Rimini Street

Anti-Money Laundering Policy

Amended and Approved as of February 21, 2024

Introduction

The purpose of this Global Anti-Money Laundering Policy (this "**Policy**") is to ensure that Rimini Street, Inc. and its subsidiaries and affiliates (collectively, the "**Company**"), as well all Rimini Street Personnel, comply with all applicable anti-money laundering laws and all laws countering the financing of terrorism, including, but not limited to, the U.S. Bank Secrecy Act, the PATRIOT Act, and the EU Directive on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing of 2015, as amended by Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 (AMLD V), and all similar anti-money laundering laws and laws countering the financing of terrorism in effect in the countries and jurisdictions where the Company conducts business and/or has operations (collectively "**Anti-Money Laundering Laws**"). Moreover, this Policy is also intended to ensure all Company business activities carried out with Third Parties comply with Anti-Money Laundering Laws. *Capitalized terms used but undefined herein have the meanings assigned to them under Section B (Definitions).*

It is the policy of the Company to prohibit and actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities by complying with all applicable Anti-Money Laundering Laws. The Company has adopted a zero-tolerance standard with respect to conduct that violates Anti-Money Laundering Laws. As such, the Company seeks to do business only with Third Parties that conduct legitimate activities and that are committed to follow these standards.

This Policy sets out guidelines and mechanisms designed to ensure that all Rimini Street Personnel are well informed and trained to be able to detect, mitigate, prevent and report acts and/or transactions which could involve potentially illegally obtained resources, as well as to promote compliance with applicable Anti-Money Laundering Laws and to avoid possible damages to the integrity, stability and reputation of the Company.

A. Roles and Responsibilities

The GVP and Chief Counsel, Chief Ethics and Compliance Officer (the "**Chief Ethics and Compliance Officer**") and the E&C Regional Compliance Managers have been designated as the "AML Compliance Officers" and shall oversee global compliance with this Policy and applicable Anti-Money Laundering Laws. The AML Compliance Officers are responsible for:

- Supervising the implementation of the Policy;
- Together with members of the Company's Legal Department, monitoring any changes in applicable laws and any prevalent techniques or cases related to Anti-Money Laundering Laws in order to ensure that the Policy remains effective and updated;
- Ensuring that training for Rimini Street Personnel is consistent with this Policy; and
- Providing to the Audit Committee of the Company's Board of Directors a summary report related to global compliance with this Policy at least once every year.

B. Definitions

For the purposes of this Policy, the following terms shall have the definitions set forth below:

"**AML**" refers to Anti-Money Laundering.

"**Cash Payment**" refers to, but is not limited to, remittances of cash (including coins and bank notes) or cash equivalents (including cryptocurrency), as well as payments via cashier's check, teller's check, traveler's check, money order, gift card and/or direct cash deposits, wire transfers or ACH transfers of cash to any Company bank account; notwithstanding this definition, a different definition could be established in accordance with applicable local law, as determined by the AML Compliance Officers.

"**E&C**" means the Company's Ethics & Compliance Department.

"**Rimini Street Personnel**" refers to the Company's officers, directors, employees, distributors, consultants, agents, contractors, business partners, interns and any other third-party representatives acting on the Company's behalf.

"**Third Party(ies)**" refers to any of the Company's clients, prospective clients, vendors, prospective vendors, suppliers, prospective suppliers and any other person, entity or organization with whom the Company does or may do business or from whom the Company accepts payments or remuneration.

"**Ultimate Beneficiary(ies)**" refers to any entity or person that ultimately owns or controls a Third Party and/or the entity or person on whose behalf a transaction is made. This includes any entity (company, partnership, corporation, trust or other legal structure) or any person that has, directly or indirectly, 25% ownership or greater (or, any percentage ownership lower than 25%, in accordance with applicable local law) in the Third Party, or exercises effective control over the Third Party.

C. Mechanics of Money Laundering

Money laundering is generally defined as engaging in acts designed to conceal or disguise the true origins of criminally derived proceeds so that the proceeds appear to have been derived from legitimate origins or constitute legitimate assets. Generally, money laundering occurs in three stages:

Stage One – Cash first enters the financial system at the "placement" stage, where the cash generated from criminal activities is converted into monetary instruments, such as money orders or traveler's checks, or deposited into accounts at financial institutions.

Stage Two – At the "layering" stage, the funds are transferred or moved into other accounts or other financial institutions to further separate the money from its criminal origin.

Stage Three – At the "integration" stage, the funds are reintroduced into the economy and used to purchase legitimate assets or to fund other criminal activities or legitimate businesses.

Terrorist financing may not involve the proceeds of criminal conduct, but rather an attempt to conceal either the origin of the funds or their intended use, which could be for criminal purposes. Legitimate sources of funds are a key difference between terrorist financiers and traditional criminal organizations. In addition to charitable donations, legitimate sources include foreign government sponsors, business ownership and personal employment. Although the motivation differs between traditional money launderers and terrorist financiers, the actual methods used to fund terrorist operations can be the same as or similar to methods used by other criminals to launder funds. Funding for terrorist attacks does not always require large sums of money, and the associated transactions may not be complex.

D. Due Diligence

The Company conducts appropriate due diligence checks ("**DD Checks**") on Third Parties with which the Company does business after assessing potential AML risks based on red flags. Rimini Street Personnel should be alert to suspicious behavior or "red flags" when doing business with, conducting DD Checks on, and/or monitoring continued engagement with Third Parties. **Appendix A** contains a non-exhaustive list of red flags that, if observed, should be reported to E&C. If a red flag is spotted, E&C should be notified and will investigate the red flag and take further action consistent with this Policy and all applicable Anti-Money Laundering Laws. Such an investigation may entail a thorough review of the business relationship with the Third Party and any previous transactions with the Third Party to ensure that such transactions were consistent with this Policy and the Company's knowledge of the Third Party, its commercial activity and risk profile, and, when necessary, the source of its funds.

The following steps may be taken, at the discretion of E&C, when a red flag is raised:

(i) Verifying the Third Party's identity. For individuals, this can include requesting a copy of their passport or the national identity document containing their name, date of birth, physical address, tax identification number and valid government identification, consistent with local laws. For a legal entity, this can include requesting incorporation or related documents or certificates of good standing and/or existence from an appropriate governmental agency, as well as data regarding their legal representatives, owners or board members;

(ii) Collecting from the Third Party a signed *Third Party Anti-Corruption Compliance Letter for Third Party(ies*) (Company internal document management system reference: GOV-005);

(iii) Identifying the Third Party's Ultimate Beneficiaries and verifying the Ultimate Beneficiaries against official documentation;

(iv) Confirming the Third Party's legal status by checking official and/or authenticated documents (such as copies of business licenses, tax registrations, articles of incorporation or organization, bank references, credit agency reports, or any other equivalents deemed reasonable);

(v) Identifying, in the case of a Third Party entity such as a company, partnership, trust, etc., its place(s) of operations and the identity and nationality of its shareholders, administrators, and directors, as well obtaining copies of its bylaws, articles of incorporation, or equivalent in each country in which it operates;

(vi) Obtaining any other Third Party information which is collected as a part of ordinary business practice, such as financial statements, credit agency reports, bank references, bank account information and ownership and control structure;

(vii) Screening the Third Party against relevant AML and sanctions lists. These include, but are not limited to, the OFAC SDN List, the U.S. State Department's Terrorist Exclusion List, other relevant sanctions lists in the jurisdictions in which the Company operates, and commercially available AML lists; and

(viii) Notifying the Third Party in writing of this Policy and the Third Party's obligation to comply with all applicable Anti-Money Laundering Laws.

Once the DD Check information has been collected, E&C shall determine whether the transaction or commercial relationship should proceed based on the information provided.

E. Payments

The Company shall undertake payment acceptance due diligence measures to reduce the risk of receiving monies involved in money laundering and terrorist financing activities. Third parties should be notified of the Company's acceptable forms of payment. The Company may accept a wire transfer which does not specify any bank account owner if it is legally permissible in the country where the transaction is taking place. The Company should keep a record of the Third Party's report of such wire transfer, including confirmation of the Third Party's bank account details (*i.e.*, bank name and account holder name).

Cash Payments

Rimini Street Personnel should review Cash Payments closely to look for any AML red flags outlined in **Appendix A.** Cash Payments should be legal and commercially reasonable in consideration of local business practices and with respect to the Third Party. The Cash Payment should be made in compliance with any notification and record keeping requirements of applicable local laws and regulations, and the Cash Payment should not be made in such a way that it appears intended to circumvent such requirements.

F. Reporting Requirements

If you become aware of any known or suspected violation of applicable Anti-Money Laundering Laws or this Policy, you should immediately report the situation to E&C at Ethics@riministreet.com. Any manager or Human Resources representative who receives a report of a potential violation of this Policy or the law must immediately inform E&C.

You can also ask questions, raise concerns, or make reports of suspected compliance violations by contacting the Rimini Street Compliance Helpline:

- By phone using a special toll-free telephone number based on the country from which you are calling. In the United States, call 844-754-3342. For a list of international country phone numbers, see our Compliance Helpline section at https://www.riministreet.com/company/ethics-and-compliance/; or
- By web available at https://riministreet.i-sight.com/portal

The Rimini Street Compliance Helpline is managed by an outside company and is available 24 hours a day, seven days a week. Where allowed by local law, you may make an anonymous report to the Compliance Helpline.

You may also raise the matter directly with the Chair of the Audit Committee of the Company's Board of Directors at:

Jack Acosta, Chair, Audit Committee audit@riministreet.com

Reports should be factual instead of speculative or conclusory and should contain as much specific information as possible to allow the persons investigating the report to adequately assess the nature, extent, and urgency of the investigation.

The Company will not permit retaliation of any kind against anyone who makes a report or complaint in good faith with a reasonable basis for believing that a violation of this Policy or other illegal, unethical, or inappropriate conduct has occurred.

The Company encourages and highly values such good faith reporting of potential conduct that may violate Anti-Money Laundering Laws or this Policy.

G. Consequences of Non-Compliance

Violations of any applicable Anti-Money Laundering Laws or this Policy may result in criminal prosecution and/or the imposition of civil sanctions, not to mention potential long-term harm to the Company's reputation. Under no circumstances shall any Rimini Street Personnel facilitate or participate in any money laundering or terrorist financing activity. The Company will not pay any fine imposed on any Rimini Street Personnel or any Third Party and will not indemnify or reimburse any Rimini Street Personnel or any Third Party for any attorney´s fees and/or costs incurred as a result of a breach of any Anti-Money Laundering Laws or this Policy. In addition, any breach of this Policy or any Anti-Money Laundering Laws may result in disciplinary action, including possible termination of employment, clawback/recoupment of bonuses or other incentive-based compensation, or such other remedial or disciplinary action as shall be appropriate under the circumstances, in accordance with applicable law. Conversely, the Company will fully support any Rimini Street Personnel or Third Parties who decline to engage in conduct that would place the Company's ethical principles and reputation at risk.

H. Amendments

Any changes or amendments to this Policy must be approved by the Company's Board of Directors with the exception of non-substantive changes/amendments to update (i) the titles of any executive officer or member of senior management identified by title herein, (ii) the name of any regulatory agency identified herein or (iii) any United States Federal or any international statute (or rules or regulations promulgated thereunder) referenced herein, which changes/amendments may

be approved by the Company's President and Chief Executive Officer upon the recommendation of the Chief Ethics and Compliance Officer.

Appendix A

Non-Exhaustive List of AML Red Flags

1. The Third Party shows unwillingness to provide identification documents, or any other data requested during the DD Check, or such information is incomplete, wrong or misleading;
2. The Third Party uses a false address;
3. The Third Party displays expired identification;
4. The Third Party provides inconsistent information;
5. The Third Party has complex shareholding structures which are not reasonably justified;
6. The Third Party's operations drastically change over time in volume or amount;
7. The Third Party shows unusual concerns related to the disclosure of any such data requested, particularly regarding its identity and type of business;
8. The Third Party unreasonably questions the requirements of documentation and handling of information;
9. The Third Party's financial information reflects asset concentration in subsidiaries or affiliates where there is an absence of audited financial statements;
10. The Third Party refuses to provide information regarding its subsidiaries and affiliates, if and when requested;
11. The Third Party has multiple accounts under the same name for no apparent purpose;
12. The Third Party, including any individual associated therewith, or any of its subsidiaries or affiliates has a negative background, such as criminal records, civil penalties of any kind, or investigations regarding tax fraud, money laundering activities, and/or organized crime;
13. The Third Party, or one of its owners or board members, is on OFAC's List of Specially Designated Nations and Blocked Persons;
14. The Third Party, or one of its owners or board members, is on the U.S. State Department's Terrorist Exclusion List;
15. The Third Party refuses to or is unable to identify a legitimate source of its funds;
16. The Third Party transacts with important public figures, such as public officials or other politically exposed persons;
17. The Third-Party attempts to send or receive a payment in cash, or cash equivalents, which are not commercially reasonable in considering of local business practices and with respect to the Third Party;
18. The Third Party makes payments through the accounts of different individuals or entities rather than through its own accounts;
19. The Third Party's payments are conducted through a credit institution of different nationality than that of the Third Party;
20. The Third Party frequently engages in transactions where payments equal the maximum amount allowed for withdrawals at financial institutions;
21. The Third Party seeks to bribe, threaten or persuade Rimini Street Personnel to avoid any obligation related to this Policy or Anti-Money Laundering Laws;
22. There are deposits in foreign currency made by multiple individuals for the same transaction;
23. The Third Party requests unjustifiably high or low prices for products or services which are not within market standards;
24. The Third Party requests or ensures that goods are transported through more than one jurisdiction for no apparent reason;
25. The Third Party frequently changes its payment instructions;

26. The Third Party requests or proposes excessive modifications to letters of credit or similar documents;
27. The Third Party provides false invoices or invoices with miscellaneous charges that have not been previously approved by the Company;
28. The Third Party makes an unusually large amount of overpayment or requests a refund to be sent to an unknown Third Party as a result of a cancelled purchase order;
29. The Third Party's representative seems not to know basic facts about the Third Party's business, which raises suspicion as to whether he or she is actually employed by the Third Party;
30. The Third Party requests the Company to issue an invoice which does not accurately reflect an invoiced price or other material terms of the transaction;
31. The Third Party structures a transaction to circumvent the notification requirements of authorities or governments, for example, by paying one invoice with numerous money orders or cashiers' checks in amounts under the notification requirements; or
32. The Third Party has a broker, attorney, or other agent to facilitate the transaction, which is unusual for the type of business, and the Company has no proper information or documentation regarding such agent or such agent's authority.