empirium

Empirium Sanctions and AML Compliance Policy

1. Scope and Purpose

Empirium (the "Company") is committed to full compliance with the sanctions rules and regulations administered by the Department of the Treasury Office of Foreign Assets Control ("OFAC") and other sanctions laws that apply to the company. The Company is committed to combatting money laundering, terrorist financing, fraud, and other financial crimes (collectively, "Money Laundering"). This Sanctions and Anti-Money Laundering ("AML") Compliance Policy (the "Policy") establishes the procedures, standards, and controls that all employees, contractors, vendors, and stakeholders (each a "Covered Party") must follow to prevent, detect, and mitigate risks under AML and sanctions laws. This Policy applies across all product offerings.

The purpose of this Policy is to inform all Covered Parties of their and Empirium's obligations and ensure compliance with sanctions and AML laws. It aims to safeguard Empirium's interests by establishing measures to manage and mitigate sanctions and AML risks. The Policy is issued by Empirium's senior management and reflects our commitment to a culture of compliance that ensures accountability and transparency. Failure to comply with sanctions and AML laws could result in criminal and civil penalties for Empirium and any person involved with a violation, including significant fines and imprisonment. In addition, Empirium could suffer reputational harm, loss of revenue, or other commercial implications for violations of these laws. Any Covered Party who fails to comply with this Policy may be subject to discipline, up to and including termination of their relationship with Empirium.

For any questions about this Policy, its requirements, or how sanctions or AML laws apply to Empirium, contact our COO, Calum Belden at calum@empirium.co.

2. Sanctions Laws

a. Regulatory Background

This Policy and Empirium's supporting procedures are designed to ensure our compliance with applicable sanctions laws. Sanctions are a tool to deter activities that are contrary to foreign policy or national security objectives. As of the effective date of this Policy, Empirium is subject to U.S. sanctions laws and complies with applicable laws in the jurisdictions in which it operates.

OFAC is the primary U.S. government agency responsible for administering and enforcing economic and trade sanctions based on U.S. foreign policy and national security goals. OFAC administers a wide range of sanctions programs, which target specific territories, entities, and individuals. This policy provides a summary of sanctions restrictions applicable to Empirium. A full list of OFAC's sanctions programs is available at https://ofac.treasury.gov/sanctions-programs-and-country-information.

b. Embargoed Regions & Sanctioned Jurisdictions

Empirium is prohibited from engaging in any transaction or business dealings involving persons in, ordinarily resident in, or incorporated in comprehensively embargoed regions. Those regions are currently Cuba, Iran, North Korea, Syria, and the Crimea (including Sevastopol), Luhansk People's Republic, and Donetsk People's Republic regions of Ukraine. In general, all business dealings – both direct and indirect – involving these "embargoed regions" are prohibited.

It is Empirium's policy to not do any business, directly or indirectly, with persons in, ordinarily resident in, or incorporated in embargoed regions without required authorization from the U.S. government or other applicable authority.

At present, Venezuela, Belarus and Russia are also subject to extensive U.S. sanctions that may limit Empirium's ability to do business in or with those countries. In this Policy, the term "sanctioned jurisdictions" refers to Venezuela, Belarus, Russia, and the embargoed regions listed above.

c. Sanctioned Persons

Individuals and entities involved in nefarious activities are added to sanctions lists published by various government authorities. Different sanctions lists impose varying restrictions, from complete bans on business to more limited restrictions.

Sanctioned persons include those listed on OFAC's List of Specially Designated Nationals and Blocked Persons ("SDN List"), among others. Individuals, entities, digital currency addresses, bank account numbers, and addresses are included on the SDN List (collectively referred to as "SDNs"). The property and interests in property of an SDN in the possession or control of Empirium must be formally "blocked" or frozen and reported to OFAC. The EU, UK, and other jurisdictions maintain similar "asset freeze" sanctions. OFAC also maintains more limited "sectoral" sanctions that prohibit certain types of dealings or transactions with the sanctioned party.

OFAC sanctions laws also apply to entities that are owned, 50 percent or more, directly or indirectly, by one or more SDNs. Under EU and UK rules, entities may also be subject to similar asset freeze sanctions if they are otherwise controlled by one or more sanctioned persons.

In addition to those applied to SDNs, OFAC also imposes blocking sanctions on the governments of Cuba, Iran, North Korea, Syria, and Venezuela. These sanctions flow down to all entities owned or controlled by the sanctioned government, and any person acting on the sanctioned government's behalf, such as government officials. Cuban nationals are also technically subject to blocking sanctions, but exceptions often apply for Cuban nationals outside of Cuba.

It is Empirium's policy to not conduct any business, directly or indirectly, with persons or property subject to U.S. blocking sanctions or other applicable sanctions laws without required authorization from the U.S. government and other applicable authorities.

d. Restricted Activities and Sanctioned Services

Some sanctions prohibit Empirium from conducting certain types of transactions, such as making new investments and providing a variety of services to Russia, including accounting, corporate/trust formation, business consulting, engineering, IT consultancy and design services, cloud-based services and IT support services for enterprise management and design and manufacturing software, among other prohibited transactions.

It is Empirium's policy to not conduct any business involving a restricted activity without authorization from the U.S. government and other applicable authorities.

e. Facilitation

Empirium and all Covered Persons are prohibited from "facilitating" or assisting a non-U.S. person with any transaction or business involving a sanctioned jurisdiction, sanctioned party, or restricted activity if we would be prohibited from engaging in that business activity directly ourselves. For example, an Empirium employee may not refer a business inquiry from Iran to a friend at a European company. The referral activity would impermissibly support or "facilitate" trade with Iran, which is broadly illegal under the U.S. law.

f. Blocking, Rejecting, and Reporting

OFAC's blocking sanctions broadly prohibit transactions and business dealings with specified individuals and entities and require the freezing of their property or interests in property in the control or possession of a U.S. person. Note that "property" and property interest are defined very broadly and include fiat currency (e.g., U.S. dollars), virtual currency, services of any nature, contracts of any nature, and any other property, real, personal, or mixed, tangible or intangible, or interests therein, present, future, or contingent, among other forms of property.

The "blocking" of property and interests in property means that the property must be formally frozen and may not be further dealt in, transferred, or modified in any way. In addition to these restrictions, certain types of property must be moved into a segregated, interest bearing account at a U.S. financial institution. To the extent that blocked property comes within the possession or control of Empirium, we shall handle the property in accordance with OFAC's requirements and shall not transfer or otherwise deal in such property except pursuant to an OFAC authorization or when the legal prohibition requiring blocking no longer applies.

Blocking actions must be reported to OFAC within 10 business days and all blocked property held by a U.S. person must be reported to OFAC on an annual basis thereafter by September 30th, so long as the property remains blocked.

We must formally "reject" transactions that are impermissible under U.S. sanctions laws, but where there is no blockable interest in the transaction (e.g., in cases where an SDN or blocked party are not involved), and report such transactions to OFAC within 10 business days. In the context of a funds transfer, a rejection involves returning the funds to the originator.

3. AML Laws

The Currency and Foreign Transactions Reporting Act of 1970, as amended, inter alia, by The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "PATRIOT Act") (which legislative framework is referred to herein as the "Bank Secrecy Act" or "BSA"), requires financial institutions, including money services businesses ("MSBs"), to help the government detect and prevent Money Laundering. The BSA requires financial institutions to take a number of precautions to guard against financial crime, including the establishment of AML programs and the filing of reports that have been determined to have a high degree of usefulness in criminal, tax, and regulatory investigations and proceedings, and certain intelligence and counter-terrorism matters.

The Financial Crimes Enforcement Network ("*FinCEN*"), a bureau of the United States Department of the Treasury, administers and issues regulations pursuant to the BSA and implements and enforces compliance with the BSA and associated regulations. Pursuant to FinCEN administrative guidance, the Company is not a financial institution or an MSB. Therefore, the Company does not need to meet the more stringent reporting and compliance obligations of an MSB.

Nevertheless, the Company is committed to guarding against the use of its platform for Money Laundering. The Company conducts know-your-customer diligence, as described in this Policy, to verify the identity of its users and check for red flags. A list of key AML red flags is attached to this policy as Exhibit A.

4. Compliance Controls and Procedures

Among others, Empirium implements the internal controls and screening procedures described below to ensure compliance with sanctions laws. Empirium will use all information that it collects about the identity and location of customers and end users to identify and decline business with persons subject to U.S. or other applicable sanctions restrictions without required government authorization.

Additional information about OFAC expectations for compliance can be found on OFAC's website, in the agency's Framework for OFAC Compliance Commitments.

a. Prohibited Countries, Regions, and Entities

As a matter of company policy, Empirium prohibits all business and interactions with persons in, ordinarily resident in, or incorporated in an embargoed region, which currently consist of: Cuba, Iran, North Korea, Syria, and the embargoed regions of Crimea (including Sevastopol), Donetsk,

and Luhansk in Ukraine and with parties subject to blocking sanctions (including the Venezuelan government) without required government authorization. These restrictions apply equally to direct dealings (e.g., Empirium subscribers) and to all parties to the transactions that Empirium's platform is used to facilitate. As described in more detail below, Empirium maintains tailored controls to address the sanctions risks associated with Venezuela, Belarus, and Russia as well.

b. IP Address Geolocation Blocking

Empirium uses geoblocking (or 'geofencing') software to prohibit access to our platform from IP addresses associated with embargoed regions, which are currently:

- Cuba,
- Iran,
- North Korea,
- Syria, and
- The Crimea (including Sevastopol), Donetsk, and Luhansk regions of Ukraine.

Empirium also maintains a geoblock against IP addresses associated with Belarus and Russia given the extensive sanctions applicable to both countries.

Empirium shall ensure that all points of access to our platform are subject to the geoblock and that the geoblock is regularly tested to ensure effectiveness.

c. VPN Use and Compliance

VPNs are a common tool to preserve privacy when accessing the internet and online services. However, if Empirium becomes aware of VPN use or other actions by customers or users to circumvent sanctions, we are obligated to act. Employees are required to report any suspected circumvention via VPN to the COO or Legal Department. Known or suspected circumvention attempts will be reviewed, and action may include suspending specific users or accounts, imposing additional restrictions, or conducting further verification.

5. Customer and Business Partner Controls

Empirium screens customers, users, and other business partner entities against applicable sanctions lists, including the SDN List and for potential affiliation with sanctioned jurisdictions. Empirium uses all available information about the customer, user, or other business partner to conduct screening. For example, to the extent collected, we will use name, address(es), tax identification numbers, website and email addresses, and phone numbers as part of our sanctions screening due diligence. Such screening occurs prior to gaining access to Empirium's platform as part of customer and supplier onboarding. The screening is conducted through the Trulioo software platform. Trulioo's screening platform conducts rescreening on an ongoing basis thereafter.

Empirium also conducts additional manual know-your-customer diligence as part of its AML procedures. This process includes collecting business identification information from entities as well as individual identification information from users. Empirium conducts heightened diligence as warranted, such as through use of Dun and Bradstreet and other KYC tools.

Pursuant to Empirium policy, we will not establish a new customer or business relationship with any party subject to U.S. or other applicable sanctions. Any existing relationships that generate a reliable match to a sanctioned party, such as an SDN, or with a sanctioned jurisdiction will be placed on hold and referred to the COO for review. No transactions or other business dealings with such a party may occur except as authorized by the COO or their delegate and then only in strict accordance with applicable law.

Our written agreements with customers and other business partners shall contain appropriate sanctions compliance clauses designed to ensure compliance with U.S. and other applicable sanctions laws, and to limit sanctions compliance risks to Empirium.

6. Training and Reporting Obligations

Empirium will provide an annual training module on OFAC compliance for all employees and contractors, covering sanctions basics, reporting obligations, the identification and handling of VPN circumvention attempts, and the correct protocols for interacting with users associated with sanctioned jurisdictions. Employees must acknowledge completion and understanding of this Policy upon finishing the training.

Employees are reminded of their responsibility to report any known or suspected violation of this Policy and any suspicious activity, including VPN use intended to bypass sanctions, directly to the COO or the Legal Department. All such reports will be confidentially reviewed to ensure compliance with this Policy and prevent any potential OFAC violations.

7. Recordkeeping

All records related to sanctions and AML compliance will be securely maintained, including any suspended users, sanctions screening results, KYC reports, reports of suspected circumvention, actions taken in response, and communications with developers or customers regarding sanctions compliance, for at least ten years since the date of the underlying transaction or event.

The COO is responsible for maintaining records related to all screening escalations and any decisions made in relation to specific customers, third parties, or other counterparties with respect to sanctions laws, this Policy, and related procedures. The COO will also maintain records relating to the management of this Policy and will make those records readily available for inspection if needed.

8. Audit Protocols, Risk Assessments, and Testing

Empirium will conduct periodic audits to ensure adherence to this Policy, with any identified gaps addressed promptly to enhance our compliance framework.

Empirium will conduct periodic risk assessments of this Policy to ensure that its procedures are appropriately designed to address the sanctions and AML risks we face and applicable regulations as those evolve over time. The risk assessments will be conducted by the COO or their delegate and results of any proposed enhancements to this Policy resulting from the assessment will subsequently be presented to the Empirium senior management team.

Empirium will also conduct sanctions and other trade-related risk assessments as part of any merger or acquisition processes and ensure that acquired entities are integrated into this Policy.

9. Policy Review and Updates

This Policy will be reviewed annually by the COO to ensure it remains aligned with current regulations and industry best practices. The Policy may also be updated as necessary to address regulatory or operational changes.

While the COO is responsible for maintenance and implementation of this Policy, all employees play an essential role by ensuring that we adhere to our compliance obligations and by identifying and reporting to the COO areas of potential non-compliance. Processes will be adapted over time to account for changes to our business and sanctions laws.

Exhibit A: Examples of Possible Money Laundering "Red Flags"

The activities below are grouped together for convenience only. As noted above, no list of "red flags" can include all activities that warrant referral to the COO.

Insufficient or Suspicious Information

- A Customer provides unusual or suspicious identification documents that cannot be readily verified.
- A Customer is reluctant to provide complete information about the nature and purpose of its business, anticipated account or transaction activity, prior banking relationships, the names of its officers and directors, or information about its business location.
- A Customer's telephone number is disconnected and/or emails to the Customer's email address bounce.
- Information provided by the Customer varies from information obtained through public records.
- The Customer's location differs from that which would be expected on the nature of its business activities.
- A Customer makes frequent or large transactions that don't appear to be consistent with the nature or size of the business.

Efforts to Avoid Reporting or Recordkeeping

- A Customer attempts to persuade Company employees to abstain from filing report or maintaining required records.
- A Customer is reluctant to provide the information needed to file a report, maintain records, or to proceed with a transaction after realizing that a report must be filed.
- A Customer requests an exemption from reporting or recordkeeping requirements.
- A Customer attempts to conduct transactions to or through locations of specific concern (e.g., countries designated by national authorities and/or the FATF) as non-cooperative countries and territories).

Inconsistent with Nature of Business

- The transaction patterns of a business show a sudden change inconsistent with normal or expected activities.

- Unusual transactions among related entities or among accounts that involve the same or related principals.

- Dramatically different patterns of transactions similar businesses or businesses in the same general location.

- The nature, amount, or extent of transaction activity is unexplained, repetitive, or shows unusual patterns without an apparent business reason or is inconsistent with the Customer's business or history.

- Funds transfer activity occurs to or from a financial secrecy haven, or to or from a high-risk geographic location without an apparent business reason, or when the activity is inconsistent with the Customer's business or history.

Suspicious Activity That May Indicate Terrorist Financing

The following activities have been identified by FATF as issues that financial institutions should pay particular attention to. This list of characteristics should be taken into account by financial institutions, along with other available information (including any lists of suspected terrorists, terrorist groups, and associated individuals and entities issued by the United Nations or appropriate national authorities).

- Customer refuses to provide information, attempts to reduce the level of information provided to the minimum, or provides information that is misleading or difficult to verify.

- An account for which several persons have signature authority, yet these persons appear to have no relation among each other (either family ties or business relationship).

- An account opened by a legal entity or an organization that has the same address as other legal entities or organizations but for which the same person or persons have signature authority, when there is no apparent economic or legal reason for such an arrangement (for example, individuals serving as company directors for multiple companies headquartered at the same location, etc.).

- An account opened in the name of a legal entity that is involved in the activities of an association or foundation whose aims are related to the claims or demands of a terrorist organization.

- Transactions to or for an individual where information on the originator, or the person on whose behalf the transaction is conducted, is not provided with the transaction, when the inclusion of such information would be expected.

- Use of multiple personal and business accounts or the accounts of non-profit organizations or charities to collect and then funnel funds immediately or after a short time to a small number of foreign beneficiaries.

- Foreign transactions that are performed on behalf of a Customer by a third party followed by wire transfers of the funds to locations having no apparent business connection with the Customer or to countries of specific concern.

- Financial transactions for which there appears to be no logical economic purpose or in which there appears to be no link between the stated activity of the organization and the other parties in the transaction.

- Unexplained inconsistencies arising from the process of identifying or verifying the Customer (for example, regarding previous or current country of residence, country of issue of the passport, countries visited according to the passport, and documents furnished to confirm name, address and date of birth).

- Transactions involving foreign currency exchanges that are followed within a short time by wire transfers to locations of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).

- Transactions to, from or through a location of specific concern (for example, countries designated by national authorities, FATF non-cooperative countries and territories, etc.).