VERRA

SANCTIONS AND ANTI-MONEY LAUNDERING COMPLIANCE POLICY

AUGUST 2023

CONTENTS

SANCTIONS AND ANTI-MONEY LAUNDERING COMPLIANCE POLICY

1. Statement of Policy

This Sanctions and Anti-Money Laundering Compliance Policy ("Policy") affirms that Verra complies with all economic sanctions and anti-money laundering (AML) and counter-terrorist financing (CFT) laws, rules, and regulations/CFT laws (collectively, the "AML/CFT laws") applicable to it in the United States and other relevant jurisdictions.

Without limiting the generality of the foregoing, Verra will ensure that it and its employees, as well as any third parties acting on its behalf, do not engage with entities—including without limitation all vendors, contractors, sub-contractors, project proponents, Verra Registry users, and validation/verification bodies—who are targets of applicable economic sanctions measures, including those measures implemented and enforced by the US Department of the Treasury's Office of Foreign Assets Control ("OFAC"), or who may seek to use legitimate business activities with Verra as a means to facilitate money laundering or terrorism financing activities or otherwise engage in transactions with Verra involving criminal proceeds.

2. Applicability and Scope

This Policy applies to all activities of Verra worldwide.

The Policy applies to Verra and its employees, as well as any third parties acting on its behalf.

3. Policy Administration

Responsibility for compliance with this Policy is the duty of individuals at every level of the organization. The Chief Executive Officer of Verra shall designate a Verra employee ("Responsible Officer") to administer this Policy. The duties of the Responsible Officer include without limitation familiarizing Verra employees and third parties acting on Verra's behalf with this Policy, providing compliance training, implementing internal controls designed to detect and prevent violations of applicable AML/CFT laws, managing and assessing sanctions screening and third-party due diligence, and conducting other compliance-related activities as needed based on identified risks.

The Responsible Officer shall have an adequate level of autonomy from other management and shall be given sufficient resources and authority to carry out this responsibility.

4. Context

Although Verra is not a "financial institution" for the purposes of the United States Bank Secrecy Act ("BSA") and related AML/CFT laws, and accordingly is not required by these laws to establish or maintain a written anti-money laundering program, Verra recognizes that certain BSA requirements apply to all US businesses and that it has an important role in minimizing the risks to the United States of money laundering, terrorist financing, and other criminal activities. Verra, therefore, adopts this Policy on a voluntary basis except with respect to Sections 12, 13, and 14.

4.1. Sanctions

Economic sanctions measures implemented by OFAC and other US government agencies generally restrict dealings by Verra and its employees, as well as third parties acting on its behalf, in or relating to:

a. Jurisdictions that are subjects of comprehensive US economic sanctions or are subjects of targeted US economic sanctions as set out in Appendix 1 of this Policy (each, a "Sanctioned Jurisdiction"); and
b. Individuals and entities who have been named on OFAC's list of Specially Designated Nationals and Blocked Persons (the "SDN List").

These restrictions extend to dealings with entities that are 50 percent or more owned directly or indirectly by one or more parties identified on the SDN List.

Additionally, the sanctions authorities of other countries where Verra conducts activities, such as the member states of the European Union and the United Kingdom, may enforce their own lists of restricted entities and individuals. (Restricted parties under US, EU, UK, and other applicable sanctions regimes are referred to collectively as "Sanctioned Persons" in this Policy.)

Violations of US economic sanctions measures can result in civil and criminal liability for Verra and its employees, as well as third parties acting on its behalf.

4.2. 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 derived from legitimate origins or constitute legitimate assets. Terrorist financing provides funds for terrorist activities and may involve funds raised from legitimate sources and legitimate activities (e.g., investments in carbon credits).

Furthermore, in light of heightened scrutiny of financial institutions by regulatory and law enforcement authorities in the area of AML/CFT compliance, it is critical that Verra does not engage with entities that could cause financial institutions with which Verra partners to question the integrity and legality of the

transactional activity in Verra's accounts, thus jeopardizing Verra's critical relationships with those financial institutions.

Dealings, including otherwise legitimate dealings, with entities engaged in money laundering or terrorist financing can expose Verra and its employees, as well as third parties acting on its behalf, to liability under various US statutes, including criminal money laundering statutes.

5. Third-Party Identification and Due Diligence

Verra shall determine and verify the identity of each third party with which it engages, including without limitation all vendors, contractors, sub-contractors, project proponents, Verra Registry users, and validation/verification bodies.

5.1. Prohibited Third Parties

Verra shall not engage with any of the following third parties:

- Any Sanctioned Person;
- Any person from a Sanctioned Jurisdiction or regime, including anyone in or normally resident in a Sanctioned Jurisdiction, companies headquartered in a Sanctioned Jurisdiction, or the governments of a Sanctioned Jurisdiction;
- Any person who resides in or is a citizen of any nation on the Financial Action Task Force ("FATF") list of non-cooperative jurisdictions;
- Any person who resides in a jurisdiction identified by FATF as requiring countermeasures or enhanced due diligence; or
- Any politically exposed person ("PEP") or a family member or associate of a PEP.

5.2. Third-Party Due Diligence

Verra shall perform reasonable risk-based due diligence on third parties.

Verra is dedicated to ensuring that it engages only with third parties that are not subject to applicable sanctions laws, rules, or regulations.

In order to mitigate risks of engaging with economic sanctions targets, including Sanctioned Persons or those who are located in restricted jurisdictions, and parties engaged in money laundering and terrorist financing activities, it is the policy of Verra to:

i. conduct diligence on all third parties with whom Verra transacts to identify third parties who may be US sanctions targets or engaged in illegal activity or who otherwise expose Verra to increased money laundering and terrorism financing risk; and

ii. monitor transactions between Verra and its third parties to identify transactions that could pose heightened sanctions or AML/CFT compliance risk.

5.3. Third-Party Transaction Monitoring

It is the responsibility of all Verra employees to alert the Responsible Officer any time when they observe or learn of conduct by a third party suggesting that the third party is engaged in activities in or relating to a jurisdiction subject to comprehensive sanctions or otherwise engaged in illicit activity. This includes observations of payment-related activity that appears suspicious or raises a red flag.

Upon escalation of behavior by a third party that is indicative of potential illicit activity (e.g., negative news suggesting the third party's involvement in illegal activity or activities that may violate sanctions), the Responsible Officer will work with the Verra employee who manages Verra's relationship with the third party at issue, along with external counsel as appropriate, to determine an appropriate course of action with respect to the third party. In circumstances where the third party at issue is not able to adequately explain the information or observed activity, an appropriate course of action could be to terminate Verra's relationship with the third party.

In the case of payment-related activity suggestive of money laundering or other criminal activity that gives rise to an escalation to the Responsible Officer, the Verra employee who manages the relationship with the third party will work with the Responsible Officer to obtain an explanation from the third party as to the business rationale for the payment at issue. If the third party cannot provide a business rationale for the payment at issue, the third party will be instructed to cease such payment activity in the future, in a circumstance where the payment has already been received into a Verra account. If Verra has not yet received the payment into a Verra account and a legitimate business rationale is not provided by the third party, Verra may refuse to accept the payment in the manner described and direct the third party to make the payment in a more transparent way.

Under no circumstance will Verra accept a payment from or make a payment to a party, other than the third party with which Verra has a business relationship, without an acceptable explanation from the third party as to the business purpose or rationale for the alternate payment method. Such rationale should be documented and retained.

6. Mandatory Awareness of AML/CFT "Red Flags"

Verra employees must be vigilant for risk factors or "red flags" that may increase the likelihood of a violation of this Policy and/or applicable laws. Red flags can generally relate to and involve a combination of unusual or unconnected sources and recipients of funds; unusual or non-transparent transactions and instructions; unusual and suspicious behaviors and counterparties; and transactions associated with higher-risk jurisdictions, including jurisdictions subject to US, EU, or UK sanctions regimes.

The following is a non-exhaustive list of red flags relating to payment activity, the observance of which should trigger an escalation to the Responsible Officer for further review and analysis as described above:

Unusual or unconnected sources and recipients of funds:

1. unexplained third-party payment from a source other than the third party owing money to Verra;
2. request by a third party to whom Verra owes money that funds be transmitted to an account with no apparent connection to the third party;
3. multiple payments from a third party via multiple entities in connection with a single invoice;

Unusual or non-transparent transactions and instructions:

4. payments in currency (e.g., cash or cash equivalents, which can be a means of limiting the ability of financial institutions or authorities from monitoring transactions);
5. inbound offshore payments from accounts located in countries other than where the third party operates or resides;
6. request from a third party for a non-standard deal structure with no apparent business or economic purpose;
7. lack of transparency about the ownership of assets or entities (e.g., inability or unwillingness to produce official proof of beneficial ownership, use of nominee shareholders or bearer shares, or other complex and non-transparent ownership structure), or when beneficial owners are identified as PEPs or government officials;
8. use of a shell company, offshore company, third parties or other intermediaries, or a P.O. Box;

Unusual and suspicious behaviors and counterparties:

9. third parties who have a poor reputation for business ethics or appear to lack integrity in their operations;
10. suspicious activity of any nature, including, for example:
    - large or frequent credits, refunds, or overpayments—this technique, known as "round-tripping," cycles money through a legitimate business to disguise its source. For example: A large deposit is made that is soon canceled, even with a penalty being deducted. The balance is refunded in "clean" money. Similarly, intentionally overpaying an invoice to receive a refund in "clean" money is a red flag.
    - "structuring," which is a form of distancing proceeds of crime from their criminal sources by breaking large payments into multiple small transactions (sometimes by different people or entities) to avoid financial controls (e.g., many small incoming wire transfers or deposits being made in a manner inconsistent with the third party's business operations and/or past practices).

11. situations where a third party:
    - provides false, misleading, or substantially incorrect information about its identity, sources of funds, ownership, and/or operations;
    - enters into transactions that do not appear to make commercial sense or departs from the usual form of business; and/or
    - raises concerns about Verra's Sanctions and Anti-Money Laundering Compliance Policy, refuses to respond to reasonable due diligence requests, or questions Verra's related procedures designed to ensure compliance.

12. transactions associated with higher-risk jurisdictions, including jurisdictions subject to sanctions payments involving jurisdictions that have been deemed to be of money laundering concern by the US government or international body (e.g., FATF) or are considered restricted under US economic sanctions laws;
13. transactions that involve banking in non-transparent, high-intensity financial crime jurisdictions or countries known to pose a high risk of money laundering or terrorist financing. For a list of countries by risk level, consult the following website: https://index.baselgovernance.org/map.

7. Contractual Provisions

It is the policy of Verra to require each third party with which it enters into a contractual agreement to make the following contractual representations:

- that it is not a target of US sanctions (i.e., a person or entity on the SDN List, owned by a Sanctioned Person, or organized or located in a jurisdiction that is a target of comprehensive US sanctions);
- that it, to the best of its knowledge and belief, complies with the laws and regulations applicable to the third party in the jurisdictions in which it operates; and
- that any payments made by the third party to Verra will not involve the proceeds of crime.

Verra employees who manage relationships with third parties are responsible for ensuring inclusion of the representations described above in all agreements with third parties.

8. Risk Assessment

It is the policy of Verra to conduct a sanctions and AML/CFT risk assessment on a periodic basis to identify changes to Verra's sanctions and AML/CFT compliance risk profile. The results of this periodic risk assessment will inform changes to Verra's sanctions and AML/CFT compliance program and this Policy as necessary.

In assessing the sanctions and AML/CFT risks posed by its business, Verra will identify the specific risk categories unique to Verra, taking into account its products, services, third parties, and the geographic locations of its third parties.

In addition, Verra shall perform a sanctions and AML/CFT risk assessment whenever there is (a) a material change in products, services, or practices within Verra; (b) a merger or acquisition involving the products, services, or business of Verra; (c) industry information, trends, or alerts that are relevant to the products, services, or practices of Verra; or (d) changes in national AML and counter-terrorism priorities as announced by the Financial Crimes Enforcement Network ("FinCEN").

9. Training

It is the policy of Verra to provide appropriate levels of training on sanctions compliance and AML/CFT risks associated with Verra's business, as well as on the requirements of this Policy, to employees and Board members. Training will be provided on a periodic basis to, at a minimum, employees who manage relationships with third parties and employees who manage receipt of payments from third parties.

10. Periodic Testing and Auditing

Compliance with this Policy by Verra employees will be verified through periodic testing and auditing as part of Verra's standard audit cycle. This compliance testing and review shall be proportionate to the level of identified risk and may employ such tools as performance reviews, compliance interviews, completion of questionnaires, renewed certifications, forensic audits, and/or other commercially reasonable actions to be determined by the Responsible Officer in consultation with Internal Audit and/or outside advisors as needed.

11. Reporting Obligations

If any sanctions or AML/CFT red flags are identified, they must be further investigated and resolved through consultation with the Responsible Officer. Compliance with this Policy requires that Verra employees err on the side of caution and discuss or report any actual or potential red flags that may arise.

While Verra will make every effort to provide compliance information and to respond to all inquiries, no policy or procedure, however comprehensive, can anticipate every situation that may present compliance issues. Consequently, Verra depends on its employees to be responsible for compliance with the Policy, including the duty to seek guidance from the Responsible Officer whenever any aspect of the Policy is in doubt and to report to the Responsible Officer any facts or circumstances that suggest a past or ongoing violation of this Policy by any officers, directors, employee, agents, consultants, or other third parties doing business with or on behalf of Verra.

Verra absolutely prohibits retaliation of any type or kind against any person who raises in good faith any questions or concerns, reports an actual or potential violation, or assists in an investigation under this Policy.

12. Complying with Legal Process

It is possible that Verra will be served with legal process or receive other written or oral requests for information from law enforcement and other government authorities in the normal course of business. It is Verra's policy to comply with each lawful request in a timely fashion and to otherwise cooperate fully with law enforcement and other government agencies within the confines of applicable federal, state, and local laws and regulations. If served with legal process, the following procedures must be followed by all Verra personnel.

If Verra is served with a subpoena, summons, search warrant, or other legal process, or if a government agency otherwise requests information or documents involving the BSA, money laundering, or terrorist activity, the matter must be referred immediately to the Responsible Officer, who will coordinate with outside counsel as necessary in responding to legal process or other requests received from law enforcement or other government authorities or otherwise communicate with law enforcement officials or other government authorities with respect to criminal and other legal matters related to the BSA, the money laundering and anti-terrorism statutes, and related criminal matters.

All Verra employees shall respond in a timely fashion to each request for assistance from the Responsible Officer. Verra will respond to each lawful request received from a law enforcement official or other government agency within the time period specified in the request unless the time period has been extended in writing.

13. Reports of Currency Payments Over $10,000 (FORM 8300)

The BSA requires each person engaged in a trade or business who, in the course of that trade or business, receives "currency" in excess of $10,000 in one transaction (or in two or more related transactions) to file a Report of Cash Payments Over $10,000 Received in a Trade or Business, on IRS Form 8300 ("Form 8300"). While currency transactions very rarely occur in Verra's business, Verra will comply with the Form 8300 filing requirements when applicable.

14. Additional Record Keeping and Filing Requirements

14.1. Foreign Bank and Financial Accounts Reporting ("FBAR")

If Verra acquires a financial interest in or signatory authority over a foreign bank account, securities, or other financial account, Verra will file an FBAR on or before June 30 of the year

following the reportable year. A financial interest includes the owner of record or holder of legal title.

14.2. International Transportation of Currency or Monetary Instruments Reporting ("CMIR")

If Verra physically transports currency or other monetary instruments in an aggregate amount exceeding $10,000 at one time from the United States to any place outside the United States, or into the United States from any place outside the United States, Verra shall make a report thereof. Verra need not report if Verra mails or ships such through the postal service or by common carrier. Verra does not intend to conduct such transactions, but any Verra employees aware of this type of transaction occurring must disclose the transaction to the Responsible Officer to ensure timely reports.

15. Penalties and Disciplinary Actions

All Verra employees, as well as third parties conducting business on Verra's behalf, should be aware that conduct violating this Policy is always considered outside the scope of employment and/or in violation of the terms of any relationship with Verra. Any Verra employee who violates the applicable sanctions or AML/CFT laws, this Policy, or any related policies or procedures will be subject to appropriate disciplinary action, up to and including termination. Any third party conducting business on behalf of Verra may have its contractual relationship with Verra terminated and/or may be the subject of a civil claim by Verra.
In addition, Verra may choose or be required to report violations to law enforcement or other regulatory agencies, and individuals may be held personally accountable under the applicable laws.

Appendix 1: List of Sanctioned Jurisdictions

The authoritative list of Sanctioned Jurisdictions is maintained and updated by the US Department of the Treasury's Office of Foreign Assets Control.

For ease of reference only, listed below are the jurisdictions that are:

1) The subject of comprehensive US economic sanctions as of the date of publication:

   - Cuba
   - Iran
   - North Korea
   - Syria
   - The following regions of Ukraine: Crimea, Donetsk, Luhansk

2) The subject of targeted US economic sanctions relevant to this Policy as of the date of publication:

   - Russia
   - Venezuela

Verra and its employees, as well as any entities acting on its behalf, must not engage in any activity in a jurisdiction, or with any national or entity of a jurisdiction, that is the subject of comprehensive US economic sanctions, and must contact the Responsible Officer before engaging in any activity in a jurisdiction, or with any national or entity of a jurisdiction, that is the subject of targeted US economic sanctions.