

LEGACY FINANCIAL STRATEGIES, LLC

CUSTOMER PRIVACY POLICY NOTICE

Background

In November of 1999, Congress enacted the Gramm-Leach-Bliley Act (GLBA). The GLBA requires certain financial institutions, such as investment advisor firms, to protect the privacy of customer information.

Policy

Legacy Financial Strategies, LLC ("Legacy" or the "Firm") requires that our clients provide current and accurate financial and personal information. For purposes of this policy, nonpublic personal information includes the client's name, address, income, social security or tax identification number, assets, account history and any financial and health information obtained from a client in connection with the Firm providing a financial product or service.

It is Legacy's policy to proactively protect the information our clients have provided in a manner that is safe, secure and professional. The Firm and its employees have an obligation to protect the security and confidentiality of such information and prevent unauthorized access to and the use of this information, which could result in harm or inconvenience to the Firm's clients.

Collection and Use of Customer Information

In the course of doing business, Legacy collects and uses various types of information provided by its customers through personal interviews, checklists, account applications and other forms, written notations, and in documentation provided to us by our customers for investment and services. Legacy uses this information to service our clients' financial needs and goals.

Safeguarding Customer Documents

Legacy is committed to safeguarding the confidential information of its clients and former clients. Legacy maintains physical, electronic and procedural safeguards to protect our clients' nonpublic personal information, including, but not limited to:

- Access to confidential information is monitored and restricted so that only those employees with approval may access the files. No individual who is not so authorized shall obtain or seek to obtain personal and financial customer information.
- No individual with authorization to access personal and financial customer information shall share that information in any manner without the specific consent of a Firm principal.
- Files containing confidential client information must be maintained in areas that provide the greatest physical security. Employees must lock file cabinets containing personal information each night to prevent potential intruders from access.
- Remote or offsite access to an employee's email or the Firm's network requires the use of 'strong' passwords that contain a minimum of six characters that are a combination of uppercase and/or lowercase letters, numbers and symbols.
- Employees are not permitted to store client information on external computers or PDAs, unless such devices have been issued by the Firm.

- Contracts with non-affiliated third-parties with whom the Firm provides access to client information for performance of services must include a confidentiality and non-disclosure provision and must comply with applicable consumer privacy rules..
- All client information and company data processed by computers and stored or transmitted electronically or otherwise must be adequately safeguarded against damage, loss, alteration, theft and unauthorized disclosure. In addition, we may also use certain artificial intelligence tools (AI) for various business or client related purposes (such as recording and summarizing meetings), but we have strict policies related to the use of AI including the tools which may be used and the use and retention of results, and we allow client to opt out of meeting recordings.
- We maintain physical, electronic, procedural and other safeguards in order to protect all client information from unauthorized access, as well as to detect and respond to security breaches Should a security breach occur, our policy is to notify affected individuals when required within 30 days of discovery.
- All business records must be retained according to the Firm's record retention policy organized in a logical and systematic manner and reviewed on a periodic basis.

Training

Legacy trains our employees and representatives on protecting confidential client information and to understand and comply with these procedures. This training occurs initially upon hire, and annually thereafter. Failure to observe Legacy's procedures regarding customer and consumer privacy will result in discipline and may lead to termination.

Sharing Nonpublic Personal and Financial Information

Legacy is committed to the protection and privacy of its customers' and consumers' personal and financial information. As such, Legacy will not share such information with any nonaffiliated third party except:

- When necessary to complete a transaction in the account, such as with the clearing firm or account custodians;
- When required to maintain or service a customer account;
- To resolve customer disputes or inquiries;
- With persons assessing compliance with industry standards, or to the attorneys, accountants, and auditors of the Firm;
- With persons acting in a fiduciary or representative capacity on behalf of the customer;
- To protect against or prevent actual or potential fraud, identity theft, unauthorized transactions, claims or other liability;
- When required by a regulatory agency, or for other reasons required or permitted by law;
- In connection with a sale or merger of Legacy Financial Strategies, LLC's business; or
- In any circumstances with the customer's instruction or consent.

Opt-Out Provisions

It is not a policy of Legacy to share nonpublic personal and financial information with unaffiliated third parties except under the circumstances noted above. Clients and former clients may however opt out from some of our sharing of information with the aforementioned parties. Please contact us by phone, mail, fax, or email to confirm such options.

For questions, please contact Bethany Boschert, Chief Compliance Officer - bethany.boschert@legacykc.com