KENMAR ■ OLYMPIA

PRIVACY POLICY AND PROCEDURES

FOR

KENMAR SECURITIES, LLC

KENMAR PREFERRED INVESTMENTS, LLC

May 2025

TABLE OF CONTENTS

I. INTRODUCTION

This Privacy Policy and Procedures ("**Privacy Policy**") explains the manner in which Kenmar[1] collects, utilizes and maintains non-public personal information about consumers, customers, clients and investors (collectively, "**customers**") who are individuals, as required under federal and other applicable law. Kenmar is committed to protecting a customer's privacy and maintaining the confidentiality and security of a customer's personal information.

The following is a list of Kenmar companies that are obligated by law to adopt this Privacy Policy:

Kenmar Securities, LLC ("**KSEC**"), a Delaware limited liability corporation, is a broker-dealer registered with the United States Securities and Exchange Commission ("**SEC**") and 33 states, and is a member of the Financial Industry Regulatory Authority ("**FINRA**").

Kenmar Preferred Investments, LLC ("**Kenmar Preferred**"), a Delaware limited liability corporation, is registered as an investment adviser with the SEC under the Advisers Act. Kenmar Preferred serves as an investment advisor for private strategies/funds for US investors.

II. REGULATORY FRAMEWORK

The Gramm-Leach-Bliley Act ("**GLBA**") requires all "**financial institutions**," defined to include investment advisers, investment companies and broker-dealers, to establish procedures and systems to assure privacy of customer personal and financial information. The privacy requirements set forth herein apply only to individual, non-entity customers, including U.S. individuals who invest in private funds.

GLBA requires that a financial institution respect the privacy of its customers and protect the security of "**non-public personal information**," defined as personally identifiable financial information provided by a customer, obtained as a result of a transaction with a customer or obtained otherwise. Regulation S-P, adopted by the SEC to implement the privacy provisions of GLBA, treats any personally identifiable information as "financial" if the financial institution received the information in connection with providing a financial product or service to a consumer. Thus, any information provided by individual investors in private or public investment funds or pools (collectively, "**investment funds**") to Kenmar in connection with the investment advisory relationship also should be considered subject to these privacy requirements. In addition, information created in the course of the relationship, such as account balances and securities positions or transactions, is subject to privacy protection.

Further, the NFA issued an Interpretive Notice, "*Compliance Rule 2-4: Misuse of Trade Secrets and Proprietary Information*" (effective on September 5, 2007) which states that NFA Compliance Rule 2-4 prohibits Members and Associates from (a) knowingly obtaining or seeking to obtain another Member's or Associate's confidential information or trade secrets without that person's permission and (b) knowingly or recklessly misusing confidential information or trade secrets in their possession when these activities may harm customers. The Notice gives three examples of behavior that violates the rule: (i) misusing customer information; (ii) disclosing customer orders; and (iii) obtaining or attempting to obtain confidential information disclosing a commodity trading advisor's historical trading positions.

[1] "**Kenmar**", "**we**" or the "**Firm**" means (i) collectively, Kenmar Securities, LLC and Kenmar Preferred Investments, LLC and (ii) private and public investment funds/pools advised by Kenmar, and (iii) each of their affiliates.

It is Kenmar's policy to keep all customer information strictly confidential and not to disclose any such information to non-affiliated third parties, except as permitted by law or set forth herein.

III. CHIEF COMPLIANCE OFFICER

Kenmar's Chief Compliance Officer ("**CCO**") is responsible for administering and enforcing this Privacy Policy and to report any material violations directly to Kenmar's senior management immediately. The CCO may designate one or more qualified persons to perform any portion of his or her requirements under this Privacy Policy. Changes to this Privacy Policy shall be made under the direction of the CCO and Kenmar's senior management and shall be provided to employees promptly after such changes are adopted.

In the discretion of Kenmar's senior management, the CCO may impose sanctions, up to and including forfeiture of compensation or termination of employment for violation of any provision of this Privacy Policy.

The CCO is responsible for ensuring that records concerning this Privacy Policy, including initial and annual privacy notices, are maintained in compliance with Rule 17a-4 under the Securities Exchange Act of 1934, as amended, ("**Exchange Act**"), the Advisers Act and other applicable law. Generally, records retained under this Privacy Policy shall be retained for a period of six (6) years.

Under this Privacy Policy, the CCO, with the assistance of appropriate personnel, will conduct periodic reviews to determine adherence to this Privacy Policy. This review will include, among other things, a review of records maintained under this Privacy Policy, including records contained in customer files. The CCO or his or her designee will document all such reviews, and any remedial steps taken as a result of such reviews.

IV. PRIVACY NOTICES

Under Regulation S-P, Kenmar must deliver **initial** and **annual** privacy notices that describe in general terms Kenmar's information sharing and collection practices. Regulation S-P calls for such disclosures to give "**clear and conspicuous**" notice of Kenmar's privacy policies and practices. Kenmar's Privacy Policy Notice is attached hereto as **Appendix A**.

A. Initial Privacy Policy Notice

Regulation S-P requires delivery of the initial privacy notice upon opening a new account for a customer, except in limited circumstances where subsequent delivery is appropriate, which include when the customer himself or herself has not elected to establish a customer relationship (because, for example, a fiduciary or non-affiliated broker-dealer establishes the customer relationship for the customer) or when to do otherwise would substantially delay the customer's transaction and the customer agrees to receive the notice at a later time. In the limited circumstances where subsequent delivery is appropriate, a broker-dealer, fund or investment adviser may satisfy the delivery requirement by providing the initial notice within a reasonable time after establishing a customer relationship.

Generally, Kenmar will deliver the initial privacy notice upon opening a new account for a customer, which would include the establishment of an investor's capital account with an investment fund, acceptance by an investment fund of an investor's subscription or investment or the issuance of interests in an investment fund. Kenmar's Investor Services and Communications Department, under the direction of the CCO, is responsible for ensuring that we provide initial

privacy notices to our customers in the Welcome Package that is sent upon the opening of a new account.

Kenmar may include the initial privacy notice with subscription or similar agreements or forms. The CCO will have the responsibility to determine whether an exception exists to the requirement that the initial privacy notice be delivered upon the foregoing and shall also determine what is a reasonable time under such circumstances within which to deliver the initial privacy notice.

The initial privacy notice must include, in general but clear terms, Kenmar's practices on information sharing and collection practices. Evidence that the initial privacy notice was sent to the customer must be maintained in separately designated customer files.

B. Annual Privacy Notice to Customers

Privacy notices are also required to be delivered annually to customers "during the continuation" of a customer relationship. Kenmar's Investor Services and Communications Department, under the direction of Kenmar's CCO, is responsible for ensuring that we provide annual privacy notices to its customers. Kenmar has decided that, in general, annual privacy notices will be sent in first calendar quarter of each year to all existing customers as of December 31.

C. Regulation S-P Exemption for Institutions

Institutional customers are not covered by Regulation S-P and no disclosures are therefore required to be made to institutional customers. In the discretion of the CCO and Kenmar's senior management, Kenmar may decide to voluntarily provide notices to institutional customers.

D. Forms ADV

Kenmar Preferred will include a summary of its privacy policies and procedures on Part II of their Form ADV, respectively, unless the CCO determines otherwise.

V. SHARING OF INFORMATION

A. Information Sharing

Kenmar may share nonpublic personal information about customers, without the customer's consent, with affiliated and nonaffiliated parties in the following situations, among others:

- In connection with the administration and operations of Kenmar and its funds, with Kenmar's brokers, attorneys, accountants, auditors, administrators or other service providers;
- To respond to a subpoena or court order, judicial process or regulatory inquiry;
- In connection with a proposed or actual sale, merger, or transfer of all or a portion of its business;
- To protect or defend against fraud, unauthorized transactions (such as money laundering violation), law suits, claims or other liabilities; and
- To assist Kenmar in offering Kenmar-sponsored products and services to customers.

The foregoing may include, among other things, responses to inquiries for purposes of compliance with anti-money laundering and anti-terrorist due diligence, disclosure or reporting requirements. Kenmar also may share nonpublic personal information about customers at customer direction or with customer consent.

B. Service Provider Arrangements

With respect to third parties with which Kenmar shares customer information or which have access to such information, we will:

- Exercise appropriate due diligence in selecting service providers and make inquiry as to their security policies and procedures (initial and ongoing);
- Require, when appropriate, service providers by contract to implement appropriate measures designed to meet the objectives of our information security policies; and
- When appropriate, require service providers to confirm that they have not shared or reused customer information in violation of privacy rules.

C. Federal Opt Out

Because Kenmar only shares nonpublic personal information about customers in accordance with permitted circumstances under Regulation S-P, Kenmar currently does not provide opt out notices.

Kenmar may not, directly or through any affiliate, disclose any nonpublic personal information about a customer to a non-affiliated third party, other than for processing and servicing of accounts or certain other exceptions (including joint marketing between financing institutions where the parties have a confidentiality agreement[2]), ***unless***:

- Kenmar has provided the required initial privacy notice;
- Kenmar has provided the required "opt out" notice in clear and conspicuous language;
- Kenmar has provided for a reasonable opportunity to "opt out"; and
- The customer does not "opt out."

Kenmar's CCO must ensure that non-public personal information is being shared with a non-affiliated third party only in accordance with permitted circumstances under Regulation S-P or under circumstances in which the above four factors have been satisfied.

In the event that circumstances change and Kenmar is required to provide opt out notices, Regulation S-P requires that customers be given a "reasonable" period of time (for example, 30 days) to exercise their opt out right. Opt-out notices will be received by Kenmar, with copies to the CCO, which will take steps, under the supervision of the CCO, to ensure that no information is

[2] This exception requires Kenmar to (1) disclose this information sharing arrangement in its privacy notices and (2) separately contract with, or amend the existing contract with the third party to require such party to maintain the confidentiality of the information and restrict its use as provided in the joint agreement.

shared about those customers who have opted out and the names are deleted from any information sharing databases we maintain.

VI. SAFEGUARDING THE SECURITY OF CUSTOMER INFORMATION

Kenmar has taken appropriate steps to implement a comprehensive information security program that is tailored to our information retention system and the needs of our customers. This includes administrative, technical and physical safeguards appropriate to our size and complexity and the nature and scope of our activities.

A. Principal Designated to Oversee our Program to Safeguard the Security of Customer Information

The CCO in conjunction with the Kenmar's IT Consultant, Compuwork ("**IT Consultant**"), have been designated as having responsibility for ensuring that the following policies and procedures regarding safeguarding customer information are carried out in a timely and appropriate fashion and that adjustments are made as required based on testing results, new technology, new or amended regulatory body rules and regulations or any other matter that may impact the security of customer information.

B. Information Security Program

Kenmar's program is designed to:

- Ensure the security and confidentiality of customer information;
- Protect against any anticipated threats or hazards to the security and 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 customer.

To meet the goals of Kenmar's information security policies, underlying measures, applications, and procedures have been internally developed or applied. These initiatives may be changed over time as business processes and technology changes. The security standards are based upon industry-accepted security practices.

C. General Information Security Standards

Security standards encompass all aspects of Kenmar that affect security. This includes not just computer security standards but also areas such as physical security and personnel procedures.

Examples of important general security standards 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 logins and passwords).

- Access restrictions at physical locations containing customer information, such as buildings, computer facilities, and records storage facilities to permit access only to authorized individuals.

- Encryption of electronic customer information for all wire transfers

- Procedures designed to ensure that customer information system modifications are consistent with Kenmar's information security program.

- Where deemed necessary, 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; adjustments and correction of master records should be reviewed by another not directly entering the data).

- 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.* use of fire resistant storage facilities and vaults; backup and store off site key data to ensure proper recovery).

Any information systems security programs utilized by Kenmar incorporate (as deemed appropriate) 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.

D. <u>Physical Security Standards</u>

Kenmar will adhere to the following physical security standards:

- Customer information shall not be left unattended in offices or conference rooms.

- As a general practice, customer files, documents, or other records shall be stored in locked cabinets or desks when not in use and, in all cases, at the end of each business day.

- Visitors shall not be allowed to walk unescorted in areas where customer information is accessible.

- As a general practice, records or documents containing customer information shall be shredded before disposal.

- Our security policies and procedures of off-site record storage facilities will be periodically assessed (with notes maintained concerning any changes deemed to be appropriate, indicating when such changes were implemented).

- Kenmar's office is generally locked when the receptionist is not present. Employees have access to building via magnetic cards and access to office via physical keys.

- Where deemed appropriate, employees who occupy offices shall lock their office doors at the end of each business day.

E. Electronic Records Security Standards

Whenever reasonably possible, Kenmar will adhere to the following electronic records security standards:

- PCs with access to customer information shall not, as a general practice, be left unattended, or in the alternative, screen savers/sleep mode will incorporate password protection.

- Password protection for access to network servers (including via remote and wireless access), customer account databases, and e-mail user accounts are required. Kenmar is using multi-factor log in protocol for email and data access.

- Electronic files, databases, and email accounts are backed up nightly.

- Anti-virus, anti-malware, and anti-spam software is installed on all PCs and servers with daily updates.

- Firewalls are regularly maintained and utilize intrusion detection and intrusion prevention schemas for all internet and point-to-point circuits.

- Entitlement processes have been developed for (a) requesting, establishing, and closing user (employee) logins; (b) tracking users and their respective access authorizations; and (c) managing these functions.

- Checking with software vendors regularly to obtain and install patches that resolve software vulnerabilities and potential security breaches

- Encryption technology shall be used to protect customer information that is communicated electronically such as wire transfers and sensitive personal data.

F. Contingency and Disaster Security Standards

Kenmar's Business Continuity Plan ("**BCP**") encompasses the identification of mission-critical or business-critical functions that protect customer information and resources that support critical functions.

Physical and environmental controls to anticipate contingencies or disasters and the development of scenarios have been employed to develop appropriate response plans to a wide range of potential events. The BCP provides procedures in the event of a significant business interruption to safeguard our employees and our own property, recover and resume business operations, make financial and operational assessments, protect our books and records, and assist customers to transact business. Kenmar will maintain up-to-date and appropriate programs and controls by, to the extent applicable:

- Addressing any breaches of physical, administrative or technical safeguards; and

- Preserving the integrity of customer information in the event of a computer or other technological failure by backing-up all customer data regularly.

Provisions relating to Kenmar's business continuity and disaster recovery protocols are set forth in greater detail in the BCP, which is reviewed and assessed on a periodic basis.

G. Employee Security Standards

Kenmar will adhere to the following employee security standards:

- All employees are required to sign a Confidentiality and Non-Solicitation Agreement containing appropriate confidentiality provisions upon hire and an acknowledgement of such annually thereafter.

- Customer information access is limited to those employees that require access to the information to either provide customer services or conduct firm operations.

- Upon hire and periodically thereafter, employees will be advised of the prohibition of disclosing customer information over the telephone or in response to an e-mail unless they have clearly identified the person to whom they are communicating as either the customer, a fiduciary representative of the customer, or a party that needs the information to complete a transaction for the customer (i.e., a clearing firm or other appropriate third party). Further, during KSEC's Annual Compliance Meeting, all registered representatives will be reminded of this prohibition. To the extent the customer is not personally known, employees are required to confirm the identity of persons requesting customer information over the telephone or by e-mail by requiring personal identifying information, such as mother's maiden name or social security number, before releasing information.

- Abiding by termination procedures which have been developed to deal with both voluntary and involuntary terminations to ensure that access to customer information is discontinued as soon as possible. This includes but is not necessarily limited to removal of access privileges, e-mail accounts, control of keys, and return of firm property. Upon dismissal, terminated employees are reminded of their continuing responsibilities for confidentiality and privacy of customer information.

H. Outside Service Providers

Outside service providers and Kenmar's attorneys, auditors and administrators, may be given access to non-public personal financial information concerning customers in connection with the provision of services to Kenmar and/or its clients or investment funds. It is Kenmar's reasonable belief that such service providers are capable of maintaining and having in place appropriate safeguards to protect customer information.

VII. RISK ASSESSMENT

The CCO, in conjunction with IT Consultant, is responsible for taking reasonable and prudent measures to:

- Identify foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems;

- Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of customer information;

- Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks and, when deficiencies are detected, make the

appropriate recommendations to senior management in order to correct such deficiencies; and

- Maintain appropriate books and records reflecting all of the above.

VIII. EMPLOYEES

All employees are advised as to their role in implementing our privacy policy upon hire and periodically thereafter. In addition, employees are required to familiarize themselves with this Privacy Policy.

Employees and new hires are provided with copies of this Privacy Policy and acknowledge, in writing, their receipt, review and understanding of it upon hire and periodically thereafter.

IX. TESTING

Kenmar's information program is tested and reviewed continually by Kenmar's IT Consultant and/or other qualified personnel that Kenmar may hire to assess whether controls, systems and procedures are operating properly. Reviews are documented and presented to Kenmar's senior management and are reviewed by senior management. Testing of the information security program will be adjusted in light of changes in technology, the sensitivity of customer information and internal and external threats to information security and other appropriate criteria.

XI. DISPOSAL OF CONSUMER REPORT INFORMATION

The Fair and Accurate Credit Transactions Act of 2003 ("**FACT Act"**), which amended the Fair Credit Reporting Act ("**FCRA**"), requires that "any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose, properly dispose of any such information or compilation."

The FCRA defines "consumer report" as "any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer's eligibility for (a) credit or insurance to be used primarily for personal, family or household purposes, (b) employment purposes or (c) any other purpose authorized under section 604." Further definitions (for example, "consumer reporting agency") and certain definitional exclusions, can be found at www.sec.gov (17 CFR Part 248, Release Nos. 34-50781, IA-2332, IC-36685; File No. S7-33-04, "Disposal of Consumer Report Information.").

A. Exclusion

Information that does not identify particular consumers and information solely as to transactions or experiences between the consumer and the person making the report, as well as the communication of that information among persons related by common ownership or affiliated by corporate control, is not covered under this disposal rule. A person is deemed to be identified based on name and a variety of other personal identifiers such as, but not limited to, social security number, phone number, physical address and e-mail address.

B. Disposal Defined

Disposal means:

- the discarding or abandonment of consumer report information; or
- the sale, donation or transfer of any medium, including computer equipment, on which consumer report information is stored.

C. Designation of Supervising Principal

The CCO will oversee Kenmar's policies and procedures to ensure that the appropriate disposal is undertaken in accordance with the requirements under the FACT Act and the FRCA, which include reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

D. Implementation of Disposal Program

The CCO, with the assistance of appropriate personnel, will determine appropriate times and methods of disposal and will take into consideration the following, among other, procedures to be followed:

(1) implementing and monitoring compliance with policies and procedures that require the burning, pulverizing or shredding of papers containing customer report information so that the information cannot practicably be read or reconstructed;

(2) implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing customer report information so that the information cannot practicably be read or reconstructed;

(3) after due diligence efforts are completed, entering into a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as customer report information, in a manner consistent with the disposal rule. Due diligence efforts may include, but are not necessarily limited to:

   (a) reviewing an independent audit of the disposal company's operations and/or its compliance with the disposal rule;

   (b) obtaining information about the disposal company from several references or other reliable sources;

   (c) requiring that the disposal company be certified by a recognized trade association or similar third party;

   (d) reviewing and evaluating the disposal company's information security policies or procedures; and

   (e) other appropriate measure to determine the competency and integrity of the potential disposal company.

If Kenmar utilizes a third party for its disposal requirements, complete records of Kenmar's due diligence efforts will be maintained by the appropriate personnel or the CCO. In all cases, customer information will be disposed of in as a secure a manner as possible to preserve the security of such customer information.

XII. CALIFORNIA FINANCIAL INSTITUTIONS PRIVACY ACT

Under the California Financial Information Privacy Act (or "**SB-1**"), financial institutions (which include broker-dealers) doing business with California consumers must provide consumers, under certain enumerated circumstances with an opportunity to either "opt in" or "opt out," as the case may be, before non-public personal information is transferred from one firm to another.

Currently, based on the exemptions in SB-1 Section 4053(c), Kenmar does not need to provide California residents with an opt-out notice.

Further, under SB-1, Kenmar may not disclose nonpublic personal information about a California customer to or with any non-affiliated third parties who do not provide financial products and services to the California customer without the explicit prior consent ("**opt in**") of the California customer to whom the information relates. This is a significant departure from the requirements of Regulation S-P.

The CCO shall be responsible for overseeing Kenmar's information sharing practices to ensure that they continue to comply with the requirements of SB-1 for customers of Kenmar who are resident in California in the event of change in Kenmar's information-sharing policy or changes to the affiliate relationship.

While it remains unclear the extent to which provisions of Regulation S-P will preempt the requirements of SB-1, Kenmar will treat California resident customers in accordance with SB-1 until such issue is resolved.

KENMAR ■ OLYMPIA

APPENDIX A

FACTS	WHAT DOES KENMAR DO WITH YOUR PERSONAL INFORMATION?
Why?	Financial companies choose how they share your personal information. Federal law gives consumers the right to limit some but not all sharing. Federal law also requires us to tell you how we collect, share, and protect your personal information. Please read this notice carefully to understand what we do.
What?	The types of personal information we collect, and share depend on the product or service you have with us. This information can include: • Social Security number, • birth date, assets and income, and • other financial and investment-related information When you are *no longer* our customer, we continue to share your information as described in this notice.
How?	All financial companies need to share customers' personal information to run their everyday business. In the section below, we list the reasons financial companies can share their customers' personal information; the reasons Kenmar chooses to share; and whether you can limit this sharing.

Reasons we can share your personal information	Does Kenmar share?	Can you limit this sharing?
For our everyday business purposes—such as to process your transactions, maintain your account(s), respond to court orders and legal investigations, or report to credit bureaus	No	N/A
For our marketing purposes—to offer our products and services to you	No	N/A
For joint marketing with other financial companies	No	N/A
For our affiliates' everyday business purposes—information about your transactions and experiences	Yes	No
For our affiliates' everyday business purposes—information about your creditworthiness	No	N/A
For our affiliates to market to you	No	N/A
For our non-affiliates to market to you	No	N/A

Questions?	If you have any questions, please call Kenmar Olympia, LLC at 212-596-3480 or send a letter to Kenmar Olympia, LLC Attention: Investor Services, P.O Box 5537, New York, New York 10185

Who we are	
Who is providing this notice?	Kenmar Olympia, LLC

KENMAR ■ OLYMPIA

What we do	
How does Kenmar protect my personal information?	To protect your personal information from unauthorized access and use, we use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. Kenmar restricts access to your personal information to those employees who need to know that information to provide products and services to you. Kenmar maintains appropriate physical, electronic and procedural safeguards to guard your personal information. Kenmar employs all of the safeguards described previously to maintain the privacy, security and service of our website, along with the following Internet-specific practices: We use firewalls, encryption, and authentication procedures to maintain the security of your online session and to protect Kenmar systems from unauthorized access.
How does Kenmar collect my personal information?	We collect your personal information, for example, about you from any of the following sources: • Applications, questionnaires, subscription documents and other information provided by you in writing, in person, by telephone, electronically or by any other means. This information may include name, address, e-mail address, Social Security number, birth date, assets and income, and other financial and investment-related information; • Transactional activity in your account (such as, investments, including account balances, investments and withdrawals/redemptions); and/or • Other interactions with Kenmar including discussions with our Investor Services Department or information you enter into our Web site.
Why can't I limit all sharing?	Federal law gives you the right to limit only • sharing for affiliates' everyday business purposes—information about your creditworthiness • affiliates from using your information to market to you • sharing for non-affiliates to market to you State laws and individual companies may give you additional rights to limit sharing. California residents please see "Important Privacy Choices for California Consumers"
Definitions	
Affiliates	*Companies related by common ownership or control. They can be financial and nonfinancial companies.* "**Kenmar**" or "**we**" means (i) collectively, Kenmar Securities, LLC and Kenmar Preferred Investments, LLC (ii) private and public investment funds/pools advised by Kenmar, and (iii) each of their affiliates.
Non-affiliates	*Companies not related by common ownership or control. They can be financial and nonfinancial companies.* Kenmar utilizes various service providers to assist in the administration of the private and public investment funds/pools advised by Kenmar.
Joint marketing	*A formal agreement between nonaffiliated financial companies that together market financial products or services to you.*

KENMAR ■ OLYMPIA

Other important information
Kenmar uses personal information in ways compatible with the purposes for which we originally requested it. We may use personal information about you to service and maintain your account; process your request for a website login, process transactions in your account, respond to inquiries from you or your representative develop, offer, and deliver products and services, or to fulfill legal and regulatory requirements. Kenmar does not disclose information about prospective customers with non-affiliated third parties, and only shares information about customers in limited circumstances as required or permitted by law.

Important Privacy Choices for California Consumers

You have the right to control whether Kenmar shares some of your personal information. Please read the following information carefully before you make your choices below.

Your Rights
You have the following rights to restrict the sharing of personal and financial information with our affiliates (companies we own or control) and outside companies that we do business with. Nothing in this form prohibits the sharing of information necessary for us to follow the law, as permitted by law, or to give you the best service on your accounts with us. This includes sending you information about some other products or services.

Your Choices
Restrict Information Sharing With Companies We Own or Control (Affiliates):
Unless you say "No," we may share personal and financial information about you with our affiliated companies.
(___) NO, please do not share personal and financial information with your affiliated companies.
Restrict Information Sharing With Other Companies We Do Business With To Provide Financial Products And Services:
Unless you say "No," we may share personal and financial information about you with outside companies we contract with to provide financial products and services to you. **As a practical matter, it may be impossible to provide products and services to you if we cannot share your personal and financial information with such service providers to your account.**
(___) NO, please do not share personal and financial information with outside companies you contract with to provide financial products and services.
Restrict Information Sharing With Other Companies That Do Not Provide Products and Services To You:
Unless you say "Yes" we may not share personal and financial information about you with outside companies who do not provide financial products and services to you.
(___) YES, I authorize you to share personal and financial information with outside companies who do not provide financial products and services to you.

Time Sensitive Reply
You may make your privacy choice(s) at any time. Your choice(s) marked here or otherwise indicated to us will remain unless you state otherwise. However, if we do not hear from you we may share some of your information with affiliated companies and other companies with whom we have contracts to provide products and services.
To exercise your choices or to modify any of your prior choices do one of the following: (1) Fill out, sign and send back this form to us using the envelope provided (you may want to make a copy for your records); or (2) call Kenmar Olympia, LLC at 212-596-3480 to communicate the information to us.

Print Name: _____

Signature: _____ Date: _____

KENMAR ■ OLYMPIA

ACKNOWLEDGEMENT

TO: Chief Compliance Officer

RE: Privacy Policies and Procedures of Kenmar

I acknowledge that I have read and understand the Privacy Policy and Procedures for Kenmar Securities, LLC and Kenmar Preferred Investments dated as of May 2025 (the "**Privacy Policies and Procedures**").

I hereby agree to adhere to the provisions thereof, including any amendments or updates thereto, at all times during my association with Kenmar and acknowledge that Kenmar may impose sanctions on me, including forfeiture of compensation or termination, for violation by me of any provision of the Privacy Policies and Procedures.

Signature: _____

Print Name: _____

Date: _____