

## **PRIVACY POLICY OF TREMONT CAPITAL MANAGEMENT, INC. AND ITS SUBSIDIARIES<sup>1</sup>**

### ***General Policy***

Tremont Capital Management, Inc. and its subsidiary companies (collectively, “Tremont”) treat its clients’ nonpublic personal information (“NPI”) with confidentiality and respect. Tremont protects personal information it may collect about individual clients by maintaining physical, electronic and procedural safeguards that meet or exceed the applicable legal requirements found in the Gramm-Leach-Bliley Act (the “GLB Act”) and those rules of the Securities and Exchange Commission, the Federal Trade Commission and the Commodity Futures Trading Commission, including Regulation S-P, implementing the GLB Act (collectively, the “Privacy Rules”). The Tremont privacy policy (the “Policy”) has been designed in respect of any natural person clients Tremont may have and partners in its funds that are natural persons, (collectively, “Clients”) to (i) insure the security and confidentiality of Client records and information; (ii) protect against any anticipated threats or hazards to the security or integrity of Client records and information; and (iii) protect against unauthorized access to or use of Client records or information that could result in substantial harm or inconvenience to any Client. While Tremont has always considered the protection of sensitive information to be a sound business practice and a foundation of Client trust, in keeping with the goals sought to be achieved by the GLB Act and the Privacy Rules, its Policy seeks to insure the protection of information relating to individual persons to whom Tremont may furnish products and/or services. Tremont’s Chief Compliance Officer shall be responsible for reviewing existing policies and procedures for compliance with the Privacy Rules.

NPI is defined within the rules to mean all information which may be obtained by a financial institution with respect to a Client to whom a financial service or product may be provided by such institution, but does not include publicly available personally identifiable financial information except to the extent such information is disclosed in a manner that indicates an individual is a consumer of the financial institution.

### ***Privacy Notices***

---

<sup>1</sup> In accordance with the Federal Trade Commission’s Rules, *Privacy of Consumer Financial Information and Standards for Safeguarding Customer Information*, the Privacy Policy of Tremont Capital Management, Inc. and its Subsidiaries, as the same may be amended from time to time, has been adopted by the following Tremont funds: <sup>1</sup> Tremont Opportunity Fund, L.P., Tremont Opportunity Fund II, L.P., Tremont Market Neutral Fund, L.P., Tremont Market Neutral Fund II, L.P., Tremont Long/Short Equity Fund, L.P., American Masters Broad Market Fund, L.P., American Masters Broad Market Prime Fund, L.P., American Masters Opportunity Insurance Fund, L.P., American Masters Market Neutral Insurance Fund, L.P., Tremont Trading Fund, LLC, LifeInvest International Insurance Fund, L.P., Tremont Value Recognition Fund, LLC, Tremont Global Macro Fund, LLC, LifeInvest Long/Short Equity Insurance Fund, L.P., Tremont Select Equities Offshore Segregated Portfolio, Tremont Select Equities Offshore ERISA Segregated Portfolio, Tremont Select Special Situations Segregated Portfolio, Tremont Select Equities Fund, Tremont Select Special Situations ERISA Segregated Portfolio, Tremont Select Special Situations Fund, Tremont Long/Short Equity Portfolio Limited, Tremont Core Strategies Portfolio Limited, Tremont Master Strategies Trust, which includes the following sub-funds: Tremont Arbitrage Fund, Tremont Emerging Markets Fund, Tremont Equity Fund, Tremont Global Macro Fund, Tremont Japan Fund, Tremont Market Neutral Investment Fund, Tremont Opportunity Investment Fund and Tremont Trading Fund, inclusive of the following Registered Investment companies: OFI Tremont Core Strategies Hedge Fund, OFI Tremont Market Neutral Hedge Fund, Oppenheimer Tremont Market Neutral Fund, LLC and Oppenheimer Tremont Opportunity Fund, LLC.

**Initial Privacy Notice:** Tremont shall provide all new Clients with an initial privacy notice (“Initial Privacy Notice”) when the Client relationship is first established. Since, for the most part, Tremont’s Clients covered under the Privacy Rules consist of individual partners in Tremont’s funds, such new partners, as a general rule, will receive a copy of the Policy along with the blank subscription document for the fund in which he or she is investing at the commencement of the relationship.

**Annual Privacy Notice:** Tremont shall provide an annual privacy notice (“Annual Privacy Notice” and together with the Initial Privacy Notice, the “Privacy Notices”) to all of its Clients not less than annually during the continuation of the Client relationship. “Annually” shall mean at least once in any period of 12 consecutive months during which that relationship exists.

Tremont’s Chief Compliance Officer shall be responsible for ensuring that all Privacy Notices are provided as required under the Privacy Rules. He shall also verify that there are internal controls in place to ensure the timely delivery of Initial and Annual Privacy Notices to Clients. Tremont shall maintain the practices, policies and protections that its notices represent it will provide. The Chief Compliance Officer shall take appropriate measures to ensure that Tremont adheres to its stated privacy policies and practices.

**Delivery:** Tremont shall provide required Privacy Notices in such fashion that each Client can reasonably be expected to receive actual notice. For purposes of this Policy, “actual notice” shall include:

- Hand delivery of a printed copy of the Privacy Notice to the Client;
- Mailing of a printed copy of the Privacy Notice to the last known address of the Client;
- For those Clients who are registered users of the website, the posting of the Privacy Notice on Tremont’s website.

### ***Assessment of Risk and Information Practices***

The Chief Compliance Officer is responsible for taking reasonable and prudent measures to: (1) identify foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of Client information systems; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of Client information; and (3) assess the sufficiency of policies, procedures, Client information systems, and other arrangements in place to control risks and, when deficiencies are detected, make the appropriate recommendations to management in order to correct such deficiencies.

Tremont shall regularly assess existing practices and procedures with respect to NPI to accurately represent them in Tremont’s Policy and to determine whether any existing practices are prohibited under the Privacy Rules. This assessment shall include a survey of any affected business units. Tremont’s Chief Compliance Officer shall periodically require business units to categorize the following:

- The NPI collected from Clients;
- The sources of NPI collected, such as subscription documents;
- The persons within each business unit who collect and have access to NPI;
- The NPI disclosed to Tremont affiliates (*See, Sharing Information Generally*)

## ***Confidentiality and Security***

Tremont employees have been made aware and are trained as to their responsibility to protect Client confidential information. Within Tremont, access to NPI regarding Clients is restricted to those employees who need to know that information in order to provide Tremont products and services to its Clients.

Tremont has taken appropriate steps to implement a comprehensive information security program that is tailored to Tremont's and each Client's needs and that include administrative, technical and physical safeguards. Tremont's information security program is designed to:

- Ensure the security and confidentiality of Client information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any Client.

To meet the goal's of Tremont's information security program, underlying standards and procedures have been developed. The policies may be changed over time as business processes and technology changes. Further, the effectiveness of all security standards is reviewed on a periodic basis. The security standards are based upon accepted security practices and have been further tailored to meet Tremont's needs.

### **General Information Security Standards:**

- 1) Access controls on Client information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from providing Client information to unauthorized individuals who may seek to obtain this information through fraudulent means (*e.g.* employees are required to use user identifications and passwords);
- 2) Access restrictions at physical locations containing Client information, such as buildings and record storage facilities to permit access only to authorized individuals (*e.g.* keycard access, file cabinet locks, intruder detection devices);
- 3) Encryption of electronic Client information while in transit or between networks or systems to which authorized individuals may have access;
- 4) Logging systems and procedures to detect actual and attempted attacks on or intrusions into Client information systems (*e.g.* data is auditable for detection of loss and accidental and intentional manipulation); and
- 5) Tremont's information security program is tested periodically by an internal auditor to ensure controls, systems and procedures are operating properly.

### **Physical Security Standards:**

- 1) Client information should not be left unattended in offices or conference rooms unless these areas are secure;

- 2) As a general practice, Client files, documents, or other records should be stored in locked cabinets or desks when not in use and, in all cases, secured at the end of the business day;
- 3) Visitors should not be allowed to walk unescorted in areas where Client information is accessible; and
- 4) Protocols have been established for “locking down” offices at the close of business and for access to offices after business hours.

Electronic Records Security Standards:

- 1) Personal computers with access to Client information should not, as a general practice be left unattended, or in the alternative, screen savers/sleep mode should incorporate password protection/lock workstation;
- 2) Password protections for access to network personal computers, Client network accounts, and e-mail user accounts have been implemented. Users are trained to avoid easy-to-guess passwords, not to divulge their passwords, and not to store their passwords where others can access them;
- 3) An appropriate schedule to back up electronic files has been implemented. Backup copies should be tested to ensure that they are fit for the purpose intended and should be stored securely; and
- 4) Encryption technology is used on inter-site e-mail communications containing Client information.

Employee Security Standards:

- 1) Employees are prohibited from disclosing Client information over the telephone or in response to an e-mail unless they have identified the person to whom they are communicating as either the Client or a fiduciary representative of the Client; and
- 2) Employees are required to verify the identity of persons requesting Client information over the telephone or by e-mail by requiring such persons to disclose personal identifying information.

***Privacy on the Internet and on Tremont’s website***

Tremont’s policy of confidentiality towards NPI extends to the Internet and Tremont’s website as well. E-mail information obtained via any electronic correspondence between Tremont and its Clients will be used only for the specific purpose of that correspondence. E-mail addresses will not be sold, nor will they be shared with others outside of Tremont unless Tremont is compelled to do so by law. Likewise, information obtained from users registering on Tremont’s website will not be sold or shared with others outside of Tremont. Tremont maintains personal information in a password-protected electronic file and limits access to such information to employees who need to have such information to provide necessary services.

A note on cookies: "Cookies" are small text files a web site can use to recognize repeat users, facilitate the user's ongoing access to and use of the site and allow a site to track usage behavior

and compile aggregate data that will allow content improvements. Cookies are not programs that come onto a user's system and damage files. Generally, cookies work by assigning a unique number to the user that has no meaning outside the assigning site. **Tremont.com does not use cookies and we do not allow advertisers on the site to set cookies.**

The information gathered by Tremont via the website is used in the following ways:

- To verify a user's identity and eligibility to receive certain products or services including the newsletter.
- To provide information to users about products and services that Tremont believes may be of interest to users.
- To record user's interest in products and services that Tremont offers.
- To respond to user's requests for information.
- Financial information is used to verify that the applicant meets Tremont's eligibility requirements for accredited investors.
- Tremont may be required by law to use information, without the user's consent, in certain circumstances. (*See, Sharing Information with the Government or in Litigation Settings herein*)

Although Tremont has used its best efforts to create a secure and reliable website for its users, the confidentiality of any material or information transmitted to Tremont via the website or by e-mail cannot be guaranteed. When disclosing any personal information, all users should be aware that this information is potentially accessible to others who may consequently collect and use this information for other purposes. Tremont retains no responsibility or liability for the security of personal information transmitted via the Internet, including Tremont's websites.

### ***Nonpublic Information Collected***

Tremont limits the use and collection of information about Clients to the extent necessary to administer its business and provide its services. In general, Tremont may collect the following information from certain of its Clients:

- Information Tremont receives on fund subscription documentation, including but not limited to, Client names, social security numbers, dates of birth, mailing and legal addresses, home and business telephone and telefax numbers, countries of citizenship, occupations and places of employment, annual household incomes and net worth, investment experiences, investment objectives, risk attitudes, consultant information and spousal and immediate family information; and
- Information about a Client Tremont may gather from Client transactions with Tremont, its affiliates or others, including transaction reports and parties to transactions.

### ***Sharing Information Generally***

Tremont is made up of certain entities, including its investment advisory and broker-dealer subsidiaries, and, in turn, is part of a larger corporate affiliation owned by the OppenheimerFunds group and Massachusetts Mutual Life Insurance Company. The Tremont entities and, in some cases, its ownership affiliates often work together to provide the financial products and services offered to Tremont Clients. By sharing information about Tremont's Clients among these

companies and affiliates, Tremont can serve Clients more efficiently. Tremont is permitted to share information concerning Client account history and experiences within and among the companies that comprise Tremont and its subsidiaries and affiliates. In addition, in supplying products and services to Clients, Tremont may engage certain service providers and may enter into joint marketing agreements with other financial institutions. Tremont shall exercise appropriate due diligence in selecting its service providers and make inquiry as to their security policies and procedures. These companies are not permitted to use Tremont's Client information for any purposes other than the services or activities intended or contemplated and only as allowed by applicable law or regulation. Generally, Tremont will insist that as a condition to utilizing any such service provider or entering into any joint marketing agreements that the provider and/or any party to such an agreement agree to treat NPI confidentially.

### ***Sharing Information with the Government or in Litigation Settings***

The United States Internal Revenue Code and various other state and Federal laws and regulations can require financial institutions to provide certain Client information to government agencies. Tremont will only disclose Client information to the government or others under circumstances when it is required to do so by such laws, regulations or by court order.

If a Client is involved in a legal proceeding, both Federal and state laws provide parties to the litigation the right to compel the production of records and other information from banks and other third party record-keepers in certain situations. Likewise, Tremont will only disclose Client information to third party litigants when it is required to do so by lawful judicial process or by court order.

### ***Important Note on Privacy Policy Updates***

**Tremont reserves the right to change this Policy at any time by distributing and/or posting a new Policy without notice. Clients of Tremont should review the Policy periodically to remain informed of any changes. Users of the website will be notified of changes to the Policy when they log on to the site subsequent to a modification in the Policy.**