PRIVACY POLICY NOTICE
KONNECT HEALTH AND WEALTH LLC

Konnect Health and Wealth Llc ("Konnect") adopted this policy, in compliance with Regulation S-P (17 C.F.R. § 248), as amended effective September 2024, Regulation S-AM (17 C.F.R. §§ 248.100–248.130), and Regulation S-ID (17 C.F.R. §§ 248.201–248.202), with recognition that protecting the privacy and security of the nonpublic personal information, including Sensitive Customer Information (as defined herein), we obtain about our clients is an important responsibility. We also know that you expect us to service you in an accurate and efficient manner. To do so, we must collect and maintain certain nonpublic personal information about you. We want you to know what information we collect and how we use and safeguard that information.

WHAT INFORMATION WE COLLECT

We collect certain nonpublic personal information about you (such as your name, address, social security number, etc.) that you provide on applications or other forms, as well as communications (electronic, telephone, written, or in person) with you or your authorized representatives (such as your attorney, accountant, etc.). We also collect information about your brokerage accounts and transactions (such as purchases, sales, account balances, inquiries, etc.). For purposes of this Policy, "Sensitive Customer Information" means any component of customer information, standing alone or in combination, that could be used to access a customer account or conduct unauthorized financial transactions, including: (a) account numbers, user names, passwords, access codes, or security codes; (b) Social Security numbers or tax identification numbers; (c) payment card numbers or expiration dates; and (d) any other information defined as "Sensitive Customer Information" under Regulation S-P § 248.30(a)(9). We may also obtain information about you from consumer reporting agencies, identity verification services, and other third-party sources consistent with applicable law.

WHAT INFORMATION WE DISCLOSE

Konnect does not disclose the nonpublic personal information we collect about our clients to anyone except: (1) in furtherance of our business relationship with clients, and then only to those persons necessary to effect the transactions and provide the services that clients authorize (such as broker-dealers, custodians, independent managers etc.); (2) to persons assessing our compliance with industry standards (e.g., professional licensing authorities, etc.); (3) our attorneys, accountants, and auditors; or (4) as otherwise provided by law.

We are permitted by law to disclose the nonpublic personal information about you to governmental agencies and other third parties in certain circumstances (such as third parties that perform administrative services on our behalf). These third parties are prohibited from using or sharing information for any other purpose. Pursuant to Regulation S-P, as amended, service providers and vendors that receive nonpublic personal information or Sensitive Customer Information on our behalf are required, by written contract, to maintain appropriate administrative, technical, and physical safeguards to protect that information and to promptly notify us of any security incidents affecting your information. If you decide to either terminate our services or become an inactive client, we will continue to adhere to our Privacy Policy, as may be amended from time to time.

We are required to report any suspected exploitation of vulnerable adult clients to the proper authorities under federal and state statutes.

SECURITY OF YOUR INFORMATION

We restrict access to your nonpublic personal information to those employees who need to know that information to service your account. We maintain physical, electronic, and procedural safeguards that comply with applicable federal and state standards, including the written safeguards program requirements of Regulation S-P (17 C.F.R. § 248.30) and the 2024 amendments thereto, to protect your nonpublic personal information.

INCIDENT RESPONSE AND BREACH NOTIFICATION

We have adopted a written Incident Response Program ("IRP") as required by the 2024 amendments to Regulation S-P (17 C.F.R. § 248.30). The IRP is designed to detect, respond to, and recover from unauthorized access to or use of customer information, including Sensitive Customer Information, and to assess and contain the impact of any security incident.

Customer Notification: In the event of a breach of security resulting in unauthorized access to or use of your Sensitive Customer Information, Konnect is required to notify affected customers as soon as reasonably practicable, and in no event later than thirty (30) calendar days after we become aware of the breach, unless law enforcement directs a delay. The notification will describe the nature of the incident, the type of information involved, the steps we have taken or are taking in response, and the steps you may take to protect yourself from potential harm.

Service Provider Reporting: If a service provider that maintains your nonpublic personal information on our behalf experiences a security incident, such service provider is contractually required to notify us within seventy-two (72) hours of becoming aware of the incident. Upon receiving such notification, we will assess the incident and, where required, provide timely notification to affected customers in accordance with the thirty-day timeframe described above.

CHANGES TO OUR PRIVACY POLICY OR RELATIONSHIP WITH YOU

Our policy about obtaining and disclosing information may change from time to time. We will provide you with notice of any material change to this policy before we implement the change.

AFFILIATE MARKETING LIMITATIONS

Regulation S-AM (17 C.F.R. §§ 248.100–248.130) limits the circumstances under which Konnect and its affiliates may use information received from one another to make marketing solicitations to you. If Konnect receives "Eligibility Information" about you from an affiliate (i.e., information bearing on your creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living, used to determine eligibility for products or services), we may not use that information to solicit you without first providing you with a notice and a reasonable opportunity to opt out.

Affiliate Marketing Opt-Out: If we intend to use Eligibility Information received from an affiliate to make a marketing solicitation to you, we will provide you with a separate notice describing your right to opt out and the method by which you may exercise that right. Your opt-out election will remain in effect for a period of at least five (5) years, unless you revoke it earlier. To opt out or for questions about affiliate marketing practices, please contact the Chief Compliance Officer at the address or phone number set forth below.

OPTING OUT

Non-Affiliated Third-Party Opt-Out (Regulation S-P): Clients retain the right to opt out of sharing information with non-affiliated third parties. However, if you opt out of sharing non-public personal information with non-affiliated third parties who provide services which are essential for the management of your account ("*Essential Parties*"), Konnect will be unable to properly manage your account. Therefore, if you choose to opt of sharing information to *Essential Parties*, you will not be able to open or maintain an advisory account with Konnect Health and Wealth Llc.

IDENTITY THEFT PREVENTION PROGRAM

Regulation S-ID (17 C.F.R. §§ 248.201–248.202) requires certain covered financial institutions and creditors to adopt and implement a written Identity Theft Prevention Program ("ITPP") designed to detect, prevent, and mitigate identity theft in connection with the opening and maintenance of covered accounts. Konnect has adopted and implemented an ITPP that includes reasonable policies and procedures to: (a) identify relevant patterns, practices, and specific forms of activity known as "Red Flags" that signal possible identity theft; (b) detect Red Flags incorporated into the Program; (c) respond

appropriately to detected Red Flags to prevent and mitigate identity theft; and (d) update the Program periodically to reflect changes in identity theft risks.

Reporting Suspected Identity Theft: If you believe your account or personal information has been subjected to unauthorized access or identity theft, please contact the Chief Compliance Officer immediately at the address or phone number set forth below. We will investigate promptly and take appropriate responsive action under our ITPP and applicable law, including applicable state identity theft notification statutes. Our ITPP is reviewed and updated at least annually by senior management and overseen by the Chief Compliance Officer.

REQUESTS FOR INFORMATION

For a copy of our Privacy Policy, please contact the Chief Compliance Officer either in writing at 1428 Strada Curva, New Braunfels, TX 78132, or by phone at (832) 871-3172.