ROOT, INC.

ANTI-MONEY LAUNDERING AND SANCTIONS POLICY

APPROVED BY THE BOARD OF DIRECTORS

Effective May 4, 2022

I. PURPOSE

Root, Inc. and its subsidiaries (together, "***Root***") are fully committed to compliance with all applicable anti-money laundering ("***AML***") and economic sanctions laws and regulations, including, the Bank Secrecy Act ("***BSA***") as amended by the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("***USA PATRIOT Act***"), its implementing regulations, and any other applicable state or federal regulations. Root is also bound by the economic sanctions and embargoes administered and enforced by the Office of Foreign Assets Control ("***OFAC***"). Such laws and regulations impose restrictions and, in some cases, prohibitions on engaging in transactions or other dealings with or involving certain countries, entities, and individuals. This policy applies to all directors, officers and employees of Root. In addition, we expect our agents, consultants, representatives, lobbyists, suppliers/vendors, resellers, distributors, customs or other brokers, contractors and other business partners to comply with the principles contained in this policy.

II. POLICY STATEMENT

Root considers compliance with applicable AML and economic sanctions laws and regulations to be a high priority. Further information relating to the requirements under the AML and economic sanctions laws are included as guidelines to this policy. You are required to read and adhere to the requirements described in this policy and the corresponding guidelines. Root will, as appropriate, update information transmitted to its directors, officers, and employees to address changes with respect to this policy and the laws and regulations cited herein.

III. ANTI-MONEY LAUNDERING COMPLIANCE GUIDELINES

The BSA, as amended by the USA PATRIOT Act requires financial institutions, including insurance companies offering certain products, to maintain and administer a risk-based AML program. The insurance regulations only apply to a limited range of products that may pose a higher risk of abuse by money launderers and terrorist financiers. A covered product, for the purposes of an AML compliance program, includes (i) permanent life insurance policy, other than a group life insurance policy,(ii) any annuity contract, other than a group annuity contract, or (iii) any other insurance product with features of cash value or investment.

Although Root does not currently offer covered products, Root has established policies and procedures (collectively, the "***AML Program***") designed to comply with the USA Patriot Act, including Section 352, which requires such programs to include the following elements: (i) development of internal policies and procedures, (ii) appointment of an AML Compliance Officer, (iii) ongoing training, and (iv) implementation of an independent audit function to test the AML Program.

III.A. DEVELOPMENT OF INTERNAL POLICIES AND PROCEDURES

III.A.1. KNOW YOUR CUSTOMER

As part of servicing new customers and customer transactions, you must generally request the following information: (i) the name; (ii) date of birth (for an individual); (iii) an address, which will be a residential or business street address (for an individual), an Army Post Office (APO) or Fleet Post Office (FPO) box number, or residential or business street address of next of kin or another contact individual (for an individual who does not have a residential or business street address), or a principal place of business, local office, or other physical location (for a person other than an individual); and (iv) identification number, which will be a taxpayer identification number (for U.S. persons), or one or more of the following: a taxpayer identification number, passport number and country of issuance, alien identification card number, or number and country of issuance of any other government-issued document evidencing nationality or residence *and* bearing a photograph or other similar safeguard (for non-U.S. persons).

Based on the risk, and to the extent reasonable and practicable, you are expected to hold a reasonable belief that you know the true identity of our customers. You are not required to take steps to determine whether the document that the customer has provided for identity verification has been validly issued. You may rely on a government-issued identification as verification of a customer's identity.

Root does not open or maintain "customer accounts" within the meaning of 31 CFR 103.122(a)(1)(i), in that we do not establish formal relationships with "customers" for the purpose of effecting transactions in securities. If, in the future, Root elects to open customer accounts or to establish formal relationships with customers for the purpose of effecting transactions in securities, we will first establish, document and ensure the implementation of appropriate procedures.

III.A.2. SUSPICIOUS ACTIVITY AND REPORTING OBLIGATIONS

The detection and reporting of suspicious activity are keys to the deterrence of money laundering and terrorist activity. You are required to monitor account activity for red flags, such as unusual size, volume, pattern, or type of transactions, taking into account risk factors that are appropriate to the Root's products and services. Red flags often include inconsistencies between the customer and their desired transaction, or comments or conduct on the part of the customer. If a customer transaction appears unusual, you should ask questions and seek further information. There may be commercially reasonable explanations for the activity being undertaken by the customer or at their request. If you are still suspicious of a transaction after gathering additional information, contact the Compliance Officer and follow their instructions.

The Compliance Officer will conduct reviews of potentially suspicious activity detected by employees. The Compliance Officer may elect to file a Suspicious Activity Report ("***SAR***") with the Financial Crime Enforcement Network ("***FinCEN***"). The Compliance Officer will conduct an appropriate investigation and review relevant information from internal or third-party sources before a SAR is filed. Relevant information may include, but is not limited to, the following: banking information, source of funds verification, and business information.

You and Root are required to keep SARs and any supporting documentation confidential. Root will not inform anyone outside of FinCEN or other appropriate law enforcement or regulatory agency about a SAR. Root will refuse any subpoena requests for SARs or for information that would disclose that a SAR has been prepared or filed and immediately notify FinCEN of any such subpoena requests that we receive. Root will segregate SAR filings and copies of supporting documentation from other books and records to avoid unintentional disclosure. The Compliance Officer will handle all subpoenas or other requests for SARs.

III.B. APPOINTMENT OF AN AML COMPLIANCE OFFICER

The Compliance Officer has working knowledge of the AML and sanctions laws and is qualified by experience, knowledge, and training to serve in this capacity. The Compliance Officer is vested with responsibility and authority to maintain and enforce Root's AML Program. The duties of the Compliance Officer include, but are not limited to, monitoring the Root's compliance with AML obligations, overseeing communication, and training employees. The Compliance Officer will also ensure that Root keeps and maintains all of the required AML records and that SARs are filed with FinCEN when appropriate.

Root will develop ongoing employee training under the leadership of the Compliance Officer. Training will be based on the Root's size, customer base, and resources and be updated as necessary to reflect any new developments in the law.

Root's training program may, but is not required to, include (i) how to identify red flags and signs of money laundering that arise during the course of your duties; (ii) what to do once the risk is identified (including how, when and to whom to escalate unusual customer activity or other red flags for analysis); (iii) what employees' roles are in Root's compliance efforts and how to perform them; (4) Root's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with this policy.

III.C. IMPLEMENTATION OF AN INDEPENDENT AUDIT FUNCTION

It is Root's policy to provide for independent testing of compliance with all applicable reporting, recordkeeping, registration and program requirements of the BSA. Accordingly, an independent audit or other review may be conducted at the direction of the Compliance Officer.

If the Compliance Officer elects to conduct such a review, the audit/review responsibility will be assigned to a person who is both independent and has the experience and skill to conduct a thorough and effective independent review (the "***Reviewer(s)***"). The Reviewer(s) should be a member of Root's internal audit department, an outside auditor, or some other independent professional. The Reviewer(s) may be an employee, but in no event may the Compliance Officer serve as the Reviewer(s). You are also disqualified from serving as a Reviewer if you or your supervisor reports to a member of management with specific BSA or AML responsibilities (e.g. Compliance Officer).

Following the completion of an independent audit/review, the Reviewer(s) will issue a written report summarizing results of the audit/review and any necessary corrective action to Root's senior management.

IV. SANCTIONS COMPLIANCE GUIDELINES

The U.S. economic sanctions laws and regulations, which are administered by OFAC, impose restrictions and, in some cases, prohibitions on engaging in transactions or other dealings with or involving certain countries, entities, and individuals. Such laws apply to U.S. persons, which include U.S. companies, certain of their affiliated businesses, U.S. citizens and lawful permanent residents, wherever located, and persons actually in the United States. Under this policy, all non-U.S. subsidiaries of Root are required to comply with the U.S. economic sanctions as if they are U.S. persons.

OFAC also prohibits engaging in any transaction that "evades or avoids [or] has the purpose of evading or avoiding" the U.S. economic sanctions.

IV.A. SANCTIONED COUNTRIES

The U.S. economic sanctions generally prohibit any and all transactions or other dealings by U.S. persons with, in, involving, or relating to certain countries or territories ("***Sanctioned Countries***"). Thus, it is Root's policy that no transactions or other dealings may be undertaken, directly or indirectly, with, involving, or relating to, any Sanctioned Countries. Because these sanctions may change rapidly based on U.S. foreign policy and national security concerns, the Compliance Officer will stay abreast of sanctions developments and will alert you to any relevant changes when appropriate.[1]

IV.B. SPECIALLY DESIGNATED NATIONALS AND BLOCKED PERSONS

In addition to prohibitions on Sanctioned Countries, under the U.S. economic sanctions regime, U.S. persons generally are prohibited from engaging in business or other dealings with or involving certain nationals and residents of Sanctioned Countries, and other individuals and entities, regardless of country of nationality or residency, designated on the List of Specially Designated Nationals ("***SDNs***") and Blocked Persons ("***SDN List***").[2]

The U.S. government designates certain individuals as SDNs to address perceived threats to U.S. national security and other foreign policy goals of the United States, such as international drug trafficking, human rights violations, international terrorism, proliferation of weapons of mass destruction and certain countries' regimes or former regimes.

Note that OFAC will consider any entity 50% or more owned or controlled by one or more SDNs also to be an SDN, regardless of whether that entity has been officially included on the SDN List.

In addition to the SDN List, OFAC maintains other sanctions lists. Individuals and entities on these lists are considered Blocked Persons.[3] It is Root's policy that no transactions or dealings may be undertaken with or involving a Blocked Persons. To the extent that you become aware that a transaction may be in some way connected to a Blocked Person, even if the Blocked Person is not the beneficiary of the transaction, you must communicate this information to the Compliance Officer immediately.

IV.C. FACILITATION

U.S. economic sanctions laws and regulations also prohibit assistance of any kind, including facilitation, approval or brokering, by U.S. persons with respect to transactions with or involving Sanctioned Countries or SDNs. The term "facilitation" is construed broadly by OFAC to encompass, for example, by (i) supervising personnel; (ii) approving business plans or credit; or (iii) providing back-office services, such as information technology services. Thus, U.S. persons are prohibited from assisting in any way in a transaction with a Sanctioned Country or SDN that may be otherwise permissible for a non-U.S. person.

---

1 Sanctions developments may be monitored by signing up for OFAC press alerts or visiting the OFAC Press Center at *http://www.treasury.gov/press-center/Pages/default.aspx*.

2 The SDN List and other sanctions lists are available on OFAC's website at *http://www.treasury.gov/ofac*.

3 "Blocked Person" means (i) a Person whose name appears on the SDN List published by OFAC, (ii) a Person, entity, organization, country or regime that is blocked or a target of comprehensive sanctions that have been imposed under U.S. economic sanctions laws or (iii) a Person that is an agent, department or instrumentality of, or is otherwise beneficially owned by, controlled by or acting on behalf of, directly or indirectly, any Person, entity, organization, country or regime described in clause (i) or (ii).

Similarly, the U.S. economic sanctions generally prohibit U.S. banks or other financial or depository institutions from processing wires, checks or other payment-side transactions relating to sanctioned countries and prohibited parties, even where the underlying transaction is entirely outside the United States and no U.S. persons are otherwise involved.

IV.D. BLOCKED PROPERTY

Property and interest in property belonging to an SDN is "blocked," or effectively frozen. U.S. persons in possession or control of the property or interest in property of such persons are required to place any such property in blocked, interest-bearing accounts and report the blocked property to OFAC within 10 business days.

IV.E. SCREENING PROCEDURES

It is Root's policy that all non-U.S. parties with whom Root formally interacts or transacts be screened against the various lists of restricted parties maintained by OFAC. Such screening must be completed prior to engaging in any or transactions. If you obtain information suggesting that Root may have or has engaged in business with a Sanctioned Country, a Blocked Person or an individual or entity in anyway affiliated with a Blocked Person, you must communicate that information to the Compliance Officer immediately.[4]

V. RECORDKEEPING

Root will maintain records, including electronic records, concerning all transactions and audits that may implicate AML and economic sanctions laws and regulations. The Compliance Officer will be responsible for ensuring that any such records are maintained as required. With respect to blocked property, records must be retained for the longer of a period of five years or for as long as such property remains blocked and, once unblocked, records relating to previously blocked property must be maintained for five years.

In addition, as part of the AML Program, Root will maintain SARs and their accompanying documentation as well as documentation on customer identity and verification for a minimum of five years. Root will keep other documents according to existing BSA and other recordkeeping requirements.

VI. VIOLATIONS / CONSEQUENCES

Failure to comply with AML and sanctions laws and regulations can result in severe consequences for you and Root. For Root, such failure may result, for instance, in substantial monetary penalties, regulatory and licensing concerns as well as adverse publicity and potential criminal prosecution. Individuals who violate these laws could be liable for substantial monetary penalties and face imprisonment. Additionally, a violation of this policy will result in appropriate disciplinary action, which may include demotion, reassignment, additional training, probation, suspension, or even termination.

---

[4] For example, OFAC's SDN List often will include a full name, address, nationality, passport, tax ID or cedula number (national identity document used in many countries in Central and South America), place of birth, date of birth, former names and aliases. Note that OFAC guidance indicates that lack of an exact name, ID number or a direct date of birth match is not dispositive in determining whether a match is genuine. In determining whether information is a match to the SDN List, Root will also take care to rely only on current and complete information. If there are a number of similarities in this information, even if there is some information that does not match, consideration should be given to contacting OFAC for further advice prior to proceeding with the transaction. If necessary, the Compliance Officer will contact OFAC. The OFAC SDN Hotline number is 1-800-540-6322.

VII. STATUS

This policy does not form part of any employment contract with you and may be amended at any time. This policy should be read in conjunction with Root's other policies and procedures.

VIII. REPORTING/QUESTIONS

You have an affirmative obligation to report all violations of this policy to the Compliance Officer, who can be reached as follows:

Root, Inc.
80 E. Rich Street, Suite 500
Columbus, Ohio 43215
Attn: General Counsel

Reports of policy violations may also be submitted anonymously by using Root's hotline number 855-930-0002. However, we encourage you to consider revealing your identity so that we can properly follow up and investigate. We will not retaliate against any individual for reporting such matters in good faith.

Where a potential violation is identified, all records should be maintained regarding any such transactions and all further transactions with such individuals or entities should be stopped pending review. You should direct any questions or concerns regarding this policy or the laws and regulations cited herein to the Compliance Officer.

Each of Root's entities are principally responsible for compliance with AML and economic sanctions laws and regulations, including each entity's transactions and other dealings with customers as well as vendors and other third parties both in and outside the United States. *However, all compliance efforts and training shall be coordinated by the Compliance Officer to maintain consistency and effectiveness.*