas as physical security and personnel procedures. Examples of important safeguarding standards that Evergreen Advisors, LLC may adopt include:

- Access controls on customer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing customer 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. intruder detection devices, use of fire and burglar resistant storage devices);

- Dual control procedures, segregation of duties, and employee background checks for employees with responsibilities for or access to customer information (e.g. require data entry to be reviewed for accuracy by personnel not involved in its preparation; adjustments and correction of master records should be reviewed and approved by personnel other than those approving routine transactions, etc.);
- 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);
- Server is backed-up on a nightly basis and we have read and feel confident in the privacy policies of our third party service providers.
- 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. backup and store off site key data to ensure proper recovery); and
- Information systems security should incorporate system audits and monitoring, security of physical facilities and personnel, the use of commercial or in-house services (such as networking services), and contingency planning.

Any employee who is authorized to possess "consumer report information" for a business purpose is required to take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. There are several components to establishing 'reasonable' measures that are appropriate for the firm:

- Assessing the sensitivity of the consumer report information we collect;
- The nature of our advisory services and the size of our operation;
- Evaluating the costs and benefits of different disposal methods; and
- Researching relevant technological changes and capabilities.

Some methods of disposal to ensure that the information cannot practicably be read or reconstructed that Evergreen Advisors, LLC may adopt include:

- Procedures requiring the shredding of papers containing consumer report information;
- Procedures to ensure the destruction or erasure of electronic media; and
- After due diligence, shredding client information and downloads where they are not required to be maintained.

Privacy Notices

Evergreen Advisors, LLC will provide each natural person client with initial notice of the firm's current policy when the client relationship is established. Evergreen Advisors, LLC shall also provide each such client with a new notice of the firm's current privacy policies at least annually. If Evergreen Advisors, LLC shares nonpublic personal information relating to a non-California consumer with a nonaffiliated company under circumstances not covered by an exception under Regulation S-P, the firm will deliver to each affected consumer an opportunity to opt out of such information sharing. If, at any time, Evergreen Advisors, LLC adopts material changes to its privacy policies, the firm shall provide each such client with a revised notice reflecting the new privacy policies. The Compliance Officer is responsible for ensuring that required notices are distributed to the Evergreen Advisors, LLC's consumers and customers.