Open Source Collective
Anti-Money Laundering (AML) Policy

1. Introduction

This Anti-Money Laundering Policy (the "Policy") of Open Source Collective ("OSC") prohibits and aims to actively prevent money laundering and any activity that facilitates money laundering or the funding of terrorist or criminal activities under United States law by complying with the legal requirements of the U.S. Bank Secrecy Act (BSA) and its implementing regulations.

This Policy applies to OSC entities whether they are subject to U.S. law. Where the laws or regulations of any other country or region impose anti-money laundering related compliance obligations on any one or more OSC entities that are more extensive than this Policy, both this Policy and the non-U.S. governing laws or regulations must be complied with.

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. Generally, money laundering occurs in three stages. 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. 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. 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 like 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.

Our AML Policy, procedures and internal controls are designed to ensure compliance with all applicable BSA regulations and FINRA rules and will be reviewed and updated on a regular basis to ensure appropriate policies, procedures and internal controls are in place to account for both changes in regulations and changes in our business.

This Policy is effective as of January 2022 (the "Effective Date").

2. AML Compliance Person Designation and Duties.

OSC has designated the OSC Board Secretary, Pia Mancini, and such person(s) as may be designated by her from time to time, as its initial Anti-Money Laundering Program Compliance Person ("AML Compliance Person"), with full authority for OSC's AML program. The AML Compliance Person may be updated by OSC from time to time. The duties of the AML Compliance Person will include monitoring the OSC's compliance with AML obligations, and overseeing communication and training for employees. The AML Compliance Person will also ensure that the OSC keeps and maintains all the required AML records and will ensure that Suspicious Activity Reports (SAR-SFs) are filed with the Financial Crimes Enforcement Network (FinCEN) when appropriate. The AML Compliance Person is vested with full responsibility and authority to enforce OSC's AML program.

An annual review of FCS information will be conducted by the AML Compliance Person or persons designated by it and will be completed with all necessary updates being provided no later than 17 business days following the end of each calendar year. In addition, if there is any change to the information, the AML Compliance Person will update the information promptly, but in any event not later than 30 days following the change.

3. Giving AML Information to Federal Law Enforcement Agencies and Other Financial Institutions

a. FinCEN Requests Under USA PATRIOT Act Section 314(a)

OSC will respond to a Financial Crimes Enforcement Network (FinCEN) request concerning accounts and transactions (a 314(a) Request) by promptly searching our records to determine whether OSC maintains or has maintained any account for, or have engaged in any transaction with, each individual, entity or organization named in the 314(a) Request as outlined in the Frequently Asked Questions (FAQ) located on FinCEN's secure web site. OSC has14 days (unless otherwise specified by FinCEN) from the transmission date of the request to respond to a 314(a) Request. OSC will designate through the FINRA Contact System (FCS) one or more persons to be the point of contact (POC) for 314(a) Requests and will promptly update the POC information following any change in such information. (*See also* Section 2 above regarding updating of contact information for the AML Compliance Person.) Unless otherwise stated in the 314(a) Request or specified by FinCEN, OSC will search those documents outlined in FinCEN's FAQ. If OSC find a match, the AML Compliance Person will report it to FinCEN via FinCEN's web-based 314(a) Secure Information Sharing System within 14 days or within the time requested by FinCEN in the request. If the search parameters differ from those mentioned above (for example, if FinCEN limits the search to a geographic location), the AML Compliance Person will structure our search accordingly.

If the AML Compliance Person searches OSC's records and does not find a matching account or transaction, then the AML Compliance Person will not reply to the 314(a) Request. OSC will maintain documentation that OSC have performed the required search.

OSC will not disclose the fact that FinCEN has requested or obtained information from us, except to the extent necessary to comply with the information request OSC will direct any questions OSC have about the 314(a) Request to the requesting federal law enforcement agency as designated in the request.

Unless otherwise stated in the 314(a) Request, OSC will not be required to treat the information request as continuing in nature, and OSC will not be required to treat the periodic 314(a) Requests as a government provided list of suspected terrorists for purposes of the customer identification and verification requirements.

b. National Security Letters

National Security Letters (NSLs) are written investigative demands that may be issued by the Federal Bureau of Investigation and other federal government authorities conducting counterintelligence and counterterrorism investigations to obtain necessary information; however, it is important to recognize that OSC is not a broker-dealer. **NSLs are highly confidential. No broker-dealer, officer, employee, or agent of OSC can disclose to any person that a government authority or the FBI has sought or obtained access to records other than OSC's legal counsel. OSC will have policies and procedures in place for processing and maintaining the confidentiality of NSLs.** If OSC files a Suspicious Activity Report (SAR-SF) after receiving a NSL, the SAR-SF should not contain any reference to the receipt or existence of the NSL.

c. Grand Jury Subpoenas

OSC understands that the receipt of a grand jury subpoena concerning a person or entity does not in itself require that OSC file a Suspicious Activity Report (SAR-SF). When OSC receives a grand jury subpoena, OSC will conduct a risk assessment of the person or entity subject to the subpoena as well as review any of that person or entity's account activity. If OSC uncovers suspicious activity during its risk assessment and review, OSC will elevate that risk assessment and file a SAR-SF in accordance with the SAR-SF filing requirements. OSC understands that none of its officers, employees or agents may directly or indirectly disclose to the person who is the subject of the subpoena its existence, its contents, or the information OSC used to respond to it. To maintain the confidentiality of any grand jury subpoena OSC receives, OSC will process and maintain the subpoena. If OSC files a SAR-SF after receiving a grand jury subpoena, the SAR-SF will not contain any reference to the receipt or existence of the subpoena. The SAR-SF will only contain detailed information about the facts and circumstances of the detected suspicious activity.

d. Voluntary Information Sharing With Other Financial Institutions Under USA PATRIOT Act Section 314(b)

OSC will share information with other financial institutions regarding individuals, entities, organizations, and countries for purposes of identifying and, where appropriate, reporting activities that OSC suspect may involve possible terrorist activity or money laundering. The AML Compliance Officer will ensure that OSC files with FinCEN an initial notice before any sharing occurs and annual notices thereafter. OSC will use the notice form found at FinCEN's web site. Before OSC shares information with another financial institution, OSC will take reasonable steps to verify that the other financial institution has submitted the requisite notice to FinCEN, either by obtaining confirmation from the financial institution or by consulting a list of such financial institutions that FinCEN will make available. OSC understands that this requirement applies even to financial institutions with which OSC is affiliated, and that OSC will obtain the requisite notices from affiliates and follow all required procedures.

OSC will employ strict procedures both to ensure that only relevant information is shared and to protect the security and confidentiality of this information, for example, by segregating it from the OSC's other books and records.

OSC also will employ procedures to ensure that any information received from another financial institution shall not be used for any purpose other than:

- identifying and, where appropriate, reporting on money laundering or terrorist activities:
- determining whether to establish or maintain an account, or to engage in a transaction; or
- assisting the financial institution in complying with performing such activities.

4. Checking the Office of Foreign Assets Control Listings

Before opening an account, and on an ongoing basis, the AML Compliance Officer will check to ensure that a customer does not appear on the SDN list or is not engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC. (*See* the OFAC web site for the SDN list and listings of current sanctions and embargoes). Because the SDN list and listings of economic sanctions and embargoes are updated frequently, OSC will consult them on a regular basis and subscribe to receive any available updates when they occur.

If OSC determines that an investor, borrower or portfolio company is on the SDN list or is engaging in transactions that are prohibited by the economic sanctions and embargoes administered and enforced by OFAC, OSC will reject the transaction and/or block their assets and file a blocked assets and/or rejected transaction form with OFAC within 10 days. OSC will also call the OFAC Hotline at (800) 540-6322 immediately.

OSC's review will include investor, borrower or portfolio company accounts and related transactions involving investors, borrowers, or portfolio companies (including activity that passes through the OSC such as wires).

5. Customer Identification Program

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

6. General Customer Due Diligence

It is important to our AML and SAR-SF reporting program that OSC obtain sufficient information about each investor, borrower or portfolio company ("customer") to allow OSC to evaluate the risk presented by that customer and to detect and report suspicious activity.

OSC will take steps to obtain sufficient customer information to comply with our suspicious activity reporting requirements. For accounts that OSC have deemed to be higher risk, OSC will follow its Foreign Corrupt Practices Act and Anti-Bribery Policy.

7. Correspondent Accounts for Foreign Shell Banks

a. Detecting and Closing Correspondent Accounts of Foreign Shell Banks

OSC does not establish, maintain, administer, or manage correspondent accounts for foreign banks.

8. Compliance with FinCEN's Issuance of Special Measures Against Foreign Jurisdictions, Financial Institutions or International Transactions of Primary Money Laundering Concern

If FinCEN issues a final rule imposing a special measure against one or more foreign jurisdictions or financial institutions, classes of international transactions or types of accounts deeming them to be of primary money laundering concern, in the event OSC maintains any accounts (including correspondent accounts) in such jurisdictions or with such institutions OSC will read FinCEN's final rule and seek to follow any prescriptions or prohibitions contained in that rule.

9. Monitoring Accounts for Suspicious Activity

OSC will follow its Foreign Corrupt Practices Act and Anti-Bribery Policy.

a. Emergency Notification to Law Enforcement by Telephone

In situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes, OSC may call an appropriate law enforcement authority. If an investor, borrower, or portfolio company appears on OFAC's SDN list, OSC will call the OFAC Hotline at (800) 540-6322. Other contact numbers OSC may use are: FinCEN's Financial Institutions Hotline ((866) 556-3974) (especially to report transactions relating to terrorist activity), and/or listed numbers for the U.S. Attorney's office, the FBI and the SEC (to voluntarily report such violations to the SEC in addition to contacting appropriate law enforcement authority). If OSC does notify the appropriate law enforcement authority of any such activity, OSC must still file a timely SAR-SF.

Although OSC is not required to, in cases where OSC has filed a SAR-SF that may require immediate attention by the SEC, OSC may contact the SEC via the SEC SAR Alert Message Line at (202) 551-SARS (7277) to alert the SEC about the filing. OSC understand that calling the SEC SAR Alert Message Line does not alleviate its obligations to file a SAR-SF or notify an appropriate law enforcement authority.

b. Red Flags

Red flags that signal possible money laundering or terrorist financing include, but are not limited to:

Customers (defined as a OSC investor, borrower, or portfolio company) – Insufficient or Suspicious Information

- Provides unusual or suspicious identification documents that cannot be readily verified.
- Reluctant to provide complete information about nature and purpose of business, prior banking relationships, anticipated account activity, officers and directors or business location.
- Refuses to identify a legitimate source for funds or information is false, misleading, or substantially incorrect.
- Background is questionable or differs from expectations based on business activities.

Efforts to Avoid Reporting and Recordkeeping

- Reluctant to provide information needed to file reports or fails to proceed with transaction.
- Tries to persuade an officer or employee not to file required reports or not to

maintain required records.
- Unusual concern with the OSC's compliance with U.S. government reporting requirements and OSC's AML policies.

Activity Inconsistent With Business

- Transactions patterns show a sudden change inconsistent with normal activities.
- Appears to be acting as an agent for an undisclosed principal but is reluctant to provide information.

Other Suspicious Customer Activity

- Law enforcement subpoenas.
- Payment by third-party check or money transfer without an apparent connection to the customer.
- No concern regarding the cost of transactions or fees (*i.e.*, surrender fees, higher than necessary commissions, etc.).

c. Responding to Red Flags and Suspicious Activity

When an officer or employee of OSC detects any red flag, or other activity that may be suspicious, he or she will notify the AML Compliance Person. Under the direction of the AML Compliance Person, OSC will determine whether and how to further investigate the matter. This may include gathering additional information internally or from third-party sources, contacting appropriate authorities, and/or filing a SAR-SF.

10. Suspicious Transactions and BSA Reporting

a. Filing a SAR-SF

OSC will file a SAR-SF and notify the appropriate law enforcement authority in situations involving violations that require immediate attention, such as terrorist financing or ongoing money laundering schemes. In addition, although OSC is not required to, OSC may contact that SEC in cases where a SAR-SF OSC have filed may require immediate attention by the SEC. Even if OSC does notify a regulator of a violation, unless it is specifically covered by one of the exceptions in the SAR rule, OSC may file a SAR-SF reporting the violation.

OSC may file a voluntary SAR-SF for any suspicious transaction that OSC believe is relevant to the possible violation of any law or regulation but that is not required to be reported by us under the SAR rule. It is OSC policy that all SAR-SFs will be reported regularly to the Board of Directors of [Circulate Capital, LLC] and appropriate senior management, with a clear reminder of the need to maintain the confidentiality of the SAR-SF.

OSC will report suspicious transactions by completing a SAR-SF, and OSC will collect and maintain supporting documentation as required by the BSA regulations. OSC will file a SAR-SF no later than 30 calendar days after the date of the initial detection of the facts

that constitute a basis for filing a SAR-SF. If no suspect is identified on the date of initial detection, OSC may delay filing the SAR-SF for an additional 30 calendar days pending identification of a suspect, but in no case will the reporting be delayed more than 60 calendar days after the date of initial detection.

The phrase "initial detection" does not mean the moment a transaction is highlighted for review. The 30-day (or 60-day) period begins when an appropriate review is conducted, and a determination is made that the transaction under review is "suspicious" within the meaning of the SAR requirements. A review must be initiated promptly upon identification of unusual activity that warrants investigation.

OSC will retain copies of any SAR-SF filed and the original or business record equivalent of any supporting documentation for five years from the date of filing the SAR-SF. OSC will identify and maintain supporting documentation and make such information available to FinCEN, any other appropriate law enforcement agencies, federal or state securities regulators or SROs upon request.

OSC will not notify any person involved in the transaction that the transaction has been reported, except as permitted by the BSA regulations. OSC understand that anyone who is subpoenaed or required to disclose a SAR-SF or the information contained in the SAR-SF will, except where disclosure is requested by FinCEN, the SEC, or another appropriate law enforcement or regulatory agency, or an SRO registered with the SEC, decline to produce the SAR-SF or to provide any information that would disclose that a SAR-SF was prepared or filed. OSC will notify FinCEN of any such request and our response.

11. AML Recordkeeping

a. Responsibility for Required AML Records and SAR-SF Filing

OSC's AML Compliance Person and his or her designee will be responsible for ensuring that AML records are maintained properly, and that SAR-SFs are filed as required.

OSC will maintain SAR-SFs and their accompanying documentation for at least five years.

b. SAR-SF Maintenance and Confidentiality

OSC will hold SAR-SFs and any supporting documentation confidential. OSC will not inform anyone outside of FinCEN, the SEC, an SRO registered with the SEC or other appropriate law enforcement or regulatory agency about a SAR-SF. OSC will refuse any subpoena requests for SAR-SFs or for information that would disclose that a SAR-SF has been prepared or filed and immediately notify FinCEN of any such subpoena requests that OSC receive. OSC will segregate SAR-SF filings and copies of supporting documentation from other OSC books and records to avoid disclosing SAR-SF filings.

OSC's AML Compliance Person will handle all subpoenas or other requests for SAR-SFs. OSC may share information with another financial institution about suspicious transactions in order to determine whether OSC will jointly file a SAR according to the provisions of Section 3.d. In cases in which OSC file a joint SAR for a transaction that has been handled both by OSC and another financial institution, both financial institutions will maintain a copy of the filed SAR.

12. Training Programs

OSC will develop ongoing employee training under the leadership of the AML Compliance Person and senior management. OSC training will occur on at least an annual basis. It will be based on OSC's size and its resources and be updated as necessary to reflect any new developments in the law.

Our training will include, at a minimum: (1) how to identify red flags and signs of money laundering that arise during the course of the employees' duties; (2) 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 and, where appropriate, the filing of SAR-SFs); (3) what employees' roles are in the OSC's compliance efforts and how to perform them; (4) the OSC's record retention policy; and (5) the disciplinary consequences (including civil and criminal penalties) for non-compliance with the BSA.

Training may include educational pamphlets, videos, intranet systems, in-person lectures and explanatory memos. OSC will maintain records to show the persons trained, the dates of training and the subject matter of their training.

13. Confidential Reporting of AML Non-Compliance

Employees will promptly report any potential violations of the OSC's AML compliance policy to the AML Compliance Person, unless the violations implicate the AML Compliance Person, in which case the employee shall report to the Chair of the Board of Directors. Such reports will be confidential, and the employee will suffer no retaliation for making them.

14. Additional Risk Areas

The OSC has reviewed all areas of its business to identify potential money laundering risks that may not be covered in the procedures described above.

15. Limitations

This Policy and OSC's adoption of this Policy shall not be construed as a consent or acknowledgement by the Fund of, or to: (a) jurisdiction under the laws of any country or territory; or (b) the application to it of the laws or regulations of any country or territory. Such consent or acknowledgment is expressly withheld. This Policy and its contents are confidential

and shall not be shared with parties outside of OSC or its affiliates without the express permission of OSC and/or its AML Compliance Person.

16. Senior Manager Approval

Senior management has approved this AML compliance policy and program in writing as reasonably designed to achieve and monitor OSC's ongoing compliance with the requirements of the BSA and the implementing regulations under it. This approval is indicated by signatures below.

Signed: Pia Mancini

Title: Board Secratary

Date: January 3, 2022