PRIVACY POLICY
DATED: NOVEMBER 2021

1. BACKGROUND

In November 2000, the SEC adopted Regulation S-P under section 504 of the Gramm-Leach-Bliley Act (GLB Act). Regulation S-P imposes notice requirements and restrictions on a financial institution's ability to disclose nonpublic personal information about consumers. In 2003, California enacted the California Financial Information Privacy Act, commonly called SB1. SB1 regulates the disclosure of personal information about California consumers by financial institutions doing business in the state. Through SB1, the California Legislature sought to accord the citizens of California with more stringent protections than those afforded under the federal privacy laws.

Pursuant to federal and state regulations, ThePARTNERS Wealth Management ("ThePARTNERS") is required to:

- Adopt policies and procedures that outline how the institution handles and ensures the privacy of client confidential non-public information (defined in Policy section below);
- Deliver a written statement (the "Privacy Notice") to each client:
  (a) At the inception of the client relationship (i.e. when client executes Client Agreement);
  (b) Annually thereafter; and
  (c) Anytime the information in the Privacy Notice is changed; and
- Provide clients, when applicable, with the ability to opt out in writing prior to sharing their confidential non-public information to both affiliates and non-affiliates under certain circumstances.

2. DEFINITIONS

Affiliate: An Affiliate is any company that controls, is controlled by, or is under common control with the financial institution.

Clear and Conspicuous: Clear and conspicuous means that the notice must be designed to call attention to the information contained in the notice, and that the notice must be reasonably understandable. This means that the typeface and size are large enough to be easily read, and that they are of such a design that will illustrate the significance of the disclosure.

Consumer: A consumer is an individual who obtains financial products or services that are to be used primarily for personal, family, or household purposes. The legal representative(s) of the client are included in the definition. Financial products and services include the investments themselves and those evaluations or analyses that led to the investment.

Consumers are not individuals who:

- Provide only their name, address, or other general contact information for the purpose of obtaining information, such as a response request;
- Have broker-dealer accounts solely for transaction execution, such as accounts cleared through a firm by an introducing or contracted broker-dealer;
- Have accounts or transactions with a firm solely due to agent or service contracts; and
- Other individuals who are not directly defined as consumers of the entity.

Continuing Relationship: A continuing relationship is one in which there is an ongoing association with the Firm. This will include:

- Any consumer with whom the Firm has had one transaction but with whom the Firm expects to develop an ongoing relationship, and future, subsequent transactions
- Any consumer who has contracted with the Firm for continuous and ongoing investment services, or investment supervisory services.

A continuing relationship is not established in cases where there is a stand-alone transaction that is not expected to result in future transactions.

Client: A client is a consumer who has a "client relationship" with the Firm.

Client Relationship: A client relationship is a continuing relationship between a consumer and an investment firm under which the Firm provides investment services.

Nonpublic Personal Information: Nonpublic personal information is essentially that information obtained or collected by the Firm that is personally identifiable financial information. The definition includes lists, groups, or other categories that have been created or derived on the basis of individual or household nonpublic information. For instance, a list of names derived from specific account numbers is nonpublic personal information.

Personally Identifiable Financial Information: Personally identifiable financial information is that information provided to the Firm by a consumer which results in a transaction with the consumer, which results in the provision of any service to the consumer, and or which is obtained by the Firm through the use of account applications, client profiles or questionnaires, or through other means.

Publicly Available Information: Publicly Available Information is that which the Firm may reasonably believe is available to the general public:

- Legally through federal, state, or local governments,
- Broadly through public media such as phone books, web listings, or newspapers.

3. CONSUMER AND CLIENT DISTINCTIONS

Generally, there are distinctions among clients and consumers, requiring differing levels of protection to each. A consumer is an individual who obtains financial products or services to be used primarily for personal purposes. Products and services can include evaluations of information, in addition to the service itself. By contrast, a client is a consumer with a continuing relationship with the entity to obtain the services of a consumer. Therefore, all clients are also consumers.

4. POLICIES AND PROCEDURES

Under Regulation S-P and SB1, ThePARTNERS must provide its clients with a clear and conspicuous written notice describing its privacy policies and practices. The notice must be reasonably understandable and must accurately describe how ThePARTNERS collects, discloses and protects nonpublic information about clients, including former clients.

Under SB1, ThePARTNERS must not sell, share, transfer, or otherwise disclose nonpublic personal information about any California client to or with any nonaffiliated third parties without the explicit prior consent of the client. To obtain such consent, financial institutions are required to utilize a form, statement, or writing that is a separate document, not attached to any other document; is dated and signed by the consumer; clearly and conspicuously discloses that by signing, the consumer is consenting to the disclosure of nonpublic personal information to nonaffiliated third parties.

Regulation S-P and SB1 also prohibit the disclosure of certain information about a financial institution's customers to non-financial institutions which ThePARTNERS has agreements with to provide financial products or services unless ThePARTNERS provides certain information to the clients and the client has not elected to opt out of the disclosure.

With the increase in identity theft and misuse of confidential nonpublic personal information, it is imperative for ThePARTNERS to ensure its employees are trained on how to adequately protect nonpublic personal information contained within its books, records and electronic mediums. State and federal regulations require ThePARTNERS to adopt policies and procedures to safeguard customer information, including the proper disposal of consumer report information and records.

Therefore, ThePARTNERS has adopted the following day-to-day business practices to: (i) maintain the security and confidentiality of client records and information; (ii) protect such client information against anticipated threats or hazards in its maintenance and disposal processes; and (iii) prohibit unauthorized access to or use of client records or information that may result in actual or potential harm to the client.

a. POLICY

ThePARTNERS' policy is to proactively protect the confidentiality of their clients' personal information. For purposes of this policy, nonpublic personal information includes the client's name, address, income, social security or tax identification number, assets in a client's account, history of a client's account and any financial information obtained from a client in connection with ThePARTNERS providing a financial product or service. It also includes similar personally identifiable data relating to ThePARTNERS Associated Persons.

The improper use of confidential client information can subject ThePARTNERS and its Associated Persons to civil liability for damages, as well as criminal penalties. ThePARTNERS and its Associated Persons 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 ThePARTNERS clients.

Training on protecting confidential client information will be conducted by ThePARTNERS for all Associated Persons at the inception of employment and periodically thereafter. Failure to comply with these procedures could result in disciplinary actions, up to and including termination of employment.

b. PROCEDURES

In order to adhere to applicable state and federal requirements and the above stated policy, ThePARTNERS has adopted written procedures that describe the basic obligations and responsibilities which Associated Persons must adhere to when handling confidential client information.

i. NOTIFICATION TO CONSUMERS

ThePARTNERS is required to deliver a written notice to clients ("Privacy Notice"), which provides clear and conspicuous notice of the Firm's privacy policies. ThePARTNERS has adopted a written Privacy Notice that outlines:

- Categories of information collected;
- Categories of information disclosed;
- To what extent, if any, the information is disclosed to non-affiliated third-parties and requires the customer to consent to such disclosure before any nonpublic information is shared;
- Any arrangements ThePARTNERS has with outside companies that perform marketing services on ThePARTNERS' behalf or agreements to provide financial products or services, and notifies customers of their right to opt-out of the sharing of such information and provides a reasonable way in which the customer may opt-out; and
- Procedures in place to protect the confidentiality of nonpublic personal information of ThePARTNERS consumers and customers.

For new clients, ThePARTNERS Privacy Notice is given at the time of engagement. Thereafter the Privacy Notice is sent (electronically or physical mail) annually to all clients. ThePARTNERS will also send (electronically or physical mail) the Privacy Notice anytime there is a material change to ThePARTNERS' Privacy Notice.

The CCO or designee is responsible for ensuring that ThePARTNERS Privacy Notice is delivered to clients initially upon engagement, and annually thereafter and for maintaining proof of such initial and annual delivery in an appropriately designated file, which includes a copy of the Privacy Notice, the date the Privacy Notice was delivered and the name of each client to whom the Privacy Notice was provided. Please refer to ***Exhibit E*** attached hereto for a copy of ThePARTNERS' Privacy Notice.

ii. SAFEGUARDING CONFIDENTIAL CLIENT INFORMATION

ThePARTNERS and its Associated Persons have an ongoing responsibility to safeguard confidential client information in both the real world and virtual world, and therefore adopt the following procedural mandates:

1. Access to confidential information will be limited to those Associated Persons who have a need to know such information in order to perform their duties. Associated Persons are instructed to only collect client information that is needed by ThePARTNERS for the performance of its services.

2. Associated Persons should limit the review of client files and records to those portions of the files relevant to their work-related needs and must not remove or duplicate confidential information except where required in connection with the performance of their duties on behalf of ThePARTNERS.

3. Files containing confidential client information must be maintained in areas that provide the greatest physical security. Associated Persons must lock file cabinets containing personal information each night to prevent potential intruders from access.

4. Remote or offsite access to an Associated Person's email or the Firm's network requires the use of 'strong' passwords preferably ones with 10 characters consisting of a combination of upper and lowercase letters, numbers, and characters.

5. Associated Persons are not permitted to store client information on external computers or PDAs, unless such devices have been issued to the Associated Person by the Firm. In any event, all computers, PDAs or similar devices which an Associated Person plans to use in connection with his or her duties or responsibilities for the Firm must be reviewed and authorized by the CCO prior to such use. Access to data held on such devices must be protected by 'strong' passwords, preferably ones with 10 characters consisting of a combination of upper and lowercase letters, numbers, and characters. Further, the device must be protected by "locking" capability, in which it locks automatically no longer than 10 minutes after its last use, and by which, where possible, it may be locked remotely by the use of computer software. In addition, in the case of PDAs and where possible personal computers, such devices must be protected by remote "wipe" capability to erase all data on such device, and Associated Persons must inform the CCO immediately of any possible breach of data security. In addition, the Associated Person must provide the necessary protocol to the CCO so that the CCO may 'wipe' the device should it be missing, should employment of the Associated Person be terminated, or for any other reason if in the view of the CCO the Firm's client or other data may be at risk.

6. Associated Persons must abide by all security procedures and records retention guidelines designed to protect the Firm's records and systems and the integrity of the data accessed through them.

7. Associated Persons must not release confidential client information except in accordance with ThePARTNERS procedures and only with the written authorization of the client or as required by law; (*e.g*., pursuant to a valid subpoena or court order).

8. Contracts with non-affiliated third-parties with whom ThePARTNERS provides access to client information for performance of services must include a confidentiality and non-disclosure provision. This provision must stipulate that the provider must not use or disclose client information other than to the extent required to provide services on behalf of ThePARTNERS.

9. 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.

10. ThePARTNERS may consider using encrypted data, firewalls, patches, routers, filters and 'strong' passwords to prevent unauthorized access to confidential client information stored electronically. Each Associated Person must shut down their computer at the end of the workday to block potential hackers.

11. ThePARTNERS electronic systems contain automatic lockout features for unsuccessful login attempts and prevent simultaneous logins. Automatic session timeout parameters must be utilized to minimize periods of session inactivity.

12. 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 for destruction or continued retention.

13. When disposing of client information, paper copies must be shredded prior to disposing in trash and electronic copies must be completely erased prior to selling, transferring and/or disposing of the computer or electronic device.

14. Upon leaving the Firm, Associated Persons are not permitted to take any nonpublic personal information relating to any clients of the Firm. To protect information after an Associated Person has been terminated, the Firm must take steps to secure the electronic and hard copies of all documentation, including preventing access to online systems and physically safeguarding records and other documentation.

15. Associated Persons must agree that, upon termination of their relationship with the Firm, any and all of ThePARTNERS' blank forms must be destroyed, and any stationary, business cards or websites must no longer contain any reference to ThePARTNERS.

iii. TRAINING OF ASSOCIATED PERSONS

The CCO or designee will provide training to Associated Persons initially upon hire and annually. Such training will include, among other things, each Associated Person receiving, reading and acknowledging receipt of a copy of this Manual at least annually, which includes the Firm's privacy and security program.

iv. ADMINISTRATION OF THE PROGRAM

The CCO or designee will perform periodic reviews of the Firm's privacy and security program to assess: (a) whether the program continues to be reasonable designed to safeguard non-public personal information, (b) whether any updates are required, and (c) whether there have been any violations of the policy and procedures.

Associated Persons are required to immediately report any potential violation or violation of these policies and procedures of which he or she becomes aware, to the CCO. No Associated Person will be sanctioned for the reporting of a potential violation or violation.

Discovery of a breach in the security of the Firm's electronic system containing client or employee non-public information or the misappropriation of such non-public information must be reported to the CCO immediately. The CCO or designee will promptly notify in writing the clients and/or employees whose personal non-public information was, or is reasonably believed to have been, acquired by an unauthorized person.

v. VIOLATIONS AND SANCTIONS

The CCO or designee will assess whether any violation has occurred. If it is determined that a violation has occurred, the CCO may impose such sanctions as he deems appropriate, which depending on the facts and circumstances, may include fines and/or dismissal from ThePARTNERS.

The CCO will create and maintain documentation that outlines each violation, what sanctions were imposed and what steps were taken to help ensure that the same violation does not happen again.