The TIFIN Group
Privacy Policy

Background: Financial institutions such as banks, broker-dealers, investment advisors and their vendors or services providers (collectively "Firms") are subject to Regulation S-P, which requires Firms to adopt policies and procedures to protect "nonpublic personal information" about consumers, and to provide customers, no later than the time a customer relationship is established, a clear and conspicuous notice that reflects (i) the policies and procedures adopted by the Firms to protect nonpublic personal information, (ii) the conditions under which nonpublic personal information about consumers will be disclosed to nonaffiliated third parties, and (iii) the methods available to consumers to prevent the sharing of such information with nonaffiliated third parties. Regulation S-P applies only non-public personal information about individuals (i.e. natural persons) who obtain financial products and services primarily for personal, family or household purposes. Regulation S-P does not apply to information about companies or about individuals who obtain financial products or services primarily for business, commercial or agricultural purposes.

Regulation S-P requires an initial notice be delivered at the time a customer relationship is established and another notice be delivered annually during the continuation of the customer relationship. "Annually" means at least once in a period of 12 consecutive months.

A Firm must provide a right to "opt out" if the Firm reserves the right to disclose nonpublic personal information about the consumer to unaffiliated third parties, unless (i) the unaffiliated third party is performing servicing or marketing services for the Firm, (ii) the consumer consents to the disclosure or (iii) the disclosure is permitted or required by law.

A ***"consumer***" is defined as an individual who obtains or has obtained a financial product or service from the Firm for personal, family or household purposes. This includes an individual who provides nonpublic personal information to a Firm, even if the individual ultimately does not open an account. An individual who provides only his or her name, address and general areas of investment interest in connection with a request for more information is not a consumer with respect to a Firm.

A ***"customer"*** is a consumer who has established a customer relationship with a Firm. A customer relationship is defined in Regulation S-P to mean a continuing relationship between the consumer and a Firm under which the Firm provides financial products and services to the consumer primarily for personal, family or household purposes. A customer relationship is established when a consumer establishes an investment advisory relationship with a Firm.

"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.

"Personally identifiable financial information" means any information: (i) the consumer provides to a Firm to obtain financial products or services, (ii) about the consumer resulting from a transaction between the consumer and a Firm, or (iii) that a Firm otherwise obtains from the consumer in connection with providing financial products or services to the consumer. Such information may include information provided on an account application, account balances and transaction information, the fact that the consumer is or has been a customer of a Firm, information relating to services performed for or transactions entered into on behalf of customers, and information from consumer reports and any data, list or analyses derived from such nonpublic personal information.

Firms that possess consumer report information for business purposes are required to properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. "*Consumer Report Information*" means any record about an individual (e.g., name, social security number, phone

number, email address, etc.), whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report. The definition includes a compilation of such records but does not include information that does not identify individuals, such as aggregate information or blind data. "*Consumer Report*" is defined in the Fair Credit Reporting Act ("FCRA"), but generally means information from a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, reputation, etc., which is used for the purpose of establishing eligibility for credit, insurance or employment or used for other purposes permitted under the FCRA. A Firm is not required to ensure perfect destruction of consumer report information. Rather, Firms are required to take "reasonable measures" to protect against unauthorized access to or use of the information in connection with its disposal. The SEC has noted that it expects Firms in devising disposal methods to consider the sensitivity of the consumer report information, the nature and size of the entity's operations, the costs and benefits of different disposal methods and relevant technological changes. The SEC also notes that "reasonable measures" are very likely to require elements such as the establishment of policies and procedures governing disposal, as well as appropriate employee training.

Finally, Regulation S-P requires written policies and procedures addressing administrative, technical and physical safeguards for the protection of customer records and information.

Policy: For a comprehensive account of the Firm's policy regarding Clients' nonpublic personal information, please refer to the Firm's Privacy Policy.

The Firm 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 the Firm or as otherwise required by any applicable law; or
- 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 the Firm, except under the circumstances described above. Employees are permitted to disclose nonpublic personal information only to other Employees who need to have access to such information to deliver our services to the client.

Security of Client Information
The Firm restricts access to nonpublic personal information to Employees who need to know such information to provide services to Clients. Any Employee who is authorized to have access to nonpublic personal information is required to keep such information in a secure, locked compartment on a daily basis as of the close of business each day. All electronic or computer files containing such information must be password secured and firewall protected from access by unauthorized persons. Any conversations involving nonpublic personal information, if appropriate at all, must be conducted by Employees in private and care must be taken to avoid any unauthorized persons overhearing or intercepting such conversations.

Delivery Requirements
The Firm will provide each customer with an initial notice of the Firm's privacy policy at the time an account is established. The Firm also shall provide each customer with a new notice of the Firm's current privacy policy at least annually, to be delivered with the annual audited financial statements, within 120 days of the end of the fiscal year. If, at any time, the Firm adopts material changes to its privacy policy, the Firm shall promptly provide each customer with a revised notice reflecting the new privacy policies. The Chief Compliance Officer is responsible for ensuring that required notices are

distributed to consumers and customers.

Disposal of Nonpublic Personal Information
The Firm will shred, deliver to a document destruction firm, or otherwise render illegible hard copies of any customer or consumer nonpublic personal information in its possession when the Firm deems possession of the information to no longer be necessary.

Nonpublic personal information stored on disk, CD, tape or other electronic media shall be cleared, purged, declassified, overwritten and/or encrypted in such a manner so that any information contained therein cannot be restored or decrypted. After the electronic media is cleared, purged, declassified, overwritten or encrypted, the Chief Compliance Officer shall check that the original information is not backed-up or saved on a hard drive, recycle bin, or other memories.

The Chief Compliance Officer shall require that each third-party service provider engaged by the Firm that necessarily obtains access to customers' nonpublic personal information during the course of their services on behalf of the Firm to adopt similar policies and procedures relating to the secure disposal of nonpublic personal information.

External Threats
The Chief Compliance Officer has delegated the following responsibilities to the Chief Technology Officer:

- Maintain reasonably up-to-date firewall protection and operating system security patches, reasonably designed to maintain the integrity of the personal information, installed on all systems processing personal information;
- Maintain reasonably up-to-date versions of system security agent software, which must include malware protection and reasonably up-to-date patches and virus definitions, installed on all systems processing personal information;
- Ensure that, to the extent technically feasible, all personal information stored on pre-approved portable devices, such as laptops or tablets, must be encrypted, as must all records and files transmitted across public networks or wirelessly, to the extent technically feasible;
- Monitor all computer systems for unauthorized use of or access to personal information; and
- Conduct reviews of all systems that monitor for external threats no less than annually. A report will be maintained by the Chief Compliance Officer as evidence of annual review.

Additional Procedures for Massachusetts Residents
For the purposes of the procedures in this subsection, "personal information" includes a Massachusetts resident's first and last name and any of the following a) social security number; b) driver's license number; or c) financial account number (e.g. bank, credit card, etc.). To the extent that a client is a Massachusetts resident, the Firm will implement the following procedures:

- Any personal information maintained or stored on a mobile devices (e.g. laptop or smartphone) will be stored in an encrypted format;
- To the extent technically feasible, any personal information transmitted wirelessly or across a public network will be transmitted in an encrypted format; and
- The Firm will take reasonable steps to ensure that its service providers who have access to the personal information of the Firm's Clients will implement and maintain appropriate security measures for the information.